

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, NW
Suite 200
Washington, DC 20009,

Plaintiff,

v.

U.S. CUSTOMS AND BORDER PROTECTION
1300 Pennsylvania Ave. NW
Washington, DC 20229,

Defendant.

Civ. Action No. 1:17-cv-1438

COMPLAINT FOR INJUNCTIVE RELIEF

1. This is an action under the Freedom of Information Act (“FOIA”), 5 U.S.C. § 552, for injunctive and other appropriate relief, seeking the release of agency records requested by the Plaintiff Electronic Privacy Information Center (“EPIC”) from Defendant Customs and Border Protection (“CBP”), a component of the U.S. Department of Homeland Security (“DHS”).

2. EPIC challenges CBP’s failure to make a timely response to EPIC’s Freedom of Information Act requests (“EPIC’s FOIA Requests”) for records about the 1:1 Facial Recognition Air Entry Pilot program and 1:1 Facial Comparison Project (“EPIC’s Biometric Air Entry FOIA Request”), CBP’s Biometric Exit program (“EPIC’s Biometric Exit FOIA Request”), and CBP’s use of iris recognition (“EPIC’s Iris Recognition FOIA Request”).

Jurisdiction and Venue

3. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 and 5 U.S.C. §§ 552, (a)(6)(E)(iii), (a)(4)(B). This Court has personal jurisdiction over Defendant CBP.

4. Venue is proper in this district under 5 U.S.C. § 552(a)(4)(B).

Parties

5. Plaintiff EPIC is a nonprofit organization, incorporated in Washington, DC, established in 1994 to focus public attention on emerging privacy and civil liberties issues. Central to EPIC's mission is oversight and analysis of government activities. EPIC's Advisory Board includes distinguished experts in law, technology, public policy, and cybersecurity. EPIC routinely disseminates information to the public through the EPIC website, the EPIC Alert, and various other news organizations. EPIC is a representative of the news media. *EPIC v. Dep't of Def.*, 241 F. Supp. 2d 5, 15 (D.D.C. 2003).

6. Defendant CBP is a component of the DHS, which is a federal agency within the meaning of 5 U.S.C. § 552(f)(1), and is headquartered in Washington, D.C.

FACTS

7. The CBP is currently in the process of implementing a Comprehensive Biometric Entry/Exit Plan.¹

8. The biometric entry/exit plan includes several initiatives to test the use of biometrics at entry/exit points within the U.S.

¹ Dep't of Homeland Sec., *Comprehensive Biometric Entry/Exit Plan: Fiscal Year 2016 Report to Congress* (2016), <https://www.dhs.gov/sites/default/files/publications/Customs%20and%20Border%20Protection%20-%20Comprehensive%20Biometric%20Entry%20and%20Exit%20Plan.pdf>.

9. CBP's exit initiatives include the testing of facial recognition for the following biometric exit programs: the Departure Information Systems Test ("DIST"), the Departure Verification System ("DVS"), the Traveler Verification Services ("TVS"), and the JetBlue self-boarding program.

10. CBP is also testing the use of facial recognition upon entry into the U.S. including for the 1:1 Facial Recognition Air Entry Pilot, which became the 1-to-1 Facial Comparison Project.

11. In addition to facial recognition, CBP has also stated that the agency is testing iris imaging capabilities for use in the agency's biometric entry/exit programs.

12. The *FY 2016 Consolidated Appropriations Act* provides up to a \$1 billion for the CBP biometric entry/exit program.

13. President Trump's Executive Order "Protecting the Nation From Foreign Terrorist Entry into the United States" explicitly calls on CBP to "expedite the completion and implementation of a biometric entry exit tracking system."²

14. Facial recognition and iris recognition pose significant threats to privacy and civil liberties.

15. Facial recognition, in particular, can be done covertly, remotely, and on a mass scale.

16. Participating in society involves exposing one's face, and there are few if any precautions that can be taken to prevent the collection of one's facial image.

