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

IN THE HOUSE OF REPRESENTATIVES

Mr. LIEU introduced the following bill; which was referred to the Committee on ____________________________

A BILL

To regulate law enforcement use of facial recognition technology, 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 “Facial Recognition Act of 2023”.

SEC. 2. INELIGIBILITY FOR CERTAIN FUNDS.

In the case of a State or unit of local government that received a grant award under subpart 1 of part E of title I of the Omnibus Crime Control and Safe Streets
Act of 1968 (42 U.S.C. 3750 et seq.), if the State or unit of local government fails to substantially to comply with the requirements under this Act for a fiscal year, the Attorney General shall reduce the amount that would otherwise be awarded to that State or unit of local government under such grant program in the following fiscal year by 15 percent.

SEC. 3. DEFINITIONS.

In this Act:

(1) ARREST PHOTO DATABASE.—The term “arrest photo database” means a database populated primarily by booking or arrest photographs or photographs of persons encountered by an investigative or law enforcement officer.

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

(3) DERIVED.—The term “derived” means that a Federal or State government would not have possessed the information or evidence but for the use of facial recognition, regardless of any claim that the information or evidence is attenuated from such recognition, and would inevitably have been discovered
or obtained the information or evidence through other means.

(4) **Facial Recognition.**—The term “facial recognition” means an automated or semi-automated process that assists in identifying or verifying an individual or captures information about an individual based on the physical characteristics of an individual’s face, head or body, or that uses characteristics of an individual’s face, head or body, to infer emotion, associations, activities, or the location of an individual.

(5) **Face Surveillance.**—The term “face surveillance” means the use of facial recognition with real-time or stored video footage to track, observe, or analyze the movements, behavior, data, or actions of an individual or groups of individuals.

(6) **Illegitimately Obtained Information.**—The term “illegitimately obtained information” means personal data or information that was obtained—

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

(B) in a manner that violates a service agreement between a provider of an electronic communication service to the public or a pro-
provider 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
(B) does not include any officer, employee, or contractor of a State department of motor vehicles.

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

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

(10) PROSECUTOR.—The term “prosecutor” means the principal prosecuting attorney of a State or any political subdivision thereof and any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure).

(11) OPERATIONAL TESTING.—The term “operational testing” means testing that evaluates a complete facial recognition system as it is used in the field, including measuring false positive and false negative error rates for field uses of the system on operational or operationally representative data and 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-
est 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 RECO-
GNITION 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-
base pursuant to an order issued under subsection (b) and the emergencies and exceptions under subsection (c).

(2) MAINTENANCE.—

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

(i) has not attained 18 years of age;

(ii) has been released without a charge;

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

(iv) was acquitted of the charged offense.

(B) RULE OF CONSTRUCTION.—Nothing in this paragraph shall be construed to prohibit an investigative or law enforcement officer from using a database for other investigative procedures, such as finger printing, and shall only apply to the use of a reference photo database for the use of facial recognition.
(3) PROCEDURES.—Any agency responsible for maintaining and operating an arrest photo database shall establish procedures to ensure compliance with paragraph (3).

(b) ORDERS.—

(1) APPROVAL.—An application for a warrant to use a reference photo database may not be submitted for consideration by a court unless the head of a law enforcement agency (or a designee) approves such an application.

(2) AUTHORITY.—Except as provided by subsection (d), the principal prosecutor of a State or any political subdivision thereof and any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure), may make an application to a court of competent jurisdiction for, in conformity with paragraph (3), an order authorizing the use of facial recognition in conjunction with a reference photo database within the jurisdiction of that judge.

(3) APPLICATION.—Except as provided in subsection (c), a court of competent jurisdiction may issue an order authorizing the use of facial recognition in conjunction with a reference photo database
if a prosecutor submits an application to that court that establishes the following:

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

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

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

(D) Any details regarding other investigative measures taken to identify such person and an explanation for why such measures failed or are reasonably unlikely to succeed.

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

(F) Probable cause to believe that such person has committed or is committing a particular offense or offenses enumerated in section 3559(c)(2)(F) of title 18, United States Code.

(4) CONTENTS OF ORDER.—The order described in this paragraph shall include the following:
(A) All information required to be included in the application pursuant to such paragraph (3).

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

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

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

(5) NOTICE TO THE PUBLIC.—

(A) IN GENERAL.—Each State department of motor vehicles shall post notices in conspicuous locations at each department office, make written information available to all applicants at each office, and provide information on the department website regarding State investigative or law enforcement officers’ searches of driver’s license and ID photos through facial recognition. The notices, written information, and online information must describe how offi-
cers use and access facial recognition in criminal investigations.

