

**BIOMETRIC DATA USE IN
INTERNATIONAL TRAVEL: THE TENSION
BETWEEN CONVENIENCE, SPEED, AND
PRIVACY**

*Deborah E. Ransom**

INTRODUCTION 349

II. BACKGROUND 353

 A. *Biometric Technology*353

 B. *Biometric Data Collection by the U.S. Government*..355

 C. *Biometric Tech in Aviation Security*.....357

 1. CBP Trusted Traveler Programs..... 357

 2. Traveler Verification Service..... 361

III. CURRENT LAWS 364

 A. *Legal Authorization for Biometric Data Collection* ..364

 B. *Federal Data Privacy Laws*.....370

 1. Privacy Act of 1974..... 370

 2. Freedom of Information Act of 1966 (FOIA)..... 373

 3. DHS Chief Privacy Officer and Other Privacy Requirements 373

IV. RISKS AND RECOMMENDATIONS 374

 A. *Risks*.....374

 1. Data Security Concerns 374

* Deborah E. Ransom received her J.D. from the University of Houston Law Center and her B.A. from Wellesley College. She practices law at Kane Russell Coleman Logan, PC as a Corporate Associate.

2. Accuracy and Civil Rights Concerns	375
3. Lack of transparency and understanding.....	376
B. <i>Proposal</i>	377
1. Institute a moratorium and amend the Facial Recognition Act.....	377
2. Cybersecurity	377
3. Improve transparency	378
4. Create a realistic, timely opt-out alternative	379
V. CONCLUSION	379

INTRODUCTION

The COVID–19 pandemic led to a shutdown of international travel due to country-imposed travel restrictions.¹ However, since the introduction of COVID–19 vaccines and gradual easing of travel restrictions, international tourism returned to 60% of pre-pandemic levels for the January to July 2022 period.² In 2023, international tourism still lagged compared to 2019—demand was at 88% of pre-pandemic levels. The United Nations World Tourism Organization expects a full recovery of international tourism to pre-pandemic levels, and initial estimates suggest a 2% growth over 2019.³

The dramatic reversal from having essentially little to no international travel to a strong demand in travel, after much of the world was in varying degrees of lockdown for about a year and a half,⁴ has posed operational challenges for travel and tourism sectors alike, chief among them, airports and airlines.⁵ Airlines have struggled to meet travel demand, leading to a high number of flight delays and cancellations.⁶ The first five months of 2022

1. See Paul Sandle & Tim Hepher, *Pent-up Demand Prompts European Travel Recovery as COVID Curbs Ease*, REUTERS (May 6, 2022), <https://www.reuters.com/world/europe/europe-sees-travel-recovery-covid-restrictions-ease-2022-05-06/> (stating that the pandemic caused a complete shut down around the world as governments curbed entry into their nations).

2. See *International Tourism Back to 60% of Pre-Pandemic Levels in January-July 2022*, UNITED NATIONS WORLD TOURISM ORG. (Sep. 26, 2022), <https://www.unwto.org/news/international-tourism-back-to-60-of-pre-pandemic-levels-in-january-july-2022> [hereinafter UNWTO]; see also Sandle & Hepher, *supra* note 1 (noting that European hotel chains and airlines have seen bookings recover to levels not seen since the beginning of the pandemic); *International Tourism to Reach Pre-Pandemic Levels in 2024*, UN Tourism (Jan. 19, 2024) <https://www.unwto.org/news/international-tourism-to-reach-pre-pandemic-levels-in-2024>.

3. UNWTO, *supra* note 2.

4. See Derrick Bryson Taylor, *A Timeline of the Coronavirus Pandemic*, N.Y. TIMES (Mar. 17, 2021), <https://www.nytimes.com/article/coronavirus-timeline.html> (providing a timeline of several countries that implemented nationwide lockdowns, including Ecuador, Peru, India and Iran).

5. UNWTO, *supra* note 2.

6. See Ian Duncan & Lori Aratani, *Airlines Tried Shifting Blame, but They're the Biggest Cause of Delays*, WASH. POST (July 23, 2022), <https://www.washingtonpost.com/transportation/2022/07/23/airline-delays-summer-cancellations/> (indicating an increase in flight delays and cancellations as a result of surging demand).

had 88,161 canceled flights in the U.S.—this five-month period represented the second-highest period of cancellations since 1988; the first was in 2020 during the COVID-19 pandemic.⁷

Considering the high number of flight cancellations and delays, such as the December 2022 Southwest Airlines “holiday meltdown,” where 71% of Southwest flights were canceled,⁸ it is not surprising that travelers sought admission into voluntary U.S. Customs and Border Protection (CBP) Trusted Traveler Programs (TTP) like TSA PreCheck and Global Entry in record numbers to “bypass traditional CBP entry inspection lines and receive expedited processing when entering the United States.”⁹ CBP expects 3.5 million applications for the 2022 fiscal year, the most it has ever received in a single year.¹⁰ CBP continues to review applications submitted since 2020 due to CBP’s five-month closure during the COVID-19 pandemic.¹¹

CBP and the Transportation Security Administration (TSA) collect traveler biometric data at airports, land ports, and seaports to “facilitat[e] the lawful flow of people and goods while preventing the entry of unauthorized individuals... and contraband.”¹² Biometric data is a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition, including fingerprints, facial, voice, or iris patterns.¹³ Since 2018, CBP and TSA have collected this data for both U.S. and non-U.S. citizens through the Traveler Verification Service (TVS), regardless of whether a

7. *See id.*

8. *See id.*; see also Karen Brooks Harper, *Southwest Airlines’ Holiday Meltdown Brings on Federal Investigation*, TEX. TRIB. (Dec. 27, 2022, 4:00 PM), <https://www.texas-tribune.org/2022/12/27/texas-swa-southwest-airlines-cancellations-flights/> (remarking on the Southwest Airlines cancellation meltdown that saw 71% of its flights canceled, which was “two-thirds of the overall number of canceled flights from any carrier into and out of the U.S. that [December] day.”).

9. *CBP Surpasses 10 Million TTP Members*, U.S. CUSTOMS & BORDER PROT., <https://www.cbp.gov/newsroom/national-media-release/cbp-surpasses-10-million-ttp-members> (May 20, 2022).

10. *Id.*

11. *Id.*

12. *See* ABIGAIL F. KOLKER, CONG. RSCH. SERV., R46783, TRUSTED TRAVELER PROGRAMS 1 (May 5, 2021), <https://crsreports.congress.gov/product/pdf/R/R46783>.

13. *See, Biometrics*, U.S. DEP’T OF HOMELAND SEC. (May 5, 2023), <https://www.dhs.gov/biometrics>.

traveler is part of a voluntary TTP or not.¹⁴ More specifically, CBP collects a traveler's faceprint, which is a precise measurement of a person's unique facial geometry, with TVS facial recognition technology pilot programs when travelers enter and exit the U.S.¹⁵ In November 2020, the Department of Homeland Security (DHS) proposed to amend the regulations to eliminate references to pilot programs, thus expanding CBP and TSA's authority to use facial recognition technology to collect biometric data permanently.¹⁶ U.S. citizens have the option to opt out of this program.¹⁷

CBP's discourse around the use and collection of faceprints and facial recognition technology presents a misleading and incomplete view of the associated risks of facial recognition technology. In a 2018 demonstration by airport and federal officials on the use of biometric facial recognition technology to replace paper boarding passes on international flights, CBP Commissioner, Kevin McAleenan, said, "Everybody knows how to pose for a picture."¹⁸ However, as critics have pointed out, this rhetoric presents a false narrative about the implications of facial recognition technology and deprives governments and civil society from the necessary discussions to evaluate the advantages and disadvantages of this technology and data.¹⁹ The data privacy and security concerns around collecting and storing biometric faceprints are especially poignant considering the rapidly changing threat landscape of increasingly sophisticated

14. See generally U.S. DEPT OF HOMELAND SEC., DHS/CBP/PIA-056, PRIVACY IMPACT ASSESSMENT FOR TRAVELER VERIFICATION SERVICE 6 (2018) [hereinafter U.S. DEPT OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR TVS] ("When the traveler presents him or herself for entry, or for exit, the traveler will encounter a camera connected to CBP's cloud-based TVS facial matching service via a secure, encrypted connection.").