17. There are a lack of well-defined federal regulations controlling the collection, use, dissemination, and retention of biometric identifiers.

² Exec. Order No. 13,780 § 8, 82 Fed. Reg. 13,209, 13,216 (Mar. 9, 2017).

18. Ubiquitous and near-effortless identification eliminates individual's ability to control their identities and poses a specific risk to the First Amendment rights of free association and free expression.

CBP's 1:1 Facial Recognition Air Entry Pilot Program

19. CBP has begun deploying facial recognition technology to be used by CBP officers at airport entry screening points used by U.S. citizens and first-time travelers from 38 countries subject to the Visa Waiver Program ("VWP").

20. On May 11, 2015, DHS released a Privacy Impact Assessment entitled "Privacy Impact Assessment for the U.S. Customs and Border Protection 1:1 Facial Recognition Air Entry Pilot"³ ("Initial Air Entry PIA").

21. According to the Initial Air Entry PIA, CBP will "determine the viability of facial recognition as a technology" and "determine if facial recognition technology can be incorporated into current CBP entry processing."⁴

22. In March 2015, CBP began a sixty-day field test of facial recognition technology of U.S. passport holders at ports of entry in the United States, including airports.⁵

23. Since March 2015, the CBP has deployed equipment to take photos of individuals at ports of entry and used facial recognition technology to compare the photo stored on the

³ U.S. Customs and Border Protection, *1:1 Facial Recognition Air Entry Pilot Privacy Impact Assessment 1* (Mar. 11, 2015), [hereinafter Pilot PIA], https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp-1-to-1-facial-recognition-air-entry-pilot-march-11-2015.pdf.

⁴ *Id.*

⁵ *Id.*

embedded computer chip in U.S. passports.⁶ According to DHS' assessment, the facial recognition software generates a "match confidence score" based on the photo comparison.⁷

24. The pilot was conducted over a nineteen-month period, which included two months of field testing at Washington Dulles International Airport from March 2015 to May 2015.⁸

25. In the Initial Air Entry PIA, the agency stated that it would prepare a report summarizing the findings of the pilot.⁹

26. In January 2016, CBP expanded the program (now renamed the "1-to-1 Facial Comparison Project") to all U.S. airports and expanded the scope to cover first-time travelers from VWP countries.¹⁰

27. In the 1:1 Facial Comparison Project Privacy Impact Assessment Update PIA ("Air Entry PIA Update I"), CBP relied on the findings of a "report that included analysis of the impact to arrival processing operations, comparison of the performance of multiple facial comparison algorithms, and an assessment of appropriate scoring thresholds."¹¹

28. Individuals, including U.S. citizens, do not enroll on the CBP facial recognition program.

⁶ *Id.* at 3.

⁷ *Id.* at 3.

⁸ U.S. Customs and Border Protection, *1:1 Facial Comparison Project Privacy Impact Assessment Update 3* (Jan. 14, 2016) [hereinafter Expansion PIA], <https://www.dhs.gov/sites/default/files/publications/DHS-CBP-PIA%20%E2%80%93%20025a%201-1%20Facial%20Comparison%20Project.pdf>.

⁹ Pilot PIA at 3, 4.

¹⁰ Expansion PIA.

¹¹ Expansion PIA at 3, 4.

29. Individuals, including U.S. citizen, do not have the option to opt-out of the facial recognition comparison process.¹²

30. According to the Air Entry PIA Update I, CBP will “retain facial images and comparison match score data from those travelers who are subject to an adverse or law enforcement action resulting from secondary inspection.”¹³

31. In October 2016, another PIA update was released for the 1-to-1 Facial Comparison Project.¹⁴ (“Air Entry PIA Update II”)

32. The Air Entry PIA Update II expanded the retention of facial images to include those “images with scores that fall in the mandatory referral range” as well as “all facial images taken during secondary inspection.”¹⁵

CBP’s Biometric Exit Program

33. In April 2016, DHS announced the agency’s intention “to redouble its efforts to achieve a biometric entry/exit system, and to begin implementing biometric exit, starting at the highest volume airports, in 2018.”¹⁶

34. From June 2016 through November 2016, CBP ran a pilot facial recognition program at Hartsfield-Jackson Atlanta International Airport, called the Departure Information Systems Test (“DIST”).¹⁷

¹² *Id.* at 2.

