XI. MODEL FACE RECOGNITION LEGISLATION

This model bill is written for either Congress or a state legislature.

- The federal bill would control all federal and state law enforcement (1) access to all arrest photo databases and driver's license and ID photo databases, and (2) use of real-time face recognition.
- The state bill would control (1) state law enforcement access to arrest photo databases, (2) state *and federal* law enforcement access to the driver's license and ID photo databases maintained by that state, and (2) state law enforcement use of real-time face recognition within the state.

Language specific to state legislation is in **blue**; federal legislation language is in **red**. To produce a copy of the state bill, delete red text and keep blue text; for the federal bill, delete blue text and keep red text.

This bill is written to regulate law enforcement use of face recognition. However, other remotely capturable biometric technology—such as iris scanning and voice or gait analysis—is rapidly evolving. The Center on Privacy & Technology would welcome the opportunity to assist community advocates or elected officials who wish to craft legislation to regulate remote biometric identification more broadly.

* * *

IN THE _____

A

BILL

To regulate law enforcement use of face recognition technology.

Be it enacted by the _____,

Section 1. Short Title.

This Act may be cited as the "Face Recognition Act of 2016."

Section 2. Definitions. As used in this Act—

(a) **"Face recognition"** means the automated or semi-automated process by which a person is identified or attempted to be identified based on the characteristics of his or her face.

(b) **"Targeted face recognition"** means the use of face recognition to identify or attempt to identify a specific person as part of a specific criminal investigation.

(c) **"Continuous face recognition"** means the use of face recognition to identify or attempt to identify groups of persons as part of a criminal investigation or general surveillance, including the use of face recognition to continuously identify persons whose images are captured or recorded by a surveillance camera.

(d) **"Arrest photo database"** means a database populated primarily by booking or arrest photographs or photographs of persons encountered by investigative or law enforcement officers.

(e) **"[State] identification photo database"** means a database populated primarily by photos from driver's licenses or identification documents made or issued by or under the authority of [the/a] State, or a political subdivision of [the/a] State [, or the United States government].

(f) **"Emergency watchlist"** means a highly targeted database populated by a specific person or persons whom there is probable cause to believe have committed, are committing, or are about to commit an offense that involves the immediate danger of death or serious physical injury to any person.

(g) ["**Investigative or law enforcement officer" means any officer of a State or a political subdivision a State or of the United States, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in the State criminal code or Title 18 of the U.S. Code, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses.**]

(h) ["**State investigative or law enforcement officer" means any officer of the State or a political subdivision the State who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in the State criminal code, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses.**]

Title I. Use of Face Recognition by Law Enforcement

Section 101. Targeted Face Recognition.

(a) Arrest photo databases.—

(1) **General.** [A state/Any] investigative or law enforcement officer shall not use or request targeted face recognition in conjunction with an arrest photo database except as provided in this section.(2)

(2) **Permitted uses.** [A state/Any] investigative or law enforcement officer may use or request targeted face recognition in conjunction with an arrest photo database maintained pursuant to paragraph (3)—

(A) To identify any individual whom the officer encounters in person under circumstances which provide the officer a reasonable suspicion that the person has committed, is committing or is about to commit a criminal offense;

(B) To identify any individual whom the officer reasonably suspects has committed, is committing or is about to commit an offense punishable by imprisonment for more than one year.

(3) Any custodian of an arrest photo database used by or at the request of an investigative or law enforcement officer in conjunction with targeted face recognition shall, every six months, eliminate from that database photos of persons—

(A) Released without a charge;

(B) Released after charges are dropped or dismissed or a nolle prosequi notice is entered; or

(C) Not convicted of the charged offense.

(b) Identification Photo Databases.[1]**—**

(1) **General.** Any investigative or law enforcement officer, state or federal, shall not use or request targeted face recognition in conjunction with [a state/an] identification photo database except as provided in this section.