15. See Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States, 85 Fed. Reg. 74162, 74163 (proposed Nov. 19, 2020).

16. *Id.* at 74162.

17. *Id.*

18. Gregory Wallace, *Instead of the Boarding Pass, Bring Your Smile to the Airport*, CNN TRAVEL (Sept. 10, 2018, 2:38 PM), <https://www.cnn.com/travel/article/cbp-facial-recognition/index.html>.

19. See *id.* ("Privacy advocates, such as the American Civil Liberties Union, have highlighted concerns that the technology could be used for expansive law enforcement purposes and that it misidentifies people, especially some racial minorities and women.").

cyberattacks and cybercriminals²⁰ and the fact that CBP's information security practices have already been proven inadequate.²¹ There are also important data sharing concerns since there is little visibility as to which U.S. government party or even international government actor, has access to travelers' data.²² Lastly, facial recognition technology has a well-documented accuracy problem, especially for women and people of color.²³

This Comment will discuss what biometric data is, how it is collected and used during international travel, how the relevant

20. See *Cybersecurity Solutions for a Riskier World*, THOUGHTLAB, <https://thoughtlabgroup.com/cyber-solutions-riskier-world/> (last visited Jan. 18, 2024) ("Over the next two years, security executives expect an increase in attacks from social engineering and ransomware as nation-states and cybercriminals become more prolific. Executives anticipate that these attacks will target weak spots primarily caused by software misconfigurations (49%), human error (40%), poor maintenance (40%), and unknown assets (30%).").

21. See U.S. DEP'T OF HOMELAND SEC. OFF. INSPECTOR GEN., REVIEW CBP'S MAJOR CYBERSECURITY INCIDENT DURING 2019 BIOMETRIC PILOT 6 (Sept. 21, 2020), <https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf> (finding that CBP's IT security controls failed to prevent one of its subcontractors from obtaining access of unauthorized passenger information, putting traveler data at risk); see also Kate Sullivan & Geneva Sands, *Feds say photos of travelers compromised in data breach*, CNN POLITICS, <https://www.cnn.com/2019/06/10/politics/customs-and-border-protection-images-travelers-data-breach> (last updated June 10, 2019, 11:34 PM) (providing an example of a subcontractor having transferred copies of license plates images and traveler images collected by CBP to the subcontractor's company network and subsequently having the information compromised in a wide spread cyber-attack).

22. See Ellen M. Gilmer, *Airport Face Scans Embraced by Agencies Despite Nagging Mistrust*, BLOOMBERG GOV'T (Mar. 30, 2022, 5:01 AM), <https://about.bgov.com/news/airport-face-scans-embraced-by-agencies-despite-nagging-mistrust/> (remarking about concerns on the broad risks associated with government collection of personal data); see also Ashley Gorski, *CBP's Plan to Expand Face Surveillance at Airports is a Civil Liberties Disaster in the Making*, ACLU (Dec. 21, 2020), <https://www.aclu.org/news/immigrants-rights/cbps-plan-to-expand-face-surveillance-at-airports-is-a-civil-liberties-disaster-in-the-making> ("The faceprints will then be stored in a government database for up to 75 years, where they may be used not only by the Department of Homeland Security, but by foreign governments and federal, state, and local law enforcement to identify individuals for a variety of purposes.").

23. This comment will not discuss constitutional concerns (First Amendment, Fourth Amendment, or due process) related to facial recognition technology. Jack Laperruque, *Facial Recognition Surveillance in Congress's Crosshairs*, THE HILL (June 4, 2019), <https://thehill.com/opinion/technology/446726-facial-recognition-surveillance-in-congress-crosshairs/>.

government actors use such data, and the laws surrounding its collection, use, and storage. These various themes will be covered in four parts. First, this Comment will provide a general overview of biometric data, how the government has historically collected biometric data, and how it is currently used in aviation security. Second, the current law will be analyzed, along with any relevant regulation(s) and legislation. Third, the concerns related to the use of biometric data and facial recognition technology will be discussed. Lastly, the Comment will conclude with recommendations and ways to move forward.

II. BACKGROUND

A. *Biometric Technology*

As previously mentioned, biometric data is a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition.²⁴ Physical characteristics include fingerprints, DNA samples, iris scans, and 3D face scans.²⁵ Behavioral characteristics include a person's voice, handwriting, and typing rhythm.²⁶ Because biometric data uses unique, and often unchangeable characteristics, biometric data is reliable, convenient, and impossible to forge.²⁷ For much the same reason, it is especially important to safeguard biometric identifying information and ensure its security due to its highly sensitive nature and the fact that it is not typically feasible to change one's biometrics.²⁸ Improperly used biometric information can lead to grave consequences like someone stealing a person's identity to commit

24. U.S. DEP'T OF HOMELAND SEC., *Biometrics*, *supra* note 13.

25. Alexa N. Acquista, *Biometrics Takes Off – Fight Between Privacy and Aviation Security Wages On*, 85 J. AIR L. & COM. 475, 478 (2020).

26. See Hrithik Saini, *What is Biometrics and How Does it Work?*, ANALYTIC STEPS (Dec. 4, 2021), <https://www.analyticssteps.com/blogs/what-biometrics-and-how-does-it-work>.

27. See Acquista, *supra* note 25, at 479.

28. Carra Pope, Comment, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data*, 26 J. L. & POL'Y 769, 774 (2018).

identity fraud or false identifications leading to mistaken prosecutions, detentions, or imprisonments.²⁹

Biometric data and technology is widely used in different contexts by private and public actors, such as in law enforcement, commercial applications, migration control, healthcare, and more.³⁰ In everyday life, face authentication is used to unlock one's smartphone, smartwatches and fitness tracking devices collect users' pulse and activity throughout the day, and fingerprints are scanned to clock into work.³¹ Many government actors collect biometric data, such as the FBI, the Department of Justice, Homeland Security, Defense, and State.³² Specifically, the Department of Homeland Security (DHS) collects biometric data through its different agencies for a variety of reasons. For example, the Transportation Security Administration (TSA) and U.S. Customs and Border Protection (CBP) use biometric data to detect and prevent illegal entry of travelers into the U.S., grant and administer proper immigration benefits, facilitate travel and trade, and enforce federal laws.³³

Biometric technology can be used for verification or identification, but the enrollment process for both is the same.³⁴ The enrollment process to collect a person's biometric characteristic, such as a fingerprint, begins by collecting the biometric characteristic and then storing it in a database.³⁵ The biometric characteristic is linked to a person's identifier, such as a passport, driver's license, or other form of identification.³⁶ Verification means that a biometric characteristic is used to authenticate, or verify, that a person is who they say they are. To undergo the verification process, the scanned biometric is compared to the stored biometric to authenticate the person's identity.³⁷ This is known as a "one-to-one comparison" since the

29. U.S. DEP'T OF HOMELAND SEC., *Biometrics*, *supra* note 13; Laperruque, *supra* note 23.

30. U.S. DEP'T OF HOMELAND SEC., *Biometrics*, *supra* note 13.

31. *Id.*; see also Pope, *supra* note 28, at 781–82.

32. Pope, *supra* note 28, at 775.

33. U.S. DEP'T OF HOMELAND SEC., *Biometrics*, *supra* note 13.

34. Acquista, *supra* note 25, at 479.

35. Saini, *supra* note 26.

36. *Id.*; Acquista, *supra* note 25, at 479.

37. Saini, *supra* note 26.

comparison is between the scanned and the stored biometric.³⁸ Identification means that a biometric characteristic is used to identify or determine someone's identity.³⁹ Identification is a "one-to-many" comparison since the comparison is between the scanned biometric and multiple stored biometrics saved in a database to ensure a person's biometric is found in that particular database.⁴⁰ Identification and verification systems may be linked to different databases.⁴¹

B. Biometric Data Collection by the U.S. Government

The U.S. government collects biometric information in a myriad of ways—through its federal agencies and state, local, and tribal law enforcement.⁴² This data is sent to the Office of Biometric Identity Management (OBIM, formerly US-VISIT), which is maintained by DHS.⁴³ OBIM does not own the biometric data collected by DHS or any of DHS's mission partners.⁴⁴ OBIM's role is to manage and protect the data on behalf of its partners.⁴⁵ DHS claims that OBIM is "helping to make travel simple, easy, and convenient for legitimate visitors, but virtually impossible for those who wish to do harm or violate U.S. laws."⁴⁶

To meet its goal, OBIM uses the Automated Biometric Identification System (IDENT), which is the primary and largest biometric repository in the U.S. government and the second-largest repository in the world.⁴⁷ IDENT stores biometric,

38. Acquista, *supra* note 25, at 479.

39. U.S. DEP'T OF HOMELAND SEC., *Biometrics*, *supra* note 13.

40. Acquista, *supra* note 25, at 479.

41. *Id.* at 480.