¹³ *Id.* at 5.

¹⁴ U.S. Customs and Border Protection, *Privacy Impact Assessment Update for the 1-to-1 Facial Comparison Project* (Oct. 18, 2016), <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-1to1facialcomparisonproject-october2016.pdf>.

¹⁵ U.S. Customs and Border Protection, *Privacy Impact Assessment Update for the 1-to-1 Facial Comparison Project 3* (Oct. 18, 2016).

¹⁶ Dep’t of Homeland Sec., *Comprehensive Biometric Entry/Exit Plan: Fiscal Year 2016 Report to Congress* (2016), <https://www.dhs.gov/sites/default/files/publications/Customs%20and%20Border%20Protection%20-%20Comprehensive%20Biometric%20Entry%20and%20Exit%20Plan.pdf>.

35. DIST required passengers on the route from Atlanta to Tokyo to submit themselves to facial recognition in order to board their departing flight.¹⁸

36. According to DIST's Privacy Impact Assessment ("DIST PIA"), the purpose of the pilot was to test the accuracy of CBP's facial recognition technology.¹⁹

37. According to CBP, facial images of U.S. citizens were retained for up to two weeks to confirm a traveler's identity, while other images are to be deleted by September 30, 2017, unless the image is associated with an open law enforcement matter.²⁰

38. A PIA for the Departure Verification System ("DVS PIA"), the next iteration of CBP's biometric exit facial recognition program, stated that DIST's matching program was able to identify travelers "with a high degree of confidence."²¹

39. The CBP also stated that the agency's "initial findings support the piloted process as a viable solution to fulfill the mandated biometric exit requirements in certain settings."²²

40. No report explaining these initial findings has been released to the public.

41. According to the DVS PIA, CBP would create exit records for passengers and retain them in CBP's Advance Passenger Information System ("APIS").²³

42. The facial recognition technology would use passenger flight manifests to compile a gallery of photos from the Automated Biometric Identification System ("IDENT"), the

¹⁷ Dep't of Homeland Sec., DHS/CBP/PIA-030(a), *Privacy Impact Assessment for the Departure Information Systems Test* (June 13, 2016), <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-dis%20test-june2016.pdf>.

¹⁸ *Id.* at 1.

¹⁹ *Id.* at 6.

²⁰ *Id.* 5-6.

²¹ Dep't of Homeland Sec., DHS/CBP/PIA-030(a), *Departure Verification System: Privacy Impact Assessment Update 2* (Dec. 16, 2016), <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-030-a-dvs-december2016.pdf>.

²² *Id.* at 2.

²³ *Id.* at 3.

Department of State's Consolidated Consular Database, and U.S. Citizen and Immigration Service's Computer Linked Adjudication Information Management System ("CLAIM 3") into flight-specific galleries in the Automated Targeting System ("ATS").²⁴

43. CBP officers would take a photo of the passenger and match it to a photo in the compiled gallery.²⁵

44. Photos of U.S. citizens could be retained until their identities were confirmed, and the photos of non-U.S. citizens could be retained for up to fifteen years in the DVS system in ATS.²⁶

45. Passengers were not allowed to opt-out of DIST or DVS.²⁷

46. On May 15, 2017, CBP released the Traveler Verification Service PIA Update ("TVS PIA Update"). The Traveler Verification Service ("TVS") is an iteration of the agency's biometric exist system that uses a cloud environment for facial recognition.²⁸

47. The TVS PIA Update stated that "a report identifying how each algorithm performed" would be produced.²⁹

48. DHS Deputy Executive Assistant Commissioner, John Wagner, has stated that TVS will be expanded to eight airports during the summer of 2017.³⁰

²⁴ *Id.* at 2-3.