(2) **Permitted uses.** [Except as provided by paragraph (4),] an investigative or law enforcement officer, state or federal, may use or request targeted face recognition in conjunction with [a state/an] identification photo database pursuant to an order issued under paragraph (3);

(3) **Orders**.—

(A) **Authority.** [Except as provided by paragraph (4),] the principal prosecuting attorney of [the/any] 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), is authorized to make an application to a [Name of State/State or federal] judge of competent jurisdiction for, and such judge may grant in conformity with subparagraph (C), an order authorizing the use of targeted face recognition in conjunction with a [a state/an] identification photo database [within the jurisdiction of that judge] to identify any person whom there is probable cause to believe has committed, is committing, or is about to commit an offense enumerated in subsections (1) and (2) of section 2516 of Title 18 of the U.S. Code.

(B) **Application.** Each application for an order authorizing the use of targeted face recognition in conjunction with a [state] identification photo database shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

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

---

1. **Authors' note:** To *prohibit* the use of driver's license and ID photos for criminal face recognition searches, delete the text in this subsection and include in its place the following statement: "Any investigative or law enforcement officer, state or federal, shall not use targeted face recognition in conjunction with a [state] identification photo database, or acquire in bulk the photos in that database." To institute a truly total ban, even in emergency cases, you will also have to amend the exceptions set out at subsection (c). To *allow* limited use of these photos, include the language set out in subsection (b).

(ii) As full and complete description as possible of the person or persons that the officer seeks to identify;

(iii) A full and complete description of the photos or video portraying that person or persons that will be used to search the [**state**] identification photo database;

(iv) A full and complete statement as to whether or not other investigative procedures to identify that person or persons, including the use of targeted face recognition in conjunction with an arrest photo database, have been tried and failed or why they reasonably appear to be unlikely to succeed;

(v) The specific [**state**] identification photo database or databases to be searched [**, and, in the case of an application to access a state identification photo database transmitted to a federal judge, a certification that the individuals portrayed in that database primarily reside within the jurisdiction of the judge or in the same federal circuit**].

(vi) The particular offense enumerated in subsections (1) and (2) of section 2516 of the U.S. Code that are being investigated; and

(vii) A full and complete statement of the facts and circumstances that provide the officer probable cause to believe that the person or persons have committed, are committing, or are about to commit that offense or offenses.

(C) Issuance.—

(i) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving the use of targeted face recognition in conjunction with [**a state**/**an**] identification photo database [**within the jurisdiction of that judge or in the same federal circuit**], if the judge determines that—

(I) there is probable cause to believe that the person or persons described committed, are committing, or are about to commit a particular offense or offenses enumerated in subsections (1) and (2) of section 2516 of Title 18 of the U.S. Code; and

(II) normal investigative procedures, including the use of targeted face recognition in conjunction with an arrest photo database, have been tried and have failed or reasonably appear to be unlikely to succeed.

(ii) Each order authorizing or approving such use shall state—

(I) The identity of the state or federal law enforcement agency authorized to conduct targeted face recognition, and of the officer authorizing the application;

(II) The authority under which the order is made;

(III) In as much detail as necessary, the person or persons that the officer seeks to identify;

(IV) The photos or video portraying that person or persons that will be used to search the identification photo database, and a prohibition on the use of future photos or video or other any photos or video not specifically listed in the order;

(V) The [state] identification photo database or databases to be searched;

(VI) The period of time within which the agency must execute the search, not to exceed seven days; and

(VII) The particular offense enumerated in subsections (1) and (2) of section 2516 of Title 18 of the U.S. Code that are being investigated.

(D) Notice to the Public. [The] State department[s] of motor vehicles shall post notices in conspicuous locations at all department driver licensing offices, make written information available to all applicants at department driver licensing offices, and provide information on the department[s'] web site[s] regarding [state] investigative or law enforcement officers' searches of driver's license and ID photos through targeted face recognition. The notices, written information, and online information must address how officers' use and access targeted face recognition in criminal investigations.

