119TH CONGRESS
1ST SESSION

S. _____

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

IN THE SENATE OF THE UNITED STATES

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 _____

A BILL

To limit the use of facial recognition technology in airports, 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 ''Traveler Privacy Protection Act of 2025''.

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

(a) IN GENERAL .—Section 44901 of title 49, United States Code, is amended by adding at the end the following new subsection:

"(m) LIMITATION ON USE OF FACIAL RECOGNITION TECHNOLOGY.—

"(1) DEFINITIONS.—In this subsection:

"(A) 1:1 MATCHING SOFTWARE.—The term '1:1 matching software' means a technology that compares a real-time biometric to a photograph on a passenger's identification document.

"(B) 1:N IDENTIFICATION SOFTWARE.—The term '1:N identification software' means a technology that compares a real-time biometric collected from a passenger to a biometric of the passenger already accessible by the Department of Homeland Security.

"(C) ADMINISTRATION.—The term 'Administration' means the Transportation Security Administration.

"(D) ADMINISTRATOR.—The term 'Administrator' means the Administrator of the Transportation Security Administration.

"(E) AFFIRMATIVE EXPRESS CONSENT.—The term 'affirmative express consent' means an affirmative act by a passenger that—

"(i) clearly communicates the authorization of the passenger for an act or practice;

"(ii) is provided in response to a notice that meets the requirements of section 2(a)(2); and

"(iii) is not—

"(I) acceptance of general or broad terms of service or a similar document; or

"(II) accomplished by entering an airport security checkpoint or standing in a line.

"(F) AIRPORT.—The term 'airport' has the meaning given such term in section 47102.

"(G) APPROVED IDENTIFICATION DOCUMENT.—The term 'approved identification document' means any document identified by the Transportation Security Administration as acceptable identification consistent with applicable laws and regulations, including—

"(i) a State driver's license or other photo identification card issued by a department of motor vehicles of a State;

"(ii) an enhanced driver's license issued by a State;

"(iii) a United States passport or passport card;

"(iv) biometrically secure card issued by a trusted traveler program of the Department of Homeland Security, including—

"(I) Global Entry;

"(II) Nexus; and

"(III) Secure Electronic Network for Travelers Rapid Inspection (SENTRI);

"(v) an identification card issued by the Department of Defense, including such a card issued to a dependent;

"(vi) a permanent resident card;

"(vii) a border crossing card issued by the Department of State;

"(viii) an acceptable photo identification issued by a Federally recognized Indian Tribe, including an Enhanced Tribal Card (ETC);

"(ix) a personal identity verification credential issued in accordance with Homeland Security Presidential Directive 12;

"(x) a passport issued by a foreign government;

"(xi) a driver's license issued by a province of Canada;

"(xii) a Secure Certificate of Indian Status issued by the Government of Canada

"(xiii) a transportation worker identification credential (TWIC);

"(xiv) a United States Citizenship and Immigration Services Employment Authorization Card (I–766);

"(xv) a Merchant Mariner Credential issued by the Coast Guard; and

"(xvi) a Veteran Health Identification Card (VHIC) issued by the Department of Veterans Affairs.

"(H) BIOMETRIC INFORMATION.—The term 'biometric information' means any data that allows or confirms the unique identification or verification of an individual and is generated from the measurement or processing of unique

biological, physical, or physiological characteristics, including—

"(i) fingerprints;

"(ii) voice prints;

"(iii) iris or retina imagery scans;

"(iv) facial or hand mapping, geometry, or templates;

"(v) deoxyribonucleic acids (DNA); and

"(vi) gait.

"(I) IDENTITY VERIFICATION.—The term 'identity verification' means the confirmation of the identity of a passenger before admittance to the sterile area of the airport.

"(J) PASSENGER.—The term 'passenger' means an individual who is not an employee or contractor of the Administration.

"(K) SCREENING LOCATION; STERILE AREA.—The terms 'screening location' and 'sterile area' have the meanings given those terms in section 1540.5 of title 49, Code of Federal Regulations.

"(L) TRUSTED TRAVELER PROGRAM.—The term 'Trusted Traveler Program' means any of the following:

"(i) Global Entry.

"(ii) The PreCheck Program.

"(iii) SENTRI.

"(iv) NEXUS.