²⁵ *Id.* at 3.

²⁶ *Id.* at 7.

²⁷ *Id.* at 6.

²⁸ Dep't of Homeland Sec., DHS/CBP/PIA-030(b), *Traveler Verification Service: Privacy Impact Assessment Update* (May 15, 2017), <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-may2017.pdf>.

²⁹ *Id.* at 11-12.

³⁰ *Visa Overstays: A Gap in the Nation's Border Security: Hearing Before the Subcomm. on Border & Mar. Sec. of the H. Comm. on Homeland Sec.*, 115th Cong. (2017) (statement of John Wagner, Deputy Exec. Assistant Comm'r, Office of Field Operations, Customs & Border Prot.), available at <https://www.dhs.gov/news/2017/05/23/written-testimony-plcy-cbp-and-ice-house-homeland-security-subcommittee-border-and>.

49. On May 31, 2017, JetBlue announced that it would collaborate with CBP to test a new self-boarding process that used CBP's facial recognition technology to verify the identity of JetBlue customers on flights between Boston's Logan International airport and Aruba's Queen Beatrix International airport.³¹

50. The JetBlue self-boarding program will utilize CBP's database of passport, visa, and immigration photographs and is part of CBP's "ongoing trials to implement a biometric exit process in the future."³²

CBP's Iris Imaging Testing

51. In addition to the use of facial recognition, the CBP is testing "iris imaging capabilities."

52. Beginning in December 2015, the CBP began phase 1 of 2 for biometric entry/exit testing at Otay Mesa Port of Entry.³³

53. Phase 1 of the testing at Otay Mesa Port of Entry included capturing the iris images of non-U.S. citizens entering the U.S.³⁴

54. Phase 2, which began in February 2016, consisted of requiring certain non-U.S. citizens to "provide facial and iris biometrics to compare to their entry record."³⁵

EPIC's FOIA Requests

EPIC's Biometric Air Entry FOIA Request

³¹ JetBlue, *Board in a Snap: JetBlue to Launch First-of-Its-Kind Self-Boarding Program Using Facial Recognition*, Business Wire (May 31, 2017), <http://www.businesswire.com/news/home/20170531005701/en/>.

³² *Id.*

³³ U.S. Customs and Border Protection, *CBP to Begin Biometric Entry/Exit Testing at Otay Mesa Port of Entry* (Dec. 10, 2015), <https://www.cbp.gov/newsroom/local-media-release/cbp-begin-biometric-entryexit-testing-otay-mesa-port-entry>

³⁴ *Id.*

³⁵ *Id.*

55. On June 14, 2016, EPIC submitted a FOIA Request (“EPIC’s Biometric Air Entry FOIA Request”) to DHS’s Privacy Office via email.

56. EPIC’s Biometric Air Entry FOIA Request was also submitted to the DHS’s Privacy Office via fax on June 15, 2016.

57. EPIC’s Biometric Air Entry FOIA Request sought records pertaining to the 1:1 Facial Recognition Air Entry Pilot and the 1-to-1 Facial Comparison Project. Specifically, EPIC sought:

1. The Report detailing all findings from the 1:1 Facial Recognition Air Entry Pilot (subsequently renamed “1-to-1 Facial Comparison Project”) implemented in 2015.
2. Any and all technical specifications for facial recognition and data retention as deployed in both the 1:1 Facial Recognition Air Entry Pilot and the expanded 1:1 Facial Comparison Project.
3. Any and all Requests for Proposal, contracts, grant allocations, and Statements of Work related to the 1:1 Facial Comparison Project.

58. EPIC sought “news media” fee status under 5 U.S.C. § 552(4)(A)(ii)(II), and a waiver of all duplication fees under 5 U.S.C. § 552(a)(4)(A)(iii).