42. Pope, *supra* note 28, at 775; *see also* U.S. DEP'T OF HOMELAND SEC., *Biometrics*, *supra* note 13.

43. U.S. DEP'T OF HOMELAND SEC., *Biometrics*, *supra* note 13.

44. *Office of Biometric Identity Management (OBIM)*, U.S. DEP'T OF HOMELAND SEC., (Dec. 1, 2022), <https://www.dhs.gov/obim> [hereinafter OBIM homepage].

45. *Id.*

46. *Office of Biometric Identity Management Identification Services*, U.S. DEP'T OF HOMELAND SEC. (Dec. 14, 2021), <https://www.dhs.gov/obim-biometric-identification-services>.

47. Elec. Frontier Found., Comments of the Electronic Frontier Foundation regarding Notice of Proposed Rulemaking on the Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, USCIS Docket No. USCIS-2019-2007, 85 Fed. Reg.

biographic, and encounter-related information⁴⁸ and supplies the technology for matching, storing, and sharing biometric data.⁴⁹ Additionally, its repository stores more than 260 million unique identities and processes more than 350,000 biometric transactions on a daily basis.⁵⁰ This data includes digital facial photographs, fingerprints, iris scans, palm prints, and latent fingerprints.⁵¹ Biographic data includes well-known identifying data like a person's name, gender, and date of birth, in addition to more specific identifiers such as their IDENT status, social security number, and citizenship.⁵² Encounter data includes any encounter the individual had with the government agency using IDENT and includes various details like the name of the organization, timestamp, and reason for fingerprinting the individual.⁵³ IDENT does not use public information or information from commercial sources.⁵⁴ IDENT users include federal, state, local, tribal, foreign, and international governmental agencies that have entered written information sharing access agreements with OBIM.⁵⁵ Each user has access to different data and not all users store biometric information.⁵⁶ IDENT users who contribute and store data on IDENT are known as data providers.⁵⁷ These providers determine who gets access to their data according to the user's DHS-approved need.⁵⁸ Further, each data provider restricts the maintenance, retention, and

56338, (Oct. 13, 2020), <https://www.eff.org/document/eff-comments-dhs-proposed-rule-collection-and-use-biometrics-october-2020>, at 6.

48. See U.S. DEPT OF HOMELAND SEC., DHS/NPPD/PIA-002, Privacy Impact Assessment for the Automated Biometric Identification System (IDENT) (2012) at 10 [hereinafter "IDENT"].

49. U.S. DEPT OF HOMELAND SEC., *Biometrics*, *supra* note 13; see generally U.S. DEPT OF HOMELAND SEC., *Office of Biometric Identity Management Identification Services*, *supra* note 46.

50. See U.S. DEPT OF HOMELAND SEC., *Biometrics*, *supra* note 13.

51. *Id.* at 11.

52. *Id.*

53. For example, entry, visa application, or credentialing application, or apprehension, etc. *Id.*

54. *Id.* at 15.

55. *Id.* at 3.

56. IDENT, *supra* note 48, at 3.

57. See *id.*

58. *Id.*

sharing of its data with other organizations.⁵⁹ If a user does not store biometric information on IDENT, then that user has “search only” access, meaning that they do not enroll or maintain their own data on the system.⁶⁰

After an individual’s biometrics are enrolled in IDENT, each subsequent enrollment is known as an encounter.⁶¹ Generally, with each encounter, IDENT cross-references a person’s biometrics against the associated identification document presented to ensure the person’s identity and “[a] watchlist of known or suspected terrorists, criminals, and immigration violators; . . . the entire database of fingerprints to . . . determine if a person is using an alias/and or attempting to use fraudulent identification. . . [and] the associated identification document presented” to ensure the person’s identity.⁶²

The National Archives and Records Administration (NARA) requires OBIM to maintain IDENT records in its custody for 75 years or until the data is no longer needed for legal or business purposes, whichever is later.⁶³ However, DHS is evaluating whether a new retention period should be adopted, but it is unclear from the IDENT Privacy Impact Assessment, published in 2012 whether such a change has been made.⁶⁴ It is important to note that international users like foreign governments are not subject to the 75-year retention period, and instead, are subject to their own data retention laws.⁶⁵

C. Biometric Tech in Aviation Security

1. CBP Trusted Traveler Programs

Trusted Traveler Programs (TTP) include the following: PreCheck, Global Entry, NEXUS, Secure Electronic Network for Travelers Rapid Inspection (SENTRI), and Free and Secure

59. *Id.* at 7.

60. *Id.*

61. *Id.* at 2.

62. IDENT, *supra* note 48, at 2.

63. *Id.* at 10.

64. *Id.*

65. *Id.* at 25.

Trade (FAST).⁶⁶ There are different eligibility requirements for these programs, but it is important to note that these are all voluntary programs.⁶⁷ These programs are available for eligible travelers to use via air, land, and sea ports of entry, depending on the TTP.⁶⁸ TSA PreCheck and Global Entry are the only programs used at airports, while NEXUS, SENTRI, and FAST provide expedited entry into the U.S. at land ports of entry.⁶⁹ These TTPs help CBP and TSA fulfill their goal of “facilitating the lawful flow of people and goods while preventing the entry of unauthorized individuals... and contraband.”⁷⁰ Although TTP guidelines vary from program to program, they all require that applicants provide personal and biometric data.⁷¹ Most of these programs require the collection of fingerprints and photographs.⁷²

TSA PreCheck is a “passenger prescreening initiative that identifies lower risk passengers” eligible for expedited security screening at participating U.S. airports.⁷³ The goal of PreCheck is to enhance aviation security by performing a prior security assessment on users and thus better allocate TSA resources on detecting travelers more likely to pose a security threat, as well as improve users’ travel experience.⁷⁴ PreCheck passengers go through a separate security screening, keep laptops and liquids inside carry-on bags, and do not remove their shoes, belts, or jackets during the screening.⁷⁵

PreCheck began in October 2011 and screens passengers for domestic and international flights.⁷⁶ From 2014 to 2020, 1.4

66. KOLKER, TRUSTED TRAVELER PROGRAMS, *supra* note 12, at 1.

67. *See generally id.* (explaining that the Trusted Traveler Programs are based on individuals who voluntarily apply for membership in the programs and therefore choose to subject themselves to the eligibility requirements).

68. *Id.* at 17, tbl. 7.

69. Because NEXUS, SENTRI, and FAST are strictly for land ports of entry, they will not form part of this comment’s analysis. *Id.*

70. *Id.* at 1.

71. *Id.* at 1; U.S. DEPT. OF HOMELAND SEC., DHS/TSA/PIA-041(A), PRIVACY IMPACT ASSESSMENT UPDATE FOR THE TSA PRE ✓ APPLICATION PROGRAM 6 (2016) [hereinafter “PreCheck Privacy Impact Assessment”]

72. *See* KOLKER, TRUSTED TRAVELER PROGRAMS, *supra* note 12, at 1–3, 5–6, 11.

73. PreCheck Privacy Impact Assessment, *supra* note 71, at 1.

74. *Id.*

75. KOLKER, TRUSTED TRAVELER PROGRAMS, *supra* note 12, at 2.

76. *Id.* at 1–2.

billion air travelers used PreCheck.⁷⁷ U.S. citizens, nationals, and lawful permanent residents of all ages can apply to TSA PreCheck.⁷⁸ Eligible individuals apply online but must enroll in-person by submitting biometric data in the form of fingerprints as well as documentation to verify their identity, like a passport or driver's license.⁷⁹ With this information, TSA performs a background check and evaluates an applicant's security threat using law enforcement, immigration, and intelligence databases.⁸⁰ Additionally, an applicant's fingerprints are enrolled in IDENT for recurrent immigration, law enforcement, and intelligence checks.⁸¹ Once TSA approves an application, the applicant can use TSA PreCheck ("PreCheck") and enjoy the expedited security lanes.⁸² TSA started using facial recognition technology in 2022 via pilot programs around the country to scan travelers' faces—first, exclusively for PreCheck users, but now for all travelers.⁸³

Global Entry is another TTP that provides expedited clearance upon international arrival into the U.S. by air to pre-approved travelers through self-service kiosks or e-gates using facial comparison technologies at more than 75 airports.⁸⁴ The program started as a pilot in 2008 and became permanent in 2012.⁸⁵ Member benefits include reduced wait times when going through CBP processing.⁸⁶ Additional benefits include no paperwork for passengers to fill out upon entry into the U.S. when returning to the U.S. from travel abroad and automatic

77. *Id.* at 3.