"(2) PRIVACY FOR PASSENGERS.—

"(A) IN GENERAL.—Except as provided in subparagraphs (B), (C), and (D) the Administrator may not, for any purpose, capture, collect, store, or otherwise process biometric information collected through or for the use of facial recognition technology or facial matching software with respect to a passenger.

"(B) USE OF TECHNOLOGY FOR VERIFICATION OF DOCUMENTS.—The Administrator may use technology to process, capture, scan and receive data from an identification document containing a photograph of a passenger to access secure flight data, authenticate the pre-screening status of a passenger, or verify the accuracy of the identification document.

"(C) TECHNOLOGY FOR TRUSTED TRAVELER PROGRAMS.—The Administrator may use facial recognition or facial matching technology

to perform identity verification solely at the screening location if the Administrator—

"(i) ensures that each passenger enrolling in a Trusted Traveler Program is given clear and conspicuous notice at the time of enrollment and renewal of enrollment of how biometric information of the passenger will be used, processed, stored, shared, and deleted;

"(ii) provides each passenger enrolled in a Trusted Traveler Program with the option to opt-out of the use of facial recognition or facial matching technology for identity verification at the screening location;

"(iii) notifies each passenger enrolled in a Trusted Traveler Program at the point of identity verification and as the passenger approaches the point of identity verification of such opt-out option via simple and clear signage, spoken announcements, and other accessible and easy-to-understand notifications;

"(iv) ensures equal ability for passengers to choose either identification option;

"(v) does not subject passengers who choose the opt-out option to discriminatory treatment, additional screening requirements, less favorable screening conditions, or other unfavorable treatment; and

"(vi) for each passenger who chooses the opt-out option, performs identity verification using an approved identification document and without collecting any biometric information from such passenger.

"(D) TECHNOLOGY FOR GENERAL PASSENGERS.—

"(i) IN GENERAL.—The Administrator shall perform identity verification for passengers not enrolled in a Trusted Traveler Program using an approved identification document and without collecting any biometric information from such passengers.

"(ii) AUTHORITY TO USE FACIAL MATCHING.—The Administrator may use facial recognition or facial matching technology to perform identity verification for

passengers not enrolled in a Trusted Traveler Program solely at the screening location if the Administrator—

"(I) provides each passenger with the option to opt-in to the use of facial recognition or facial matching technology for identity verification at the screening location;

"(II) notifies each passenger at the point of identity verification and as the passenger approaches the point of identity verification of such opt-in option via simple and clear signage, spoken announcements, and other accessible and easy-to-understand notifications;

"(III) ensures equal ability for passengers to choose either identification option;

"(IV) receives affirmative-express consent from the passenger to use facial recognition or facial matching technology for identity verification prior to each use of facial recognition

or facial matching technology with respect to such passenger; and

''(V) does not subject passengers who do not choose the opt-in option to discriminatory treatment, additional screening requirements, less favorable screening conditions, or other unfavorable treatment.''.

''(E) NOTIFICATION GUIDELINES.—A notification provided in accordance with subparagraph (C)—

''(i) shall—

''(I) notify passengers of the option described in subparagraph (C)(ii) via simple and clear signage, spoken announcements, and other accessible and easy to understand notifications;

''(II) describe the specific steps passengers may take to exercise such option;

''(III) notify passengers that an election not to use facial recognition technology or facial matching software will not subject them to discriminatory treatment, additional screening

requirements, less favorable screening conditions, or other unfavorable treatment solely as a result of that election; and

''(IV) be properly placed across relevant areas of the airport including airline check-in areas, airport security checkpoints, and airport gate areas; and

''(ii) may not encourage passengers to choose one method of identity verification over another method.

''(F) EXCEPTION.—The option described in subparagraph (D)(ii) does not apply with respect to a passenger—

''(i) who does not provide an acceptable form of identification at a security checkpoint; and

''(ii) whose identity the Administrator may need to verify through alternative measures to enter the sterile area.