(B) LANGUAGE REQUIREMENT.—Notices required under subparagraph (A) shall be posted, as necessary and reasonable, in Spanish or any language common to a significant portion of the department’s customers, if they are not fluent in English. The department shall provide translations of the poster and an electronic link that leads to the department’s website upon request.

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

(A) in subsection (a)—

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

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

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

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

(B) in subsection (b)(1), by inserting before the period at the end the following: “but if
the personal information or highly restricted personal information to be disclosed is a person’s photograph to be used or enrolled in a law enforcement facial recognition system, only on a case-by-case basis that does not involve the bulk transfer of persons’ photographs to a State or Federal law enforcement agency or a qualified third party entity that will allow law enforcement to access those photographs for the purposes of facial recognition”; and

(C) by adding at the end the following:

“(f) LAW ENFORCEMENT ACCESS TO FACIAL RECOGNITION SYSTEMS.—A State department of motor vehicles, and any officer, employee, or contractor thereof, may make available a department-operated facial recognition system to a State or Federal law enforcement agency, or perform searches of such a system on behalf of the agency, only pursuant to an order issued under section 101 of the Facial Recognition Act of 2023.”.

(e) EMERGENCIES AND EXCEPTIONS.—

(1) INITIAL USE.—Notwithstanding subsections (a) and (b), an investigative or law enforcement officer may use or request facial recognition in conjunction with a reference photo database—
(A) to assist in identifying any person who is deceased, incapacitated or otherwise physically unable of identifying himself, or the victim of a crime, whom the officer determines, in good faith, cannot be identified through other means;

(B) to assist in identifying a person whom the officer believes, in good faith, is the subject of an alert through an AMBER Alert communications network, as that term is used in section 301 of the Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act of 2003 (34 U.S.C. 20501);

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

(D) to assist in identifying any person—

(i) if the appropriate prosecutor determines that an emergency situation exists—

(I) that involves immediate danger of death or serious physical injury to any person; or

(II) that requires the use of facial recognition in conjunction with a
reference photo database to occur before an order authorizing such use can, with due diligence, be obtained; and

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

(2) Subsequent Authorization.—If an investigative or law enforcement officer uses facial recognition pursuant to paragraph (1)(D), the prosecutor shall apply for an order approving the use under subsection (b) within 12 hours after the use occurred. The use shall immediately terminate when the application for approval is denied, or in the absence of an application, within 12 hours. In cases where an order is not obtained or denied, the officer shall destroy all information obtained as a result of the search.

(3) Affidavit Required.—With respect to use of facial recognition pursuant to paragraph (1)(D), an appropriate prosecutor shall submit an affidavit to the court identifying specific details on why they believe that an emergency situation under clause (i) exists.
(d) **State Law Preserved.**—The authorities provided by subsections (b) and (c) do not authorize access reference photo databases maintained by a State, or a political subdivision of a State, unless State law expressly and unambiguously authorizes an investigative or law enforcement officer to—

1. access driver’s license and identification document photos; and
2. use facial recognition to conduct searches of those photos.

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

(a) **In General.**—An investigative or law enforcement officer may not—

1. use facial recognition to create a record describing how any individual exercises rights guaranteed by the Constitution, including free assembly, association, and speech;
2. rely on actual or perceived race, ethnicity, national origin, religion, disability, gender, gender identity, or sexual orientation in selecting which person to subject to facial recognition, except when there is trustworthy information, relevant to the locality and time frame, in the context of a particular area and for a particular period of time, that links a person with a particular characteristic described in
this subsection to an identified criminal incident or scheme; or

(3) use facial recognition to enforce the immigration laws of the United States or share facial recognition data with other agencies for the purposes of enforcing the immigration laws of the United States.

(b) Prohibition on Use With Body Cameras.—Any investigative or law enforcement officer may not use or request facial recognition in conjunction with any image obtained from a body camera worn by that or any other officer, dashboard camera, or any aircraft camera, including a drone.

(c) Prohibition on Certain Facial Recognition.—Any investigative or law enforcement officer may not use or request facial recognition for the purpose of face surveillance.

(d) Ensuring Corroboration and Preventing Over Reliance on Matches.—A facial recognition match may not be the sole basis upon which probable cause is established for a search, arrest, or other law enforcement action. Any investigative and law enforcement officers using information obtained from the use of facial recognition shall examine results with care and consider the possibility that matches could be inaccurate.
(c) Prohibition on Illegitimately Obtained Information.—An investigative or law enforcement office may not use facial recognition in conjunction with a database that contains illegitimately obtained information.

SEC. 103. Logging of Searches.

A law enforcement agency whose investigative or law enforcement officers use facial recognition shall log its use of the facial recognition to the extent necessary to comply with the public reporting and audit requirements of sections 104 and 105 of this Act.

SEC. 104. Reporting.