78. *Id.* at 2.

79. *Id.* at 2–3.

80. *Id.* at 3.

81. KOLKER, TRUSTED TRAVELER PROGRAMS, *supra* note 12, at 4.

82. *Id.* at 3.

83. Geoffrey A. Fowler, *TSA Now Wants to Scan Your Face at Security. Here are Your Rights.*, WASH. POST (Dec. 2, 2022), <https://www.washingtonpost.com/technology/2022/12/02/tsa-security-face-recognition/>.

84. PreCheck Privacy Impact Assessment, *supra* note 71, at 20; KOLKER, *supra* note 12, at 5.

85. KOLKER, *supra* note 12, at 5.

86. Global Entry Frequently Asked Questions, U.S. CUSTOMS & BORDER PROT. (Dec. 30, 2022), <https://www.cbp.gov/travel/trusted-traveler-programs/global-entry/frequently-asked-questions> [hereinafter "U.S. Customs and Border Protection, Global Entry FAQ"].

enrollment in PreCheck.⁸⁷ The following people are eligible to join the program: U.S. citizens and lawful permanent residents, along with citizens of Argentina, Brazil, Bahrain, India, Colombia, Germany, Mexico, the Netherlands, Panama, Singapore, South Korea, Switzerland, Taiwan, and the U.K..⁸⁸

The Global Entry enrollment interview process is similar to that of PreCheck where applicants provide fingerprints and facial images for identity verification and undergo a background check.⁸⁹ Applicants must not:

provide false...application information; have any previous criminal convictions, pending criminal charges, or outstanding warrants in any country; have any previous customs, immigration, or agriculture violations in any country; be the subject of an ongoing investigation by any law enforcement agency in any country; be inadmissible to the U.S.; have any known or suspected terrorist connections; or be unable to satisfy CBP that they are low-risk.⁹⁰

Also, like PreCheck, applicants' biometric data is stored in IDENT.⁹¹

Previously, Global Entry members verified their identity by swiping their passports and scanning their fingerprints in the Global Entry kiosk.⁹² The kiosk would take this data and cross-reference it with the previously collected data stored in IDENT.⁹³ The kiosk would also take a picture of the member and save it to IDENT, but this was not used to verify the traveler's identity.⁹⁴ However, because of CBP's Traveler Verification

87. KOLKER, TRUSTED TRAVELER PROGRAMS, *supra* note 12, at 5.

88. *Id.* at 6.

89. *Id.*

90. *Id.* at 9.

91. U.S. Dep't of Homeland Sec., Privacy Impact Assessment for GES, *infra* note 96, at 2-3.

92. *Id.* at 2-4.

93. *Id.*

94. *Id.*

Service (discussed *infra*), this process is slightly different now due to the use of facial recognition technology.⁹⁵ Members no longer scan their fingerprints nor their passports at the Global Entry kiosk.⁹⁶ A traveler's face is automatically recognized, and, like in the previous process, the image is still stored in IDENT.⁹⁷

2. Traveler Verification Service

In addition to TTPs, TSA and CBP have collected travelers' personal and biometric data since 2017 through the Traveler Verification Service (TVS) for international travelers entering and exiting the U.S.⁹⁸ TVS is a cloud-based facial recognition technology system used to verify a traveler's identity.⁹⁹ Before entry or exit, CBP collects a traveler's faceprint, a precise measurement of a person's unique facial geometry¹⁰⁰ through CBP, airline, airport authority, or cruise line-owned camera equipment.¹⁰¹ This means that TVS involves both public and private actors. Then, TVS compares the new photo with previous images in the DHS's ownership, such as passport photos, visas, or other travel documents; photos taken by CBP in the entry inspection; or photographs from previous DHS encounters.¹⁰²

In contrast to TTP programs, which are voluntary, only certain groups of people can opt out of TVS and request a manual document inspection by a CBP official.¹⁰³ These people include the following: U.S. citizens and certain exempt non-U.S. citizens,

95. See generally U.S. DEP'T OF HOMELAND SEC., Privacy Impact Assessment for TVS, *supra* note 14.

96. U.S. DEP'T OF HOMELAND SEC. PRIVACY IMPACT ASSESSMENT FOR THE GLOBAL ENROLLMENT SYSTEM (GES): GLOBAL ENTRY FACIAL RECOGNITION, DHS/CBP/PIA-002(e) 2 (2019) [hereinafter "U.S. Dep't of Homeland Sec., Privacy Impact Assessment for GES"].

97. *Id.*

98. U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR TVS, *supra* note 14, at 3; see also Acquista, *supra* note 25, at 483–84.

99. U.S. DEP'T OF HOMELAND SEC. OFF. INSPECTOR GEN., *supra* note 21, at 2.

100. Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States, 85 Fed. Reg. 74162, 74163 (proposed Nov. 19, 2020).

101. U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR TVS, *supra* note 14, at 6–8.

102. *Id.* at 8.

103. ABIGAIL F. KOLKER, CONG. RSCH. SERV., R47541, IMMIGRATION: THE U.S. ENTRY-EXIT SYSTEM AT 6–7 (2023).

including Canadian citizens, children under the age of 14, anyone over 79, foreign nationals admitted on certain visas, or certain Taiwan officials.¹⁰⁴ Non-U.S. citizens must go through TVS's facial recognition technology to enter and exit the U.S.¹⁰⁵ TVS is used in the entry processes at all international airports and in the exit processes at 36 airport locations.¹⁰⁶ Further, CBP uses facial biometrics at 36 seaports and all pedestrian lanes at the southwest and northern border ports of entry.¹⁰⁷ CBP runs this program in partnership with several airlines.¹⁰⁸

CBP secures traveler photos in four different ways—through secure encryption and authentication, biometric templates, brief retention periods, and secure storage.¹⁰⁹ First, regarding secure encryption and authentication, CBP IT systems conform to the security and privacy controls required by the National Institute of Standards and Technology (NIST) and the DHS Chief Information Officer.¹¹⁰ The data transfers between the camera taking the picture on their scan, TVS, and DHS systems use two-factor authentication and strong encryption.¹¹¹ The encryption keys for the cloud service provider that stores the data from TVS are stored on hardware hosted by the cloud service provider.¹¹² Second, regarding biometric templates, CBP creates these templates from photos collected for matching and storage purposes; biometric templates are “strings of multiple numbers

104. For the complete list of exempt non-U.S. citizens, see 8 CFR 235.1(f)(ii); see also 8 CFR 215.8(a)(1).

105. KOLKER, IMMIGRATION: THE U.S. ENTRY-EXIT SYSTEM, *supra* note 103, at 7.

106. *Where is it Deployed?*, U.S. CUSTOMS & BORDER PROT. (Feb. 5, 2024), <https://www.cbp.gov/travel/biometrics>.

107. *Id.*

108. Marcy Mason, *How CBP is Meeting its Mandate and Keeping America Safe*, U.S. CUSTOMS & BORDER PROT. (Sept. 28, 2002), <https://cbp.gov/frontline/cbp-biometric-testing>; Elaine Glusac, *Your Face Is, or Will Be, Your Boarding Pass*, N.Y. TIMES (Dec. 7, 2021), <https://www.nytimes.com/2021/12/07/travel/biometrics-airports-security.html>.

109. *CBP Simplified Travel Air Entry/Exit Tear Sheet*, U.S. CUSTOMS & BORDER PROT. (Dec. 1, 2023), <https://www.cbp.gov/document/fact-sheets/cbp-simplified-travel-air-entry-exit-tear-sheet>.