(E) Conforming Amendments.[2]—[The Driver's Privacy Protection Act, section 2721 of Title 18 of the U.S. Code, shall be amended as follows—

(i) Insert after subparagraph (a)(2) the following subparagraph: "(3) a department-operated face recognition system, except as provided in subsection (c) of this section";

(ii) Insert at the end of subparagraph (b)(1) the following text: "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 face 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 third party entity that will allow law enforcement to access those photographs for the purposes of face recognition"; and

(iii) Insert after subsection (b) the following section: "(c) Law Enforcement Access to Face Recognition Systems.— A State department of motor vehicles, and any officer, employee, or contractor thereof, may make available a department-operated face 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 subparagraph (b)(3) of Title 1 of the Face Recognition Act, or pursuant to the exceptions enumerated in subsection (c) of that Act."]

---

2. **Authors' note:** The federal government has a driver's privacy law (18 U.S.C. 2721); most states do, too. To prevent loopholes, that law has to be amended to ensure (1) that DMV face recognition systems only allow law enforcement to search or request searches of their face recognition systems pursuant to this statute; and (2) that law enforcement agencies do not transfer, in bulk, the photos in those systems to themselves or a third party. The language below amends the federal driver's privacy law to achieve that objective. For state bills, the state driver's privacy law *will* need to be amended in a similar manner.

(4) State Law Preserved.—[The authorities provided by paragraphs (2) and (3) of this subsection do not authorize access to state identification databases maintained by a State, or a political subdivision of a State, where state law prohibits law enforcement—

(A) access to driver's license and identification document photos; or

(B) use of face recognition to conduct searches of those photos.]

(c) Emergencies and exceptions.—

(1) Notwithstanding subsections (a) and (b), [a state/an] investigative law enforcement officer may use or request targeted face recognition in conjunction with an arrest photo database, and an investigative law enforcement officer, state or federal, may use or request targeted face recognition in conjunction with a [state] identification photo database—

(A) To identify 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 identify a minor whom the officer believes, in good faith, is the subject of an AMBER Alert, as that term is used in section 5791 of Title 42 of the U.S. Code;

(C) To identify 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 conduct targeted face recognition in conjunction with [a state/an] identification photo database to identify any person—

(i) if the principal prosecuting attorney of [the/any] State or any political subdivision thereof, or any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) determines that an emergency situation exists that involves immediate danger of death or serious physical injury to any person; or that requires the use of targeted face recognition in conjunction with an identification 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 chapter to authorize such use.

(2) If an investigative or law enforcement officer uses targeted face recognition pursuant to subparagraph (D) above, he shall apply for an order approving the use under paragraph (b)(3) above within twelve 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 twelve hours. In cases where an order is not obtained, the officer shall destroy all information obtained as a result of the search.

(3) [The authority provided by paragraph (1) shall authorize access to state identification databases maintained by a State, or a political subdivision of a State, where state law prohibits law enforcement—

(A) access to driver's license and identification document photos; or

(B) use of face recognition to conduct searches of those photos.]

Section 102. Continuous Face Recognition.[3]

(a) **General.** [A state/any] investigative or law enforcement officer shall not use or request continuous face recognition [within the State] except as provided in this section.

(b) **Permitted uses.** [A state/any] investigative or law enforcement officer may use or request continuous face recognition pursuant to an order issued under paragraph (3);

(1) **Authority.** The principal prosecuting attorney of [the/any] State or any political subdivision thereof [, and the Attorney General of the United States, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division specially designated by the Attorney General,] is authorized to make an application to a [Name of State/state or federal] judge of competent jurisdiction for, and such judge may grant in conformity with paragraph (3), an order authorizing the use of continuous face recognition within [the State/that judge's jurisdiction] in conjunction with a emergency watchlist.

(2) **Application.** Each application for an order authorizing continuous face recognition shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

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

(B) The number of persons on the emergency watchlist;

(C) As full and complete description as possible of the person or persons on the emergency watchlist, or their identities, if known, and the photos or video through which they have been enrolled on the emergency watchlist;

(D) A full and complete description of the nature and specific locations within [the State/the judge's jurisdiction] where continuous face recognition will be performed;

---

3. **Authors' note:** To *prohibit* the use of continuous face recognition, delete the text in this section and include in its place the following statement: "(a) General.—[A state/any] investigative or law enforcement officer shall not use continuous face recognition [within the State]." To institute a truly total ban, even in emergency cases, you will also have to amend the exceptions set out at subsection (c). To *allow* limited use of continuous face recognition, include the language set out below.