(a) State Reporting Required.—

(1) State Judiciary.—Not later than the last day of the first January after the date of the enactment of this Act, and each January thereafter, each State judge who has issued a court order authorizing or approving facial recognition in conjunction with a reference photo database shall report to a State agency (as determined by the chief executive of the State) the following information:

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

(B) Whether the order or extension was issued pursuant to section 101(b) or section 102(c).
(C) Whether the order or extension was granted as applied for, was modified, or was denied.

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

(E) The identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application.

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

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

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

(C) The arrests that such searches contributed to, and the offenses for which the arrests were made, disaggregated by race, ethnicity, gender, and age.

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

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

(F) The types and names of databases that were used and the number of photos removed with respect to arrest photo databases that were confirmed to have been removed in accordance with this section.

(3) REPORT TO BUREAU OF JUSTICE ASSISTANCE.—Not later than 90 days after such report is submitted under paragraph (1), and annually thereafter, the State agency shall report the information
collected under paragraph (1) to the Director of the
Bureau of Justice Assistance.

(4) Report to Administrative Office of
the United States Courts.—Not later than 90
days after such report is submitted under paragraph
(2), and annually thereafter, the State agency shall
report the information collected under paragraph (2)
to the Director of the Administrative Office of the
United States Courts.

(b) Federal Reporting Required.—Not later
than the last day of the first January after the date of
the enactment of this Act, and each January thereafter—

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

(2) and a Federal prosecutor who requested
such order, shall submit to the Director of the Ad-
ministrative Office of the United States Courts a re-
port including the information under subparagraphs
(A) through (G) of subsection (a)(2).
(c) Public Reporting.—In June of each year the Director of the Administrative Office of the United States Courts shall release to the public, post online, and transmit to the Congress a full and complete report concerning the use of facial recognition in conjunction with reference photo databases, including the information reported to the Director pursuant to subsections (a) and (b).

(d) Rules.—The Director of the Bureau of Justice Assistance and the Director of the Administrative Office of the United States Courts shall issue rules with respect to the content and form of the reports required to be filed under subsections (a) through (c) of this section and sections 105 and 106 of this Act.

SEC. 105. AUDITS.

(a) Federal Level Audit.—

(1) In general.—Any Federal law enforcement agency whose investigative or law enforcement officers use facial recognition, regardless of whether they use a system operated by that agency or another agency, shall annually submit data with respect to their use of facial recognition for audit by the Government Accountability Office to prevent and identify misuse and to ensure compliance with sections 101, 102, and 103 of this Act, including—
(A) a summary of the findings of the audit, including the number and nature of violations identified; and

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

(2) SUSPENSION.—

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

(B) PUBLIC NOTICE.—If use of facial recognition is suspended pursuant to subparagraph (A), the Federal law enforcement agency shall notify the public of such suspension.

(b) STATE LEVEL AUDIT.—

(1) IN GENERAL.—Any State or local law enforcement agency whose investigative or law enforcement officers use facial recognition, regardless of whether they use a system operated by that agency or another agency, shall annually submit data with respect to their use of facial recognition to an independent State agency (as determined by the chief ex-
executive of the State) to prevent and identify misuse and to ensure compliance with sections 101, 102, and 103 of this Act. Such independent State agency shall report—

(A) a summary of the findings of the audit, including the number and nature of violations identified, to Director of the Administrative Office of the United States Courts, and subsequently release that information to the public and post it online;

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

(C) any violations identified by the independent State agency.

(2) SUSPENSION.—

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

(B) PUBLIC NOTICE.—If use of facial recognition is suspended pursuant to subparagraph
(A), the State or local law enforcement agency
shall notify the public of such suspension.

(c) **Disaggregated Data.**—Data collected pursuant
to subsection (a) or (b) shall, when feasible, be collected
in a manner that allows such data to be
disaggregated by race, ethnicity, gender, and age.

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

(a) **Benchmark Testing.**—No investigative or law
enforcement officers may use a facial recognition system
or information derived from it unless that system is annually submitted to the National Institute of Standards and Technology’s benchmark facial recognition test for law enforcement to determine—

(1) the accuracy of the system; and

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

(b) **Benchmark Testing for New Systems.**—No
investigative or law enforcement officers may begin using
a new facial recognition system or information derived
from it unless that system is first submitted to independent testing to determine—

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

(c) PROHIBITION.—Any investigative or law enforcement officer may not use facial recognition that has not achieved a sufficiently high level of accuracy, including in terms of overall accuracy and variance on the basis of race, ethnicity, gender, or age, as determined by the National Institute of Standards and Technology, on its annual benchmark test for law enforcement use.