110. U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR TVS, *supra* note 14 at 15, n. 56, 27.

111. U.S. CUSTOMS & BORDER PROT., *supra* note 109.

112. U.S. CUSTOMS & BORDER PROT., *supra* note 109; U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR TVS, *supra* note 14 at 26.

representing images that can be matched against other templates that represent facial images.”¹¹³ This means that anyone outside of CBP could not reverse-engineer the templates and anyone outside the TVS system would not be able to recognize the photos.¹¹⁴ Third, regarding retention periods, CBP does not retain photos of U.S. citizens and “exempt aliens”¹¹⁵ for more than 12 hours after TVS identifies the traveler. Non-U.S. citizens’ photos outside of the “exempt aliens” group previously mentioned are deleted within 14 days from CBP systems but may be retained longer in IDENT as a biometrically-confirmed entry or exit.¹¹⁶ The deletion of data from CBP systems is documented.¹¹⁷ However, some argue that because biometric data is not regulated, there is little accountability for the government to destroy the data according to their timelines or at all.¹¹⁸ Fourth, regarding secure storage, photos are encrypted and biographic exit records photos for U.S. citizens and lawful permanent residents are stored for 15 years, while non-U.S. citizens’ data is stored for 75 years.¹¹⁹ Any CBP partner using TVS, such as airlines, airport authorities, and cruise lines, is restricted from using the photos for their business purpose.¹²⁰

113. U.S. CUSTOMS & BORDER PROT., *supra* note 109; U.S. DEP’T OF HOMELAND SEC., DHS/TSA/PIA-046(d), PRIVACY IMPACT ASSESSMENT FOR TRAVEL DOCUMENT CHECKER AUTOMATION USING FACIAL IDENTIFICATION 3 n.15 (2022).

114. U.S. DEP’T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR TVS, *supra* note 14, at 15 n. 3.

115. This is the same list of exempt non-U.S. citizens as previously mentioned, *supra* note 105; see 8 CFR § 235.1(f)(ii); see 8 CFR § 215.8(a).

116. U.S. DEP’T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR TVS, *supra* note 14, at 9, 20–21.

117. U.S. DEP’T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR TVS, *supra* note 14, at 26.

118. Pope, *supra* note 28, at 778.

119. U.S. DEP’T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR TVS, *supra* note 14, at 20–21.

120. U.S. CUSTOMS & BORDER PROT., *supra* note 109.

III. CURRENT LAWS

A. *Legal Authorization for Biometric Data Collection*

Historically, there have been numerous federal statutes requiring an integrated entry/exit system for non-U.S. citizens into the U.S.¹²¹ These statutes have been amended over time and different requirements have been added. Further, Congress has shifted responsibility over who should develop the entry/exit program, but currently, this responsibility falls to the Department of Homeland Security (DHS).¹²² The following discussion covers the most relevant statutory and executive authority.

Section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 is one of the earliest statutes where Congress required the Attorney General to develop an “automated entry and exit control system” for every border crossing that a non-citizen made into the U.S.¹²³ The Act required that the system match the non-U.S. citizen’s departure to their entry record and have online searching capabilities to identify any unlawful overstays.¹²⁴ Congress also required the Attorney General to provide yearly reports to Congress with specifics on the departure records.¹²⁵ Congress specified that border crossing

121. These include: (1) Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, § 110, div. C, 110 Stat. 3009–558; (2) Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), Pub. L. No. 106-215, § 2(a), 114 Stat. 337; (3) Visa Waiver Permanent Program Act of 2000, Pub. L. No. 106-396, § 205, 114 Stat. 1637, 1641; (4) Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, § 414, 115 Stat. 272, 353 [hereinafter USA PATRIOT Act]; (5) Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act), Pub. L. No. 107-173, § 302, 116 Stat. 543, 552; (6) Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. No. 108-458, § 7208, 118 Stat. 3638, 3817; (7) Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 711, 121 Stat. 266, 338; (8) Trade Facilitation and Trade Enforcement Act of 2015, Pub. L. No. 114-125, § 802, 130 Stat. 122, 199; (9) 6 U.S.C. § 211(c)(10).

122. Ron Nixon, *Facial Scans at U.S. Airports Violate Americans’ Privacy*, *Report Says*, N.Y. TIMES (Dec. 21, 2017), <https://www.nytimes.com/2017/12/21/us/politics/facial-scans-airports-security-privacy.html>.

123. Illegal Immigration Reform and Immigrant Responsibility Act of 1996 § 110.

124. *Id.*

125. *Id.* § 107.

identification cards should include a “biometric identifier (such as the fingerprint or handprint of [a non-U.S. citizen]) that is machine readable.”¹²⁶ Four years later, Congress echoed the requirement in 2000.¹²⁷

The September 11 attacks in 2001 brought a renewed urgency in devising an entry/exit system to protect U.S. citizens from terrorist attacks from foreign nationals, especially considering that State Department policy at the time prevented the consular officers from “properly scrutinizing” the visa applications of several of the foreign nationals that murdered about 3,000 Americans.¹²⁸ 9/11 marked a turning point in national security law due to the expansion of the federal government to advance national security; this federal government expansion requires further analysis outside of the breadth of this comment.

In the aftermath of 9/11, Congress outlined that the entry-exit system should focus on biometric technology.¹²⁹ Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)¹³⁰ to collect biometric exit data for all non-U.S. citizens required to provide biometric entry data.¹³¹ The IRTPA requires that the system have an interoperable component for databases maintained by DHS, the Department of State, and the Department of Justice, current and immediate access to information in federal law enforcement agencies and intelligence community databases, and requires the Secretary of Homeland Security to develop a plan to accelerate full implementation of an automated biometric entry and exit data system.

Nonetheless, officials struggled to implement a biometric exit system because the technology to collect the data was “slow to take hold.” Airports also struggled logistically because national and international flights often depart from the same terminal,

126. *Id.* § 104.

127. See 8 U.S.C. § 1365a (2023); see also Illegal Immigration Reform and Immigrant Responsibility Act of 1996 § 104(a); Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), Pub. L. No. 106-215, § 2(a), 114 Stat. 337, 338.

128. Exec. Order No. 13769, 82 Fed. Reg. 8977 §§ 1, 7 (Jan. 27, 2017).

129. USA PATRIOT Act, *supra* note 121, at § 414.

130. 8 U.S.C. § 1365b (2023).

131. *Id.*; *Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States*, 85 Fed. Reg. 74162, at 74163 (proposed Nov. 19, 2020).

leading to a lack of space for additional scanning equipment.¹³² In the 2016 Consolidated Appropriations Act, Congress required DHS to submit a comprehensive plan for implementing the system and created a funding mechanism starting in the 2017 fiscal year.¹³³ Congress allocated \$1 billion over one decade for DHS to meet its goal.¹³⁴

In 2017, President Trump issued two executive orders urging DHS to make a biometric entry/exit system a priority and expedite the creation of the system.¹³⁵ Specifically, in January 2017, President Trump emphasized the need to speed up the deployment of the biometric system to airports and limited the entry of refugees into the U.S.¹³⁶ President Trump suspended the entry of citizens from Iran, Iraq, Libya, Somalia, Sudan, Syria, and Yemen for 90 days due to these countries “presenting heightened concerns about terrorism and travel to the United States.”¹³⁷ The second executive order related to this matter was passed on March 6, 2017, and required that the Secretary of Homeland Security periodically report to the President on DHS’s progress.¹³⁸

Up to this point in time, DHS only had authorization to require *certain non-U.S. citizens* to provide biometrics when leaving under pilot programs at land ports and at up to 15 airports and seaports.¹³⁹ But, as previously mentioned in this Comment’s introduction, DHS proposed to amend the regulations in November 2020 to remove the references to pilot programs and expand their authority to allow collection of biometric data from aliens leaving from any airport, land port, seaport, or any other

132. Nixon, *supra* note 122.

133. Rebecca Gambler, *Actions Needed by DHS to Address Long-Standing Challenges in Planning for Biometric Exit System*, U.S. GOV’T ACCOUNTABILITY OFF. (Jan. 20, 2016), https://tracfed.syr.edu/tracker/dynadata/2016_02/674704.2.pdf.

134. U.S. CUSTOMS & BORDER PROT., BIOMETRIC ENTRY-EXIT H-1B AND L-1 FEES SPEND PLAN FISCAL YEAR 2023 REPORT TO CONGRESS 4 (2023).