(E) A statement of the period of time for which the continuous face recognition is required to be maintained;

(F) A full and complete statement as to whether or not other investigative procedures to locate the person or persons on the emergency watchlist have been tried and failed or why they reasonably appear to be unlikely to succeed;

(G) The particular offense involving the immediate danger of death or serious bodily injury that are being investigated;

(H) A full and complete statement of the facts and circumstances that—

(i) provide the officer probable cause to believe that the person or persons have committed, are committing, or are about to commit that offense or offenses; and

(ii) give reason to believe that an emergency situation exists that requires the use of continuous face recognition without delay;

(I) Where the application is for the extension of an order, a statement setting forth the results thus far obtained from the continuous face recognition, or a reasonable explanation of the failure to obtain such results.

(J) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Issuance.—

(A) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving the use of continuous face recognition within [**the State**/**that judge's jurisdiction**] in conjunction with a emergency watchlist, if the judge determines that—

(i) there is probable cause to believe that the specific person or persons on the emergency watchlist committed, are committing, or are about to commit a particular offense involving the immediate danger of death or bodily injury to any person;

(ii) normal investigative procedures to locate the person or persons on the emergency watchlist, have been tried and have failed or reasonably appear to be unlikely to succeed; and

(iii) an emergency situation exists that requires the use of continuous face recognition without delay.

(B) Each order authorizing or approving such use shall specify—

(i) The identity of the law enforcement agency authorized to conduct continuous face recognition, and of the officer authorizing the application;

(ii) The authority under which the order is made;

(iii) In as much detail as necessary, the person or persons on the emergency watchlist, or their identities, if known, and the photos or video through which they have been enrolled on the emergency watchlist;

(iv) The nature and specific locations within [**the State**/**that judge's jurisdiction**] where continuous face recognition will be performed;

(v) The particular offense that is being investigated; and

(vi) The period of time during which such continuous face recognition is authorized.

(C) No order entered pursuant to this paragraph may authorize or approve continuous face recognition for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than 7 days. Extensions of an order for a maximum of 7 days may be granted, but only upon application for an extension made in accordance with paragraph (2) of this subsection and the court making the findings required by subparagraph (3)(A) of this subsection.

(D) Whenever an order authorizing continuous face recognition is entered pursuant to paragraph (3), the order may require reports to be made to the judge who issued the order showing what progress has been made toward the achievement of the authorized objective and the need for ongoing continuous face recognition. Such reports shall be made at such intervals as the judge may require.

(c) Emergencies and exceptions.—

1. Notwithstanding subsections (a) and (b), [**a state**/**any**] investigative law enforcement officer may use or request continuous face recognition in conjunction with a emergency watchlist if—

(A) the principal prosecuting attorney of [**the**/**any**] State or any political subdivision thereof [**, or the Attorney General of the United States, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division specially designated by the Attorney General,**] determines that—

(i) an emergency situation exists that involves immediate danger of death or serious bodily injury to any person;

(ii) that requires the use of continuous face recognition in conjunction with a emergency watchlist before an order authorizing such use can, with due diligence, be obtained; and

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

(2) If [a state/an] investigative or law enforcement officer uses continuous face recognition pursuant to subparagraph (1) above, the officer shall apply for an order approving the use under paragraph (b)(2) above within twelve hours after the use occurred or began. The use shall immediately terminate when the application for approval is denied, or in the absence of an application, within twelve hours. In cases where an order is not obtained, the officer shall destroy all information obtained as a result of the search.

Section 103. Civil Rights and Civil Liberties. [A state/an] investigative or law enforcement officer shall not—

(a) use face recognition to create a record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual for whom the record is created or unless pertinent to and within the scope of an authorized law enforcement activity where there is reasonable suspicion to believe the individual has engaged, is engaging, or is about to engage in criminal activity; or

(b) rely on actual or perceived race, ethnicity, national origin, religion, disability, gender, gender identity, or sexual orientation in selecting which person to subject to face recognition, except when there is reasonable suspicion, relevant to the locality and timeframe, that links a person with a particular characteristic described in this subsection to an identified criminal incident or scheme.