(d) OPERATIONAL TESTING.—No investigative or law enforcement agencies may use a facial recognition system or information derived from it unless that system is annually submitted to operational testing conducted by an independent entity, in accordance with National Institute of Standards and Technology’s training protocol for operational testing, to determine—

(1) the accuracy of the system;

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

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

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

(f) RULEMAKING REQUIRED.—The Assistant Attorney General of the Department of Justice Civil Rights Division shall issue a rule that establishes what is a sufficiently high level of accuracy for a facial recognition system used by law enforcement, including in terms of overall accuracy and variance on the basis of race, ethnicity, gender, and age. The Assistant Attorney General of the Department of Justice Civil Rights Division shall consult with outside experts in civil rights, civil liberties, racial justice, data privacy, bioethics, law enforcement, public defense, and forensic science and other relevant areas of expertise in drafting the proposed rule.

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

SEC. 107. ENFORCEMENT.

(a) SUPPRESSION.—In the case that the use of facial recognition has occurred, no results from the use and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof.
if the use of facial recognition violated this Act or if the
use was conducted in an emergency under section 101 and
the officer or agency did not subsequently obtain an order
for that use as required under such section.

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

c) CIVIL ACTION.—

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

(2) RELIEF.—In an action under this sub-
section, appropriate relief includes—
(A) such preliminary and other equitable
or declaratory relief as may be appropriate;

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

(C) a reasonable attorney’s fee and other
litigation costs reasonably incurred.

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

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

(B) $50,000 for each violation.

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

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

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

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

(d) CIVIL ACTION FOR DISPARATE IMPACT.—An in-
dividual may bring a civil action when use of facial re-
ognition or face surveillance by a law enforcement agency, or any technological element, criteria, method, or design feature thereof acting individually or in concert, results in disparate treatment or adverse impact against an individual or class of individuals on the basis of race, ethnicity, gender, or age.

SEC. 108. NOTICE REQUIREMENT.

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

(1) a notice of—

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

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

(2) a copy of—

(A) the order that authorized the use of facial recognition;

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

(C) each probe image that was used by the agency;
(D) any modifications made to the probe image;

(E) the candidate list, in rank order, produced by the facial recognition system; and

(F) any other police documentation related to the use of facial recognition in the law enforcement investigation.

(b) LANGUAGE REQUIREMENT.—The information required under subsection (a) shall be provided to such individual in an appropriate language for such individual if the individual is not fluent or literate in English.

TITLE II—CERTAIN REQUIREMENTS AND LIMITATIONS ON FACIAL RECOGNITION SYSTEMS AND RESEARCH

SEC. 201. NATIONAL INSTITUTE FOR STANDARDS AND TECHNOLOGY ASSISTANCE.

(a) In General.—The National Institute of Standards and Technology (hereinafter in this section referred to as “NIST”) shall—

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

(2) develop and offer an ongoing benchmark facial recognition test for law enforcement that—
(A) conducts evaluations of actual algorithms used by law enforcement agencies;

(B) uses the types of probe images, including in terms of quality, actually used by law enforcement agencies in its testing;

(C) evaluates algorithms on larger databases that reflect the size of databases actually used by law enforcement; and

(D) evaluates whether the accuracy of a facial recognition algorithm varies on the basis of race, ethnicity, gender, or age and assessments of bias in facial recognition systems;

(3) develop an operational testing protocol that independent testers and law enforcement agencies may implement for annual operational testing to determine—

(A) the accuracy of the facial recognition system;

(B) the impact of human reviewers on facial recognition system accuracy; and

(C) whether the accuracy of the facial recognition system varies significantly on the basis of race, ethnicity, gender, or age; and

(4) study and develop training standards for human operators reviewing the results of facial rec-
ognition searches to ensure accuracy and prevent bias.

(b) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the National Institute of Standards and Technology to carry out subsection (a) $5,000,000 for each of the fiscal years 2024 through 2027.

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

(a) RULE OF CONSTRUCTION.—Nothing in this Act shall be construed to preempt concurrent or more stringent limitations on the use of facial recognition, or any other privacy, civil rights, and civil liberties laws and rules, by the Federal Government, a State, or a political subdivision of a State.

(b) USE OF FACIAL RECOGNITION.—Nothing in this Act shall be construed to authorize the use of facial recognition by a State, or a political subdivision of a State, unless the laws of that State or political subdivision expressly and unambiguously authorizes such use.

SEC. 203. POLICY ON USE OF FACIAL RECOGNITION SYSTEMS REQUIRED.

Not later than 90 days after the date of the enactment of this Act, each agency covered by this statute shall establish and make publicly available on the internet
website of such agency a policy governing the agency’s use
of facial recognition systems to ensure investigative or law
enforcement officer compliance with the requirements of
this Act.

SEC. 204. LIMITATION ON LIABILITY.

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