

119TH CONGRESS
1ST SESSION

S. 1691

To limit the use of facial recognition technology in airports, and for other purposes.

IN THE SENATE OF THE UNITED STATES

MAY 8, 2025

Mr. MERKLEY (for himself, Mr. KENNEDY, Mr. MARKEY, Mr. MARSHALL, Mr. VAN HOLLEN, and Mr. DAINES) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

A BILL

To limit the use of facial recognition technology in airports, 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 “Traveler Privacy Pro-
5 tection Act of 2025”.

1 **SEC. 2. LIMITATION ON USE OF FACIAL RECOGNITION**
2 **TECHNOLOGY.**

3 (a) IN GENERAL.—Section 44901 of title 49, United
4 States Code, is amended by adding at the end the fol-
5 lowing new subsection:

6 “(m) **LIMITATION ON USE OF FACIAL RECOGNITION**
7 **TECHNOLOGY.**—

8 “(1) **DEFINITIONS.**—In this subsection:

9 “(A) **1:1 MATCHING SOFTWARE.**—The
10 term ‘1:1 matching software’ means a tech-
11 nology that compares a real-time biometric to a
12 photograph on a passenger’s identification doc-
13 ument.

14 “(B) **1:N IDENTIFICATION SOFTWARE.**—
15 The term ‘1:N identification software’ means a
16 technology that compares a real-time biometric
17 collected from a passenger to a biometric of the
18 passenger already accessible by the Department
19 of Homeland Security.

20 “(C) **ADMINISTRATION.**—The term ‘Ad-
21 ministration’ means the Transportation Secu-
22 rity Administration.

23 “(D) **ADMINISTRATOR.**—The term ‘Admin-
24 istrator’ means the Administrator of the Trans-
25 portation Security Administration.

1 “(E) AFFIRMATIVE EXPRESS CONSENT.—
2 The term ‘affirmative express consent’ means
3 an affirmative act by a passenger that—

4 “(i) clearly communicates the author-
5 ization of the passenger for an act or prac-
6 tice;

7 “(ii) is provided in response to a no-
8 tice that meets the requirements of section
9 2(a)(2); and

10 “(iii) is not—

11 “(I) acceptance of general or
12 broad terms of service or a similar
13 document; or

14 “(II) accomplished by entering
15 an airport security checkpoint or
16 standing in a line.

17 “(F) AIRPORT.—The term ‘airport’ has
18 the meaning given such term in section 47102.

19 “(G) APPROVED IDENTIFICATION DOCU-
20 MENT.—The term ‘approved identification docu-
21 ment’ means any document identified by the
22 Transportation Security Administration as ac-
23 ceptable identification consistent with applicable
24 laws and regulations, including—

1 “(i) a State driver’s license or other
2 photo identification card issued by a de-
3 partment of motor vehicles of a State;

4 “(ii) an enhanced driver’s license
5 issued by a State;

6 “(iii) a United States passport or
7 passport card;

8 “(iv) biometrically secure card issued
9 by a trusted traveler program of the De-
10 partment of Homeland Security, includ-
11 ing—

12 “(I) Global Entry;

13 “(II) Nexus; and

14 “(III) Secure Electronic Network
15 for Travelers Rapid Inspection
16 (SENTRI);

17 “(v) an identification card issued by
18 the Department of Defense, including such
19 a card issued to a dependent;

20 “(vi) a permanent resident card;

21 “(vii) a border crossing card issued by
22 the Department of State;

23 “(viii) an acceptable photo identifica-
24 tion issued by a Federally recognized In-

1 dian Tribe, including an Enhanced Tribal
2 Card (ETC);

3 “(ix) a personal identity verification
4 credential issued in accordance with Home-
5 land Security Presidential Directive 12;

6 “(x) a passport issued by a foreign
7 government;

8 “(xi) a driver’s license issued by a
9 province of Canada;

10 “(xii) a Secure Certificate of Indian
11 Status issued by the Government of Can-
12 ada;

13 “(xiii) a transportation worker identi-
14 fication credential (TWIC);

15 “(xiv) a United States Citizenship and
16 Immigration Services Employment Author-
17 ization Card (I-766);

18 “(xv) a Merchant Mariner Credential
19 issued by the Coast Guard; and

20 “(xvi) a Veteran Health Identification
21 Card (VHIC) issued by the Department of
22 Veterans Affairs.