Section 104. Logging of Searches. [A state/an] law enforcement agency whose investigative or law enforcement officers use targeted or continuous face recognition shall log its use of the technology to the extent necessary to comply with the public reporting and audit requirements of sections 105 and 106 of this Act.

Section 105. Public Reporting.

(a) In January of each year, any judge who has issued an order under subparagraph (b)(3)(C) of section 101 of this Act or an order (or extension thereof) under paragraph (b)(3) of section 102 of this Act in the preceding calendar year, or who has denied approval of an application for such orders or extensions during that period, shall report to [the chief judge of the highest court of the State/the Administrative Office of the United States Courts]—

(1) the fact that an order or extension was applied for;

(2) whether the order or extension was issued pursuant to subparagraph (b)(3)(C) of section 101 of this Act, or paragraph (b)(3) of section 102 of this Act;

(3) the fact that the order or extension was granted as applied for, was modified, or was denied;

(4) the offense specified in the order or application, or extension of an order;

(5) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application;

(6) for orders issued pursuant to subparagraph (b)(3)(C) of section 101 of this Act, the [state] identification photo database that was searched;

(7) for orders issued pursuant to subparagraph (b)(3) of section 102 of this Act—

(A) the number of persons in the emergency watchlist;

(B) the nature and specific locations [within the State] where continuous face recognition was performed; and

(C) the period of time during which continuous face recognition was performed.

(b) In March of each year, the principal prosecuting attorney for [the/a] State, or the principal prosecuting attorney for any political subdivision of [the/a] State [, and the Attorney General, an Assistant Attorney General specially designated by the Attorney General], shall report to [the chief judge of the highest court of the State/the Administrative Office of the United States Courts], with respect to the preceding calendar year—

(1) For the use targeted face recognition in conjunction with an arrest 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 resulted from such searches, and the offenses for which arrests were made;

(D) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained; and

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

(2) For orders granted under subparagraph (b)(3)(C) of section 101 for targeted face recognition in conjunction with [a state/an] identification photo database, for each order—

(A) the information specified in paragraphs (1) through (6) of subsection (a); and

(B) the information specified in subparagraphs (B) through (E) of paragraph (1) in this subsection;

(3) For orders or extensions of orders granted under paragraph (b)(3) of section 102 for continuous face recognition, for each order—

(A) the information specified in paragraphs (1) through (5) and (7) of subsection (a); and

(B) the information specified in subparagraphs (B) through (E) of paragraph (1) in this subsection.

(c) In June of each year [the chief judge of the highest court of the State/the Administrative Office of the United States Courts] shall release to the public, post online, and transmit to [the State Legislature/the Congress] a full and complete report concerning the use of targeted and continuous face

recognition in conjunction with arrest photo databases, [state] identification databases, and emergency watchlists, including—

(1) the number of applications for orders or extensions authorizing or approving targeted face recognition in conjunction with [a state/an] identification photo database or continuous face recognition in conjunction with an emergency watchlist and the number of orders and extensions granted or denied pursuant to this Act during the preceding calendar year.

(2) a summary and analysis of the data required to be filed with [the chief judge of the highest court of the State/the Administrative Office of the United States Courts] by subsections (a) and (c) of this section and sections 106 and 107 of this Act.

(d) The [the chief judge of the highest court of the State/the Administrative Office of the United States Courts] is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (a) and (c) of this section and sections 106 and 107 of this Act.

Section 106. Audits. Any [state] law enforcement agency whose [state] investigative or law enforcement officers use targeted or continuous face recognition, regardless of whether they use a system operated by that agency or another agency, shall annually audit that use to prevent and identify misuse and to ensure compliance with sections 101, 102, and 103 of this Act, and shall report—

(a) a summary of the findings of the audit, including the number and nature of violations identified, to [the chief judge of the highest court of the State/the Administrative Office of the United States Courts], and subsequently release that information to the public and post it online; and

(b) any violations identified to [the principal prosecuting attorney for the State/the Attorney General].