135. See Exec. Order No. 13769, 82 Fed. Reg. 8977 § 7 (Jan. 27, 2017); see Exec. Order No. 13780, 82 Fed. Reg. 13209 § 8 (Mar. 9, 2017).

136. Exec. Order No. 13769, 82 Fed. Reg. 8977 §§ 5, 7 (Jan. 27, 2017).

137. Exec. Order No. 13780, 82 Fed. Reg. 13209 § 1 (Mar. 9, 2017).

138. *Id.* § 8.

139. 8 C.F.R. 215.8(a).

point of departure.¹⁴⁰ DHS also proposed to amend the regulations so that Customs and Border Protection (CBP) could use facial recognition technology for taking photographs on entry and exit to the U.S. for “verifying the identity of aliens [and making the process] more efficient, accurate, and secure.”¹⁴¹ The proposed regulations would include all non-U.S. citizens, including children;¹⁴² U.S. citizens may opt out of participating in this program.¹⁴³ This proposal’s goal is along the same thread as the previously mentioned executive order and congressional mandates—to address “the national security concerns arising from the threat of terrorism, the fraudulent use of legitimate travel documentation, aliens who overstay their authorized period of admission or present in the U.S. without having been admitted or paroled, and incorrect or incomplete biographic data for travelers.”¹⁴⁴

Critics point out that DHS’s use of facial recognition technology is not justified by congressional authority because Congress only granted DHS authority to develop an entry/exit system using biometric data, not to collect faceprints as part of the entry/exit system.¹⁴⁵ So, this latest proposal to amend the regulations seems to be outside of CBP’s scope and authority.¹⁴⁶ It is also important to note that IRTPA was passed in 2004, years before CBP began using facial recognition technology, so the passing of IRTPA does not mean that Congress approved CBP’s use of facial recognition technology.¹⁴⁷ Also, Congress has never

140. Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States, 85 Fed. Reg. 74162, 74163 (proposed Nov. 19, 2020).

141. *Id.* at 74162.

142. Gorski, *supra* note 22.

143. Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States, 85 Fed. Reg. 74162, 74177 (proposed Nov. 19, 2020).; Gilmer, *supra* note 22.

144. Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States, 85 Fed. Reg. 74162, 74163 (proposed Nov. 19, 2020).

145. See Gorski, *supra* note 22 (explaining that while Congress has authorized the collection of certain biometrics, it has not authorized the collection of faceprints and similar biometrics that can be collected covertly without consent and pose an unprecedented risk of persistent government surveillance).

146. *Id.*

147. See 8 U.S.C. § 1365b; see also *CBP Deploys Facial Recognition Biometric Technology at 1 TSA Checkpoint at JFK Airport*, U.S. CUSTOMS AND BORDER PROT. (Feb.

clearly ordered the collection of biometrics from U.S. citizens using face recognition technology.¹⁴⁸ Even if CBP follows its own procedures and deletes the data according to its published storage policies, CBP does not have authority to be scanning Americans' faces to start with if there is no clear, congressional authority granting it the authority to do so.

In fact, both Democrat and Republican members of Congress have raised concerns about the use of facial recognition technology,¹⁴⁹ and there have been recent congressional proposals to limit law enforcement's use of facial recognition surveillance.¹⁵⁰ The 2021 Facial Recognition and Biometric Technology Moratorium Act proposes "to prohibit biometric surveillance by the Federal Government without explicit statutory authorization" until an effective regulatory regime is passed.¹⁵¹ This Act argues that it is better to pause the use of facial recognition until there is congressional legislation limiting its use rather than continuing to collect data in the current environment; some civil society groups also take this position.¹⁵²

While many bills on facial recognition have been proposed, the House of Representatives introduced the Facial Recognition Act in 2022, a comprehensive bill that sought to regulate state and federal government use of facial recognition technology.¹⁵³ The Act includes important provisions to limit the government's use of facial recognition technology and explicitly prohibits the use of

03, 2017), <https://www.cbp.gov/newsroom/national-media-release/cbp-deploys-facial-recognition-biometric-technology-1-tsa-checkpoint>.

148. HARRISON RUDOLPH, LAURA M. MOY & ALVARO M. BEDOYA, NOT READY FOR TAKEOFF: FACE SCANS AT AIRPORT DEPARTURE GATES 2 (2017), https://www.airportface-scans.com/sites/default/files/Biometrics_Report__Not_Ready_For_Takeoff.pdf.

149. Frank Konkel, *Bipartisan Calls to Regulate Facial Recognition Tech Grow Louder*, NEXTGOV (July 14, 2021), <https://www.nextgov.com/cxo-briefing/2021/07/bipartisan-calls-regulate-facial-recognition-tech-grow-louder/183761/>.

150. Jake Laperruque, *The Facial Recognition Act: A Promising Path to Put Guardrails on a Dangerously Unregulated Surveillance Technology*, LAWFARE BLOG (Nov. 1, 2022), <https://www.lawfareblog.com/facial-recognition-act-promising-path-put-guardrails-dangerously-unregulated-surveillance-technology> [hereinafter Jake Laperruque, *The Facial Recognition Act*].

151. Facial Recognition and Biometric Technology Moratorium Act of 2021, S. 2052, 117th Cong. § 3(b).

152. Jake Laperruque, *The Facial Recognition Act*, *supra* note 150.

153. *Id.*; Facial Recognition Act of 2022, H.R. 9061, 117th Cong. (102c).

facial recognition to enforce the immigration laws of the U.S. or share facial recognition data with other agencies to enforce immigration laws.¹⁵⁴ The Act defines facial recognition as:

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.¹⁵⁵

This means that CBP's biometric entry/exit programs using facial recognition technology like Global Entry and the Traveler Verification Service would essentially be banned. However, it remains unclear whether any TSA program using facial recognition technology would fall under this broad immigration enforcement ban since TSA could argue that it falls under an exception to use the technology to investigate terrorist plots.¹⁵⁶ Another ambiguity, or perhaps an outright gap in the Act, is that there is no reference to government contractors or sub-contractors, whom are also involved in the use of facial recognition programs and should also fall under the definition of law enforcement agency.¹⁵⁷

Nonetheless, it is a bit shocking that the Act outright prohibits facial recognition in immigration enforcement contexts, considering that the previously examined law in this Comment granted the federal government broad authority to meet its purpose. Despite its introduction in the House, the bill did not

154. Facial Recognition Act of 2022, *supra* note 153, § 102.

155. *Id.* § 3(4) (emphasis added).

156. See generally Jake Laperruque, *The Facial Recognition Act*, *supra* note 150.

157. Facial Recognition Act of 2022 § 3(8) (defining law enforcement agency as "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.").

advance past the committee stage.¹⁵⁸ It was referred to the House Committee on the Judiciary and the Committee on Science, Space, and Technology, but did not get a committee vote.¹⁵⁹

B. Federal Data Privacy Laws

The U.S. has no federal data privacy law, which would likely include biometrics data in its terms, nor specific federal biometrics privacy laws. However, three federal laws provide some framework for understanding biometric data collection by the government:¹⁶⁰ the Privacy Act of 1974,¹⁶¹ the Freedom of Information Act of 1966,¹⁶² and the Implementing the Recommendations of the 9/11 Commission Act of 2007.¹⁶³

1. Privacy Act of 1974

In the aftermath of surveillance activities performed by President Nixon and J. Edgar Hoover in the early 1970s,¹⁶⁴ Congress passed the Privacy Act of 1974, which applies strictly to the public sector and any government contractor accomplishing an agency function.¹⁶⁵ The Act limits the collection, use, dissemination, and maintenance of personally identifiable information (PII) about individuals maintained in a system of records by federal agencies.¹⁶⁶ The Act defines a system of records

158. *H.R. 9061 – Facial Recognition Act of 2022*, CONGRESS.GOV (last visited July 28, 2024) <https://www.congress.gov/bill/117th-congress/house-bill/9061/all-actions> (describing the timeline of the Act and its referral to committee without progressing past that point).

159. *Id.*

160. Pope, *supra* note 28 at 770.

161. 5 U.S.C. § 552a; see U.S. Dep't of Just., *Privacy Act of 1974*, JUSTICE.GOV (last updated Oct. 4, 2022), <https://www.justice.gov/opcl/privacy-act-1974>.

162. 5 U.S.C. § 552; see *About the Freedom of Information Act*, U.S. DRUG ENF'T ADMIN., <https://www.dea.gov/foia> (last visited Mar. 1, 2024).