23 “(H) BIOMETRIC INFORMATION.—The
24 term ‘biometric information’ means any data
25 that allows or confirms the unique identification

1 or verification of an individual and is generated
2 from the measurement or processing of unique
3 biological, physical, or physiological characteris-
4 tics, including—

5 “(i) fingerprints;

6 “(ii) voice prints;

7 “(iii) iris or retina imagery scans;

8 “(iv) facial or hand mapping, geom-
9 etry, or templates;

10 “(v) deoxyribonucleic acids (DNA);

11 and

12 “(vi) gait.

13 “(I) IDENTITY VERIFICATION.—The term
14 ‘identity verification’ means the confirmation of
15 the identity of a passenger before admittance to
16 the sterile area of the airport.

17 “(J) PASSENGER.—The term ‘passenger’
18 means an individual who is not an employee or
19 contractor of the Administration.

20 “(K) SCREENING LOCATION; STERILE
21 AREA.—The terms ‘screening location’ and
22 ‘sterile area’ have the meanings given those
23 terms in section 1540.5 of title 49, Code of
24 Federal Regulations.

1 “(L) TRUSTED TRAVELER PROGRAM.—The
2 term ‘Trusted Traveler Program’ means any of
3 the following:

4 “(i) Global Entry.

5 “(ii) The PreCheck Program.

6 “(iii) SENTRI.

7 “(iv) NEXUS.

8 “(2) PRIVACY FOR PASSENGERS.—

9 “(A) IN GENERAL.—Except as provided in
10 subparagraphs (B), (C), and (D) the Adminis-
11 trator may not, for any purpose, capture, col-
12 lect, store, or otherwise process biometric infor-
13 mation collected through or for the use of facial
14 recognition technology or facial matching soft-
15 ware with respect to a passenger.

16 “(B) USE OF TECHNOLOGY FOR
17 VERIFICATION OF DOCUMENTS.—The Adminis-
18 trator may use technology to process, capture,
19 scan and receive data from an identification
20 document containing a photograph of a pas-
21 senger to access secure flight data, authenticate
22 the pre-screening status of a passenger, or
23 verify the accuracy of the identification docu-
24 ment.

1 “(C) TECHNOLOGY FOR TRUSTED TRAV-
2 ELER PROGRAMS.—The Administrator may use
3 facial recognition or facial matching technology
4 to perform identity verification solely at the
5 screening location if the Administrator—

6 “(i) ensures that each passenger en-
7 rolling in a Trusted Traveler Program is
8 given clear and conspicuous notice at the
9 time of enrollment and renewal of enroll-
10 ment of how biometric information of the
11 passenger will be used, processed, stored,
12 shared, and deleted;

13 “(ii) provides each passenger enrolled
14 in a Trusted Traveler Program with the
15 option to opt-out of the use of facial rec-
16 ognition or facial matching technology for
17 identity verification at the screening loca-
18 tion;

19 “(iii) notifies each passenger enrolled
20 in a Trusted Traveler Program at the
21 point of identity verification and as the
22 passenger approaches the point of identity
23 verification of such opt-out option via sim-
24 ple and clear signage, spoken announce-

1 ments, and other accessible and easy-to-un-
2 derstand notifications;

3 “ (iv) ensures equal ability for pas-
4 sengers to choose either identification op-
5 tion;

6 “ (v) does not subject passengers who
7 choose the opt-out option to discriminatory
8 treatment, additional screening require-
9 ments, less favorable screening conditions,
10 or other unfavorable treatment; and

11 “ (vi) for each passenger who chooses
12 the opt-out option, performs identity
13 verification using an approved identifica-
14 tion document and without collecting any
15 biometric information from such passenger.

16 “(D) TECHNOLOGY FOR GENERAL PAS-
17 SENGERS.—

18 “(i) IN GENERAL.—The Administrator
19 shall perform identity verification for pas-
20 sengers not enrolled in a Trusted Traveler
21 Program using an approved identification
22 document and without collecting any bio-
23 metric information from such passengers.