Section 107. Accuracy and Bias Testing.

(a) Any [state] law enforcement agency whose [state] investigative or law enforcement officers operate a system of targeted or continuous face recognition shall regularly submit that system 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.

(b) A summary of the findings of the tests required by subsection (a) shall be submitted to the [the chief judge of the highest court of the State/the Administrative Office of the United States Courts], released to the public, and posted online.

Section 108. Enforcement.

(a) **Suppression.** Whenever targeted or continuous face recognition has occurred, no results from those searches 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 face recognition violated sections 101, 102 or 103 of this Act or if the use was conducted in an emergency pursuant to subparagraph (c)(1)(D) of section 101 or paragraph (c)(1) of section 102 and the officer or agency did not subsequently obtain an order for that use as required by paragraph (c)(2) of section 101 and section (c)(2) of section 102.

(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 willfully or intentionally with respect to the violation, the agency shall promptly initiate a proceeding to determine whether disciplinary action against the officer is warranted.

(c) Civil Action.

(1) In General. Any person who is subject to targeted identification or attempted identification through targeted continuous face recognition in violation of this Act may in a civil action recover from the [state] investigative or law enforcement officer or the state or [federal law] enforcement agency which engaged in that violation such relief as may be appropriate.

(2) Relief. In an action under this subsection, appropriate relief includes—

(i) such preliminary and other equitable or declaratory relief as may be appropriate;

(ii) damages under subparagraph (2) and punitive damages in appropriate cases; and

(iii) 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—

(i) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(ii) statutory damages of whichever is the greater of $500 a day for each day of violation or $50,000;

(4) Defense. A good faith reliance on—

(i) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization; or

(ii) a good faith determination that subsection (c) of section 101 or subsection (c) of section 102 of this Act permitted the conduct complained of;

is a complete defense against any civil or criminal action brought under this chapter.

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

Title II. Funding for Law Enforcement Face Recognition Systems and Research

Section 201. Law Enforcement.[4]

(a) No [state/federal] financial assistance or funds may be expended for the creation, maintenance, or modification of a law enforcement face recognition system unless the agency operating that system—

(1) certifies compliance with sections 104, 105, 106 and 107 of this Act;

(2) certifies that the algorithm employed by its face recognition system has been submitted for testing in the most recent Face Recognition Vendor Test administered by the National Institute of Standards and Technology;

(3) provides documentation to confirm that the agency has released to the public and posted online a use policy governing its use of face recognition and, in the case of a law enforcement agency serving a subdivision of [a/the] State, has secured approval for that policy from a city council or other body primarily comprised of elected officials.

(b) Subsection (a) shall take effect 18 months after the enactment of this Act, except for paragraph (2) of that subsection, which shall take effect five years after enactment.

[Section 202. The National Institute for Standards and Technology

(a) The National Institute of Standards and Technology (NIST) shall—

(1) Develop best practices for law enforcement agencies to evaluate the accuracy of their face recognition systems;

(2) Offer biennial Face Recognition Vendor Tests to evaluate the accuracy of face recognition algorithms;

(3) Develop, and implement as part of Face Recognition Vendor Tests, evaluations of whether the accuracy of a face recognition algorithm varies on the basis of race, ethnicity, gender or age; and

(4) Develop large, high-quality publicly available datasets of facial images to support NIST accuracy and bias testing and similar testing conducted by independent entities.

(b) There is authorized to be appropriated to the National Institute of Standards and Technology to carry out subsection (a) $_____ for each of the fiscal years 2018, 2019, 2020 and 2021.]

---

4. **Authors' Note:** This section (1) uses the power of the purse to condition federal or state funding for law enforcement face recognition on agencies' adopting measures to ensure transparency and accountability; and, in the case of federal legislation, (2) authorizes additional funding for the National Institute of Standards and Technology. Appropriations legislation is highly complex; this language will have to be adapted to the state in which it is offered. Furthermore, these provisions, particularly section 201, may best function as stand-alone amendments to *other* funding legislation. If these subsections are indeed offered as "riders," additional provisions may be added that incorporate some of the protections of sections 101, 102 and 103 of this legislation.