163. Implementing the Recommendations of the 9/11 Commission Act of 2007, 121 Stat. 266.

164. Privacy Policy Guidance Memorandum from Hugo Teufel III, Chief Priv. Officer, U.S. Dep't of Homeland Sec. (Dec. 29, 2008) (available at <https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf>).

165. Privacy Act of 1974, 5 U.S.C. § 552a(m)(1); 5 U.S.C. § 552(f)(1).

166. Privacy Act of 1974, Pub. L. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a).

as “a group of any records” under agency control and from which information is retrieved by a number of categories, including a person’s name or identifying number, symbol, or other identifying particulars assigned to the individual.¹⁶⁷

At its core, the Act follows the Fair Information Practice Principles (FIPP), a framework later embraced by DHS as the foundational principles for privacy policy and implementation governing the use of PII.¹⁶⁸ These principles are transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, and accountability and auditing.¹⁶⁹ The Act is the only law in the U.S. that can currently be used to regulate federal data privacy protection because biometric data is PII by definition. Thus, although the Act does not explicitly mention biometric data, it nonetheless regulates TSA, CBP, and overall DHS biometric data collection.¹⁷⁰

The Act places several requirements and limitations on an agency’s collection of PII. For example, the Act requires agencies to save only the relevant and necessary information about an individual to accomplish the agency’s purpose as required by statute or executive order.¹⁷¹ An agency must provide public notice in the Federal Register for each database of PII it maintains; this requirement includes a description of the character, categories, and uses of the information collected.¹⁷² An agency must also give public notice in the Federal Register 30 days before any new use or intended use of the information in the system and must include specific information regarding the change, as well as grant the public an opportunity to voice their opinion and submit written comments.¹⁷³ An agency must also establish rules of conduct for persons involved in the design,

167. 5 U.S.C. § 552a(a)(5).

168. Teufel, *supra* note 164.

169. *Id.*

170. Michael Monajemi, *Privacy Regulation in the Age of Biometrics That Deal with a New World Order of Information*, 25 U. MIA INT’L & COMP. L. REV. 371, 382, 395, 397 (2018).

171. 5 U.S.C. § 552a(e).

172. 5 U.S.C. § 552(e)(4).

173. 5 U.S.C. § 552(e)(11).

development, operation, or maintenance of any system of records and establish controls to ensure that the data is secure, confidential, and otherwise protected against any anticipated threat.¹⁷⁴ Generally, the Act does not allow an agency to disclose any record by any means of communication to any person or other agency, unless the disclosure is routine use.¹⁷⁵ Lastly, the Act penalizes anyone for improper disclosure and provides civil remedies and civil lawsuits against the government.¹⁷⁶

The Act provides little guidance for how private entities, such as technology vendors or airlines, are restricted or limited in handling user data. While the Act references government contractors and states the following,

when an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system,¹⁷⁷

the Act does not say anything else about government contractors. Most importantly, the Act does not define government contractors, so it is unclear whether technology vendors or airlines using or servicing CBP biometric systems fall into the “government contractors” category. DHS might have private agreements with such private actors dictating how they can use the data, but without published regulations on the matter or transparency as to what the agreements say, it is hard to not be skeptical about how private entities might use this information.¹⁷⁸

174. *Id.*

175. *Id.*

176. Teufel, *supra* note 164; 5 U.S.C. § 552a(g)(1)(D).

177. 5 U.S.C. § 552a(m)(1).

178. RUDOLPH ET AL., *supra* note 148, at 15.

2. Freedom of Information Act of 1966 (FOIA)

Under FOIA, any U.S. government agency is required to fully or partially disclose previously unreleased or uncirculated information and documents controlled by the U.S. government, state, or other public authority upon request.¹⁷⁹ A person can also file complaints against an agency.¹⁸⁰ The Act intends to “encourage accountability through transparency” to ensure an open government.¹⁸¹

3. DHS Chief Privacy Officer and Other Privacy Requirements

It is useful to consider privacy laws other than the ones already mentioned, as they provide a framework for understanding the authorities and responsibilities of the DHS Privacy Office and Chief Privacy Officer (CPO).¹⁸² The Homeland Security Act of 2002 created the Privacy Office and CPO role. The CPO leads the Privacy Office to uphold privacy and transparency throughout DHS, as well as leading FOIA policy as the Chief FOIA Officer.¹⁸³ The Privacy Office enables DHS to “accomplish its mission while embedding and enforcing privacy protections and transparency in all DHS activities” and follows the DHS FIPP policies to identify and mitigate privacy risks.¹⁸⁴ The E-Government Act of 2002 mandates privacy impact assessments for all federal agencies when there are new collections or technologies of PII.¹⁸⁵ Privacy impact assessments are thorough

179. Isabella Getgey, *AIIA FOIA Series: Source of Funds Review at I-829 stage*, AM. IMMIGRANT INV. ALL. (Feb. 18, 2023), <https://goaiia.org/aiia-foia-source-of-funds-review-829-stage/>.

180. Mark Skerry, Note, *Protect America by Being Unique: How Changes in Biometric Data Collection Procedures Can Improve U.S.-VISIT*, CASE W. RESERVE J.L. TECH. & INTERNET, Spring 2011, at 71, 89–90.

181. Memorandum on the Freedom of Information Act, 2009 Daily Comp. Pres. Doc. (Jan. 21, 2009), <https://www.govinfo.gov/content/pkg/DCPD-200900009/pdf/DCPD-200900009.pdf>.

182. Skerry, *supra* note 180, at 89–90.

183. *Privacy Office*, U.S. DEPT OF HOMELAND SEC. (Aug. 9, 2023), <https://www.dhs.gov/privacy-office>.

184. *Id.*

185. E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899.

documents that describe the data being collected, how the information will be shared and used, why the data is collected, and where it is collected from.

IV. RISKS AND RECOMMENDATIONS

A. *Risks*

1. Data Security Concerns

In considering U.S. Customs Border and Protection (CBP) imposed security measures on traveler information, it is important to note that there have already been data breaches of CBP-collected traveler images.¹⁸⁶ One of these breaches occurred in May 2019 and compromised 184,000 traveler images; 19 images were posted to the dark web.¹⁸⁷ The breach occurred when a CBP subcontractor for a CBP pilot program implemented at land border crossings got access to traveler photos between August 2018 and January 2019 without CBP's authorization or knowledge.¹⁸⁸ The subcontractor downloaded the biometric data to an unencrypted hard drive, transferred copies to its own unencrypted company network in violation of the Department of Homeland Security (DHS) security and privacy protocols, and later suffered a malicious cyber-attack.¹⁸⁹ This incident begs the question of just how effective and secure CBP's system and procedures are and how little control CBP has over users with access to their biometric data.

There seems to be a disconnect between CBP security policies in writing versus in practice. In writing, CBP's policies to secure traveler photos via secure encryption and authentication, biometric templates, brief retention periods, and secure storage seem like good processes. However, in practice, there is something clearly wrong if a subcontractor can download traveler photos with an unencrypted hard drive and upload them to its own

186. See Pope, *supra* note 28, at 770 (discussing a 2015 data breach that exposed 5.6 million federal employees' fingerprints were stolen from the Office of Personnel Management).

187. *Id.*

188. U.S. DEP'T OF HOMELAND SEC. OFF. INSPECTOR GEN., *supra* note 21.

189. *Id.*

unencrypted network. A system that allows for such easy manipulation and oversight by one of its subcontractors is not suitable for collecting millions of travelers' data.