24 “(ii) AUTHORITY TO USE FACIAL
25 MATCHING.—The Administrator may use

1 facial recognition or facial matching tech-
2 nology to perform identity verification for
3 passengers not enrolled in a Trusted Trav-
4 eler Program solely at the screening loca-
5 tion if the Administrator—

6 “(I) provides each passenger with
7 the option to opt-in to the use of fa-
8 cial recognition or facial matching
9 technology for identity verification at
10 the screening location;

11 “(II) notifies each passenger at
12 the point of identity verification and
13 as the passenger approaches the point
14 of identity verification of such opt-in
15 option via simple and clear signage,
16 spoken announcements, and other ac-
17 cessible and easy-to-understand notifi-
18 cations;

19 “(III) ensures equal ability for
20 passengers to choose either identifica-
21 tion option;

22 “(IV) receives affirmative-express
23 consent from the passenger to use fa-
24 cial recognition or facial matching
25 technology for identity verification

1 prior to each use of facial recognition
2 or facial matching technology with re-
3 spect to such passenger; and

4 “(V) does not subject passengers
5 who do not choose the opt-in option to
6 discriminatory treatment, additional
7 screening requirements, less favorable
8 screening conditions, or other unfavor-
9 able treatment.”.

10 “(E) NOTIFICATION GUIDELINES.—A noti-
11 fication provided in accordance with subpara-
12 graph (C)—

13 “(i) shall—

14 “(I) notify passengers of the op-
15 tion described in subparagraph (C)(ii)
16 via simple and clear signage, spoken
17 announcements, and other accessible
18 and easy to understand notifications;

19 “(II) describe the specific steps
20 passengers may take to exercise such
21 option;

22 “(III) notify passengers that an
23 election not to use facial recognition
24 technology or facial matching software
25 will not subject them to discrimina-

1 tory treatment, additional screening
2 requirements, less favorable screening
3 conditions, or other unfavorable treat-
4 ment solely as a result of that elec-
5 tion; and

6 “(IV) be properly placed across
7 relevant areas of the airport including
8 airline check-in areas, airport security
9 checkpoints, and airport gate areas;
10 and

11 “(ii) may not encourage passengers to
12 choose one method of identity verification
13 over another method.

14 “(F) EXCEPTION.—The option described
15 in subparagraph (D)(ii) does not apply with re-
16 spect to a passenger—

17 “(i) who does not provide an accept-
18 able form of identification at a security
19 checkpoint; and

20 “(ii) whose identity the Administrator
21 may need to verify through alternative
22 measures to enter the sterile area.

23 “(3) DATA MINIMIZATION OF PASSENGERS.—
24 Beginning on the date that is 30 days after the date
25 of the enactment of this subsection, in processing bi-

1 ometric information collected through the use of 1:1
2 matching software or 1:N identification software
3 with respect to a passenger, the Administrator—

4 “(A) may capture facial images only as di-
5 rectly relevant and necessary to accomplish the
6 identity verification of the passenger; and

7 “(B) may not, except as provided in para-
8 graph (4)—

9 “(i) share outside of the Administra-
10 tion any biometric information collected
11 through the use of facial recognition or fa-
12 cial matching technology;

13 “(ii) store biometric information col-
14 lected through 1:1 matching software for
15 longer than is necessary to complete iden-
16 tity verification of a passenger or through
17 1:N identification software for longer than
18 24 hours after the scheduled flight depar-
19 ture time of the passenger; or

20 “(iii) compare the image of a pas-
21 senger against anything other than the
22 photo identification document provided by
23 the passenger, except to the extent nec-
24 essary to operate a Trusted Traveler Pro-
25 gram.

1 “(4) EXCEPTION FOR TESTING AND EVALUA-
2 TION.—The Administrator may, for the purpose of
3 testing and evaluation, in a separate area from the
4 general passenger screening area, retain the cap-
5 tured facial image of a passenger undergoing iden-
6 tity verification as a part of a Trusted Traveler Pro-
7 gram taken at a screening location so long as—

8 “(A) the screening location where the iden-
9 tity verification is conducted and images are
10 processed for testing otherwise meets the re-
11 quirements described in paragraphs (2) and (3);

12 “(B) the Administrator gives notice to the
13 passenger in accordance with section 552a of
14 title 5 (commonly referred to as the ‘Privacy
15 Act of 1974’) regarding the storage, use, and
16 sharing of biometric information by the Admin-
17 istration;

18 “(C) the notice described in subparagraph
19 (B) provides clear and conspicuous notice to
20 passengers at the point of identity verification
21 and as passengers approach the point of iden-
22 tity verification of how biometric data collected
23 will be stored, used, shared, or otherwise proc-
24 essed;

1 “(D) images collected, shared, stored, or
2 otherwise processed by the Administration, in-
3 cluding images collected prior to the date of en-
4 actment of this subsection, are deleted not later
5 than 90 days after collection; and

6 “(E) captured facial images are not used
7 for any purpose other than to test and evaluate
8 the 1:1 matching software or 1:N identification
9 software used by the Administration.