''(3) DATA MINIMIZATION OF PASSENGERS.—Beginning on the date that is 30 days after the date of the enactment of this subsection, in processing biometric information collected through the use of 1:1

matching software or 1:N identification software with respect to a passenger, the Administrator—

"(A) may capture facial images only as directly relevant and necessary to accomplish the identity verification of the passenger; and

"(B) may not, except as provided in paragraph (4)—

"(i) share outside of the Administration any biometric information collected through the use of facial recognition or facial matching technology;

"(ii) store biometric information collected through 1:1 matching software for longer than is necessary to complete identity verification of a passenger or through 1:N identification software for longer than 24 hours after the scheduled flight departure time of the passenger; or

"(iii) compare the image of a passenger against anything other than the photo identification document provided by the passenger, except to the extent necessary to operate a Trusted Traveler Program.

"(4) EXCEPTION FOR TESTING AND EVALUATION.—The Administrator may, for the purpose of testing and evaluation, in a separate area from the general passenger screening area, retain the captured facial image of a passenger undergoing identity verification as a part of a Trusted Traveler Program taken at a screening location so long as—

"(A) the screening location where the identity verification is conducted and images are processed for testing otherwise meets the requirements described in paragraphs (2) and (3);

"(B) the Administrator gives notice to the passenger in accordance with section 552a of title 5 (commonly referred to as the 'Privacy Act of 1974') regarding the storage, use, and sharing of biometric information by the Administration;

"(C) the notice described in subparagraph (B) provides clear and conspicuous notice to passengers at the point of identity verification and as passengers approach the point of identity verification of how biometric data collected will be stored, used, shared, or otherwise processed;

"(D) images collected, shared, stored, or otherwise processed by the Administration, including images collected prior to the date of enactment of this subsection, are deleted not later than 90 days after collection; and

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

"(5) DISPOSAL OF FACIAL BIOMETRICS.—Not later than 90 days after the date of the enactment of this subsection, the Administrator shall dispose of any biometric information, including images and videos, collected, or stored by the Administration prior to such date of enactment that, if collected or stored on or after such date of enactment, would violate this subsection.

"(6) PROHIBITION ON PASSIVE SURVEILLANCE.—Under no circumstances may the Administrator use facial recognition technology or facial matching software to track or identify passengers outside of the screening location, or to profile, target, or discriminate against any passenger solely for exercising their Constitutional rights or to enable

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

''(7) GAO REPORT ON USE OF FACIAL RECOGNITION TECHNOLOGY.—

''(A) IN GENERAL.—Not later than 1 year after the date of the enactment of this subsection, and annually thereafter, the Comptroller General of the United States shall study the use of 1:1 matching software and 1:N identification software by the Administration, and submit to Congress a report that includes—

''(i) an assessment of the effectiveness of the use by the Administration of 1:1 matching software and 1:N identification software—

''(I) to strengthen security;

''(II) to improve the experiences of passengers and air carrier, airport, and Administration employees at airports; and

''(III) to manage the costs of security screening;

''(ii) an assessment of false positive and false negative facial identification matches to identification documents de-

tected at airports using 1:1 matching software and 1:N identification software at screening locations and at airports not using such technology or software;

''(iii) a summary of the methodology and results of any testing performed by the Comptroller General in relation to the efficacy of the use of 1:1 matching software and 1:N identification software by the Administration, including any research on bias, disaggregated by age, race, ethnicity to the extent practicable, and sex, the different technologies used by the Administration, and efforts to minimize the bias in operations of the Administration; and

''(iv) recommendations to protect passenger privacy, civil rights, and civil liberty interests.

''(B) FORM.—A report submitted under subparagraph (A) shall be submitted in unclassified form but may include a classified annex.

''(C) RULE OF CONSTRUCTION; PROTECTION OF PERSONAL INFORMATION.—Nothing in this paragraph shall be construed to authorize or require the unauthorized disclosure of the

personal information of passengers, and the report required by this paragraph shall be released in a manner that protects personal information from unauthorized use or unauthorized disclosure.''.

(b) AMENDMENTS TO AVIATION AND TRANSPORTATION SECURITY ACT.—The Aviation and Transportation Security Act (Public Law 107–71; 115 Stat. 597) is amended—

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

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

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

(1) in subsection (c)(3), by inserting '', subject to the restrictions of section 44901(n),'' after ''other technology'';

(2) in subsection (g)(2)(G), by inserting ", subject to the restrictions of section 44901(n)," after "technologies"; and

(3) in subsection (h)(4)(E), by inserting ", subject to the restrictions of section 44901(n)," after "technology".