59. EPIC also sought expedited processing under 5 U.S.C. § 552(a)(6)(E)(v)(II).

60. In an email dated April 5, 2017, EPIC National Security Counsel, Jeramie Scott, emailed the DHS Privacy Office to ascertain the status of EPIC’s Biometric Air Entry FOIA Request.

61. In an email dated April 6, 2017, the DHS Privacy Office confirmed that the EPIC’s Biometric Air Entry FOIA Request had been received and was transferred to the CBP FOIA office on July 6, 2016.

62. The CBP has not made a determination on or acknowledged EPIC's Biometric Air Entry FOIA Request.

EPIC's Biometric Exit FOIA Request

63. On June 13, 2017, EPIC submitted a FOIA Request ("EPIC's Biometric Exit FOIA Request") to DHS's CBP division via fax.

64. EPIC's Biometric Exit FOIA Request sought records pertaining to CBP's biometric exit programs that use facial recognition. Specifically, EPIC sought:

1. All technical specifications, contracts, and statements of work for purchases and acquisitions related to CBP's biometric exit programs and partnerships, including but not limited to the Departure Information Systems Test ("DIST"), the Departure Verification System ("DVS"), the Traveler Verification Service ("TVS"), the JetBlue self-boarding program, and the June 2017 Washington Dulles International Airport ("Dulles Airport") biometric exit deployment;
2. All policies and procedures for the collection, storage, analysis, use, dissemination, retention, and/or deletion of data obtained through the JetBlue self-boarding program, the June 2017 Dulles Airport biometric exit deployment, and any other biometric exit program;
3. All records concerning the dissemination of data collected by any biometric exit program, past or present, with other agencies, whether federal, state, local, or international, or third parties;
4. Any correspondence between CBP and JetBlue and/or SITA concerning the facial recognition pilot program, and any correspondence with other airlines, airports, and/or companies concerning the use of facial recognition for a biometric exit program;
5. Reports, memoranda, or other documents analyzing the biometric exit pilot programs, including but not limited to reports on the accuracy and/or possible racial bias of the facial recognition technology used in DIST, DVS, TVS, and any other biometric exit program;
6. Any audits of the systems used for photo collection or facial recognition in DIST, DVS, TVS, or any other biometric exit program;
7. Any training materials for the systems used in DIST, DVS, TVS, or any other biometric exit program, including any training materials shared with JetBlue or any other airline, third party, or agency, whether federal, state, or local;

8. Memoranda or other documents about expansion of the biometric exit program, including but not limited to plans to implement further public/private partnerships and partnerships with local, state, and federal agencies;
9. Any memorandum of understanding or similar agreement with federal, state, local, or international agencies or companies involved with the biometric exit program.

65. EPIC sought “news media” fee status under 5 U.S.C. § 552(4)(A)(ii)(II), and a waiver of all duplication fees under 5 U.S.C. § 552(a)(4)(A)(iii).

66. EPIC also sought expedited processing under 5 U.S.C. § 552(a)(6)(E)(v)(II).

67. The CBP has not made a determination on or acknowledged EPIC’s Biometric Exit FOIA Request.

EPIC’s Iris Recognition FOIA Request

68. On March 2, 2017, EPIC submitted a FOIA Request (“EPIC’s Iris Recognition FOIA Request”) to DHS’s CBP division via fax.

69. EPIC’s Iris Recognition FOIA Request sought records pertaining to CBP’s use of iris recognition. Specifically, EPIC sought:

1. Policies and procedures for CBP scanning U.S. citizens’ eyes, including iris and retinal scans, upon entry and/or exit to the U.S., including but not limited to policies and procedures pertaining to the collection, access, dissemination, and retention of iris and retinal scans;
2. Technical specifications and contracts related to CBP scanning U.S. citizen eyes, including iris and retinal scans, upon entry and/or exit to the U.S.;
3. Passenger complaints from U.S. citizens related to CBP eye scans, including iris and retinal scans, upon entry and/or exit to the U.S.;
4. Reports or studies concerning the reliability of the eye scans, including iris and retinal scans, used by CBP for traveler identification; and

5. Memorandums of Understanding or other agreements for the dissemination or access to iris and retinal scan information collected by the CBP or agreements for CBP access to iris and retinal scan information collected by other entities.