10 “(5) DISPOSAL OF FACIAL BIOMETRICS.—Not
11 later than 90 days after the date of the enactment
12 of this subsection, the Administrator shall dispose of
13 any biometric information, including images and vid-
14 eos, collected, or stored by the Administration prior
15 to such date of enactment that, if collected or stored
16 on or after such date of enactment, would violate
17 this subsection.

18 “(6) PROHIBITION ON PASSIVE SURVEIL-
19 LANCE.—Under no circumstances may the Adminis-
20 trator use facial recognition technology or facial
21 matching software to track or identify passengers
22 outside of the screening location, or to profile, tar-
23 get, or discriminate against any passenger solely for
24 exercising their Constitutional rights or to enable

1 systemic, indiscriminate, or wide-scale monitoring,
2 surveillance, or tracking.

3 “(7) GAO REPORT ON USE OF FACIAL REC-
4 COGNITION TECHNOLOGY.—

5 “(A) IN GENERAL.—Not later than 1 year
6 after the date of the enactment of this sub-
7 section, and annually thereafter, the Comp-
8 troller General of the United States shall study
9 the use of 1:1 matching software and 1:N iden-
10 tification software by the Administration, and
11 submit to Congress a report that includes—

12 “(i) an assessment of the effectiveness
13 of the use by the Administration of 1:1
14 matching software and 1:N identification
15 software—

16 “(I) to strengthen security;

17 “(II) to improve the experiences
18 of passengers and air carrier, airport,
19 and Administration employees at air-
20 ports; and

21 “(III) to manage the costs of se-
22 curity screening;

23 “(ii) an assessment of false positive
24 and false negative facial identification
25 matches to identification documents de-

1 tected at airports using 1:1 matching soft-
2 ware and 1:N identification software at
3 screening locations and at airports not
4 using such technology or software;

5 “(iii) a summary of the methodology
6 and results of any testing performed by the
7 Comptroller General in relation to the effi-
8 cacy of the use of 1:1 matching software
9 and 1:N identification software by the Ad-
10 ministration, including any research on
11 bias, disaggregated by age, race, ethnicity
12 to the extent practicable, and sex, the dif-
13 ferent technologies used by the Adminis-
14 tration, and efforts to minimize the bias in
15 operations of the Administration; and

16 “(iv) recommendations to protect pas-
17 senger privacy, civil rights, and civil liberty
18 interests.

19 “(B) FORM.—A report submitted under
20 subparagraph (A) shall be submitted in unclas-
21 sified form but may include a classified annex.

22 “(C) RULE OF CONSTRUCTION; PROTEC-
23 TION OF PERSONAL INFORMATION.—Nothing in
24 this paragraph shall be construed to authorize
25 or require the unauthorized disclosure of the

1 personal information of passengers, and the re-
2 port required by this paragraph shall be re-
3 leased in a manner that protects personal infor-
4 mation from unauthorized use or unauthorized
5 disclosure.”.

6 (b) AMENDMENTS TO AVIATION AND TRANSPOR-
7 TATION SECURITY ACT.—The Aviation and Transpor-
8 tation Security Act (Public Law 107–71; 115 Stat. 597)
9 is amended—

10 (1) in section 109(a)(7) (49 U.S.C. 114 note)
11 by inserting “, subject to the restrictions of section
12 44901(n) of title 49, United States Code,” after
13 “technologies”; and

14 (2) in section 137(d)(3) (49 U.S.C. 44912
15 note), by inserting “, subject to the restrictions of
16 section 44901(n) of title 49, United States Code,”
17 after “biometrics”.

18 (c) ADDITIONAL MODIFICATIONS WITH RESPECT TO
19 AIR TRANSPORTATION SECURITY.—Section 44903 of title
20 49, United States Code, is amended—

21 (1) in subsection (c)(3), by inserting “, subject
22 to the restrictions of section 44901(n),” after “other
23 technology”;

1 (2) in subsection (g)(2)(G), by inserting “, sub-
2 ject to the restrictions of section 44901(n),” after
3 “technologies”; and

4 (3) in subsection (h)(4)(E), by inserting “, sub-
5 ject to the restrictions of section 44901(n),” after
6 “technology”.

○