Trusted Traveler Programs (TTPs) and Traveler Verification Services (TVS) were created with similar aims of enhancing national security, while increasing the flow of travelers entering and exiting the U.S. in a quick and efficient manner.¹⁹⁰ But, if those are the goals, then how does the use of facial recognition technology help CBP, the Transportation Security Administration (TSA), and DHS do this? How is efficiency and safety measured here? Without answers to these questions, it is hard to justify new applications for something that CBP had successfully done in another, safer way.¹⁹¹

2. Accuracy and Civil Rights Concerns

The use of facial recognition technology presents accuracy and civil rights concerns.¹⁹² Poor datasets give facial recognition systems a "coded gaze," especially when scanning women, people of color, the young or elderly, and transgender people.¹⁹³ A 2019 study by the National Institute of Standards and Technology (NIST) found that Black and Asian people were up to 100 times more likely to be misidentified than white men, depending on the algorithm and other factors.¹⁹⁴ The accuracy of the technology has likely increased from the 2019 study, but accuracy issues remain.¹⁹⁵

190. KOLKER, TRUSTED TRAVELER PROGRAMS, *supra* note 12, at 1; Gilmer, *supra* note 22.

191. Gilmer, *supra* note 22.

192. See, e.g., Laperruque, *supra* note 23; Gorski, *supra* note 22; RUDOLPH ET. AL., *supra* note 148.

193. Laperruque, *supra* note 23; Gorski, *supra* note 22; Morgan Klaus Scheuerman et al., *How Computers See Gender: An Evaluation of Gender Classification in Commercial Facial Analysis and Image Labeling Services*, 3 ACM ON HUM.-COMPUT. INTERACTION 144:1, 144:1, 144:19 (2019).

194. NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software, NAT'L INST. OF STANDARDS AND TECH. (Dec. 19, 2019), <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software>.

195. See, e.g., Konkel, *supra* note 149 (noting that the accuracy of facial recognition technology has increase in recent years from the 2021 date of publication); William Crumpler, *How Accurate are Facial Recognition Systems – and Why Does It Matter?*, CSIS

In an immigration context at airports, this could result in face-matching errors that lead to interrogations, missed flights, and wrongful deportations,¹⁹⁶ which would all disproportionately affect travelers who are not white men.¹⁹⁷ Also, taking into account CBP's and TSA's record of separating families, detaining people in deplorable conditions, using lethal force, and profiling travelers racially and religiously, it is not hard to imagine situations where CBP or TSA subjects travelers to similar or worse treatment due to inaccurate identifications.¹⁹⁸

3. Lack of transparency and understanding

Although CBP and TSA have a lot of public information on TTPs and TVS, the collection of biometric data, the use of facial recognition technology, and the storage of traveler data, this information is not transparent nor easy for the U.S. public to understand. The current approach seems to be more about dumping information rather than about providing travelers transparency and comprehension about how data is collected, used, and stored. Much of the difficulty in understanding the information stems from several facts: (1) the large amount of information available; (2) the ambiguity around whether a publication is current or not; (3) the way that the information is

STRATEGIC TECH. BLOG (Apr. 14, 2020), <https://www.csis.org/blogs/strategic-technologies-blog/how-accurate-are-facial-recognition-systems-and-why-does-it> (describing the dramatic improvements of facial recognition technology in just a few years); Larry Anderson, et al., *What Are the New Developments in Facial Recognition?*, SEC. NEWS (Sep. 20, 2021), <https://www.securityinformed.com/insights/developments-facial-recognition-co-823-ga-co-1508-ga-co-11020-ga-co-1554360262-ga-co-1554987129-ga-off.1632136286.html> (explaining that technological improvements and attention to the issue of racial bias has improved the accuracy of facial recognition software in recent years).

196. Gorski, *supra* note 22.

197. See e.g., Kade Crockford, *How is Face Recognition Surveillance Technology Racist?*, ACLU NEWS & COMMENTARY (June 16, 2020), <https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist> (discussing the technology's bias against many gender and racial groups other than white men); Nandita Rao Narla, *TSA's Plans to Expand Facial Recognition at Airports: A Privacy Perspective*, ISACA NOW BLOG (June 15, 2023), <https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/tsas-plans-to-expand-facial-recognition-at-airports> (discussing the concerns of expanding facial recognition software at airports due to its racial bias against most racial groups that are not white men).

198. Gorski, *supra* note 22.

presented, especially considering the technical knowledge necessary to understand much of this information; (4) and the lack of a clear explanation for how TTPs, TVS, any other related pilot program, or IDENT interplay with each other. Perhaps not even DHS, CBP, or TSA has better information available internally, considering that a Government Accountability Office audit found that more than a dozen federal agencies did not know “the full scope of their facial recognition efforts and lacked effective means to track the technology’s use.”¹⁹⁹

B. Proposal

1. Institute a moratorium and amend the Facial Recognition Act

A first step in the right direction would be to pass the Moratorium Act of 2021 to stop the current biometric surveillance that has no explicit statutory authorization until Congress passes legislation governing its use. Another important step would be to make important additions to the proposed Facial Recognition Act to clarify some of its gaps. For example, the Facial Recognition Act could define government contractors and subcontractors and subject them to the same requirements as law enforcement agencies. This would prevent law enforcement agencies from using government contractors and subcontractors to evade requirements under the Act and make government and subcontractors liable for any violation of the Act. Also, considering that DHS will probably fight the ban of facial recognition for immigration enforcement, Congress could work with CBP or require CBP to present to Congress the viability of using other, less intrusive biometrics like fingerprints as part of an entry/exit system.²⁰⁰

2. Cybersecurity

At a minimum, CBP and the Transportation Security Administration (TSA), along with government contractors and

199. Konkel, *supra* note 149.

200. Jake Laperruque, *The Facial Recognition Act*, *supra* note 152.

subcontractors, should have state-of-the-art security systems to adequately protect traveler data and strong, ongoing compliance mechanisms to evaluate and audit its processes. Neither the Automated Biometric Identification System (IDENT) nor the Traveler Verification Service (TVS) Privacy Impact Assessments detail ongoing work that DHS or CBP undergo to ensure the adequate protection of users' data. This lack of transparency and accountability decreases public trust that the government is adequately handling data. The risk of not having an ongoing process, or worse, of having outdated technology to protect IDENT from cyberattacks, is too big of a risk to gamble with. The compliance process should also audit who has access to what information in order to limit unauthorized users and information sharing. Without any frequent audit mechanism, there is a risk of previously authorized users continuing to have access in perpetuity.

3. Improve transparency

Congress should also consider imposing requirements on the DHS Privacy Office to increase the public's trust by providing better information that actually provides valuable transparency for how all of its biometric entry/exit programs work, and update information published online. This could be done through a congressional amendment to the E-Government Act of 2002. The information overhaul should be in addition to the current information requirements and should be done with a view to educate users. There should also be a frequent auditing mechanism to make sure that information online remains accurate. This might seem onerous, but this is part of living in today's online world and should be a standard baseline if the government is collecting travelers' personally identifiable information. This information would serve as a middle point between dense, long privacy impact assessments and simplistic CBP messaging that mischaracterizes the use of facial recognition technology as merely 'smiling for the camera.'²⁰¹ It would also be helpful to provide a data flow diagram to identify any party involved in the biometric data collection, what data they are

201. Wallace, *supra* note 18.

collecting, where it is stored, and who has access to it. There is a way to be transparent without being paternalistic.

4. Create a realistic, timely opt-out alternative

The current default of having users opt out of facial recognition technology for Global Entry, TVS, and TSA PreCheck in certain airports should also be modified. It is not realistic to launch programs and say that they are “opt out” when the first time that you hear about the program or the opt out provision is when you are standing in line waiting to board your flight or enter the country. Albert Fox Cahn, the founder of the Surveillance Technology Oversight Project, says that “[t]here is no place more coercive to ask people for their consent than an airport.”²⁰² No one wants to endure an extra pat-down or miss their flight.

A better alternative would be to inform a user about the program and what it does *before* the traveler is at the airport—this could be done as a notice when someone buys their airline ticket. At that point, a traveler could decide to opt-into using facial recognition technology (if such use continues) rather than the current opt-out default.

V. CONCLUSION

Although facial recognition technology and biometric data collection at international airports may improve certain individuals’ travel experiences, the current risks outweigh the benefits. This Comment found that Customs and Border Protection (CBP) and Transportation Security Administration (TSA) do not have clear congressional authority to use facial recognition technology nor to collect travelers’ faceprints. CBP and TSA have not justified to Congress their need for facial recognition technology, nor have they proved that facial recognition is accurate enough to be relied upon. Further, TSA and CBP’s security practices related to the collection and storage of travelers’ biometric data are lacking and simply confusing to understand. Finally, the Comment recommended options that Congress and the Department of Homeland Security might take

202. Fowler, *supra* note 83.

to provide greater transparency to travelers, increase the U.S. public's trust, and better protect travelers' rights. It remains to be seen whether Congress will continue challenging CBP and TSA's use of facial recognition technology and how these programs will change, if at all, to meet congressional requirements.