70. EPIC sought “news media” fee status under 5 U.S.C. § 552(4)(A)(ii)(II), and a waiver of all duplication fees under 5 U.S.C. § 552(a)(4)(A)(iii).

71. EPIC also sought expedited processing under 5 U.S.C. § 552(a)(6)(E)(v)(II).

72. On March 9, 2017, CBP acknowledged receipt of EPIC’s Iris Recognition FOIA Request.

73. On March 16, 2017, the CBP’s online FOIA portal listed EPIC’s Iris Recognition FOIA Request as in the “Assignment” stage and estimated the date of completion as April 3, 2017.

74. The CBP has not made a determination regarding EPIC’s Iris Recognition FOIA Request.

EPIC’s Constructive Exhaustion of Administrative Remedies

75. Today is the 378th day since the CBP received EPIC’s Air Entry FOIA Request.

76. Today is the 36th day since the CBP received EPIC’s Biometric Exit FOIA Request

77. Today is the 139th day since the CBP received EPIC’s Iris Recognition FOIA Request.

78. The CBP has failed to make a determination with respect to all of EPIC’s FOIA Requests within the time period required by 5 U.S.C. § 552(a)(6)(B).

79. The CBP’s failure to make a determination within the statutory time limit violates the FOIA.

80. EPIC has constructively exhausted all administrative remedies under 5 U.S.C. § 552(a)(6)(C)(i).

Count I

Violation of FOIA: Failure to Comply With Statutory Deadlines

81. Plaintiff asserts and incorporates by reference paragraphs 1-80.

82. Defendant CBP has failed to make a determination regarding EPIC's Air Entry FOIA Request for 378 days and has thus violated the deadline under 5 U.S.C. § 552 (a)(6)(B).

83. Defendant CBP has failed to make a determination regarding EPIC's Biometric Exit FOIA Request for 36 days and has thus violated the deadline under 5 U.S.C. § 552 (a)(6)(B).

84. Defendant CBP has failed to make a determination regarding EPIC's Iris Recognition FOIA Request for 139 days and has thus violated the deadline under 5 U.S.C. § 552 (a)(6)(B).

85. Plaintiff has constructively exhausted all applicable administrative remedies with respect to EPIC's FOIA Requests. 5 U.S.C. § 552(a)(6)(C)(i).

Count II

Violation of FOIA: Unlawful Withholding of Agency Records

86. Plaintiff asserts and incorporates by reference paragraphs 1-85.

87. Defendant has wrongfully withheld agency records requested by Plaintiff.

88. Plaintiff has constructively exhausted applicable administrative remedies with respect to Defendant's withholding of the requested records.

89. EPIC has exhausted the applicable administrative remedies with respect to EPIC's FOIA Requests. 5 U.S.C. § 552(a)(6)(C)(i).

90. Plaintiff is entitled to injunctive relief with respect to the release and disclosure of the requested records.

Requested Relief

WHEREFORE, Plaintiff prays that this Court:

- A. Order Defendant to immediately conduct a reasonable search for all responsive records;
- B. Order Defendant to disclose to Plaintiff all responsive, non-exempt records;
- C. Order Defendant to produce records sought without the assessment of search fees;
- D. Order Defendant to grant EPIC's request for fee waiver;
- D. Award EPIC costs and reasonable attorney's fees incurred in this action; and
- E. Grant such other relief as the Court may deem just and proper.

Respectfully submitted,

Marc Rotenberg, D.C. Bar# 422825
EPIC President and Executive Director

Alan Butler, D. C. Bar# 1012128
EPIC Senior Counsel

By: /s/ Jeramie D. Scott
Jeramie D. Scott, D.C. Bar # 1025909
EPIC National Security Counsel

ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Dated: July 19, 2017