

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

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W., Suite 200
Washington, D.C. 20009,

Plaintiff,

v.

U.S. DEPARTMENT OF STATE,
2201 C Street, N.W.
Washington, D.C. 20520

Defendant.

Civ. Action No. 1:19-cv-1468

COMPLAINT FOR INJUNCTIVE RELIEF

1. This is an action under the Freedom of Information Act (“FOIA”), 5 U.S.C. § 552, to compel disclosure of records requested by Plaintiff Electronic Privacy Information Center (“EPIC”) from Defendant U.S. Department State (“State Department”).

2. EPIC seeks the release of records related to the Bureau of Consular Affairs’ Consular Consolidated Database (“CCD”). In this Complaint, EPIC challenges (1) the State Department’s failure to make a timely decision about EPIC’s FOIA Request; and (2) the State Department’s failure to release records responsive to EPIC’s FOIA Request. EPIC seeks injunctive and other appropriate relief.

Jurisdiction and Venue

3. This Court has subject matter jurisdiction over this action under 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 State Department.

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, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC pursues public education, government oversight, and analysis of government activities that impact individual privacy, free expression, and democratic values in the information age.¹

EPIC's Advisory Board includes distinguished experts in law, technology, and public policy.

6. EPIC maintains one of the most popular privacy websites in the world, <https://epic.org>, which provides EPIC's members and the public with access to information about emerging privacy and civil liberties issues. EPIC has a robust FOIA practice and routinely disseminates information obtained under the FOIA to the public through the EPIC website, EPIC's biweekly newsletter the *EPIC Alert*, and various 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).

7. Defendant U.S. State Department is a federal agency within the meaning of the FOIA, 5 U.S.C. § 552(f)(1). The State Department is headquartered in Washington, D.C.

Facts

8. The Consular Consolidated Database ("CCD") is a "data warehouse," under the control of the State Department, that collects and maintains sensitive personal information obtained from

¹ See EPIC, *About EPIC* (2018), <https://epic.org/epic/about.html>.

visa and passport applicants.² The personal data stored in the CCD includes immutable³ biometric data, such as fingerprints and facial photographs.⁴

9. The State Department, by means of the CCD, transfers this personal data to various agencies external to the State Department and for reasons not clearly related to the processing of visa and passport applications, the purpose of collection.⁵ One such agency is the Department of Homeland Security (“DHS”), which maintains the Traveler Verification Service database for use by U.S. Customs and Border Protection (“CBP”).

10. The Traveler Verification Service is part of a system of facial recognition at 17 major U.S. airports, managed by the CBP.⁶

11. The CBP has failed to undertake a public comment process on the use of facial recognition at U.S. airports.

12. There are Memoranda of Understandings (“MOU”) between the State Department and other federal agencies that “generally define[] a set of responsibilities and requirements” for the transfer of this personal data.⁷

² U.S. Dep’t of State, *Consular Consolidated Database (CCD) Privacy Impact Assessment (PIA)*, 1-3 (Oct. 2018), <https://www.state.gov/documents/organization/242316.pdf> [hereinafter CCD PIA].

³ See, e.g., Catie Edmondson, *An Airline Scans Your Face. You Take Off. But Few Rules Govern Where Your Data Goes.*, N.Y. TIMES (Aug. 6, 2018), <https://www.nytimes.com/2018/08/06/us/politics/facial-recognition-airports-privacy.html>, (“But biometric data, including scans of passengers’ faces and fingerprints, is among the most sensitive, according to privacy experts, because unlike other means of identification such as a Social Security number, it cannot be changed.”).

⁴ CCD PIA, *supra* note 2, at 3.

⁵ See, e.g., U.S. Dep’t of Homeland Sec., *Automated Biometric Identification System Privacy Impact Assessment (PIA)*, IDENT Appendix: A, 1 (Nov. 2017), <https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-identappendices-november2017.pdf>; U.S. Dep’t of Homeland Sec., DHS/CBP/PIA-056, *Privacy Impact Assessment for the Traveler Verification Service*, 4 (Nov. 14, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-november2018_2.pdf [hereinafter TVS Nov. 2018 PIA].

⁶ TVS Nov. 2018 PIA, *supra* note 5, at 1, 4; U.S. Customs and Border Prot., U.S. Dep’t of Homeland Sec., *Biometrics*, <https://www.cbp.gov/travel/biometrics> [last accessed Mar. 14, 2019].

⁷ CCD PIA, *supra* note 2, at 11.

13. These MOUs have not been made public. As a consequence, the public, the Congress, and the individuals to whom the data pertains do not know the circumstances under which biometric identifiers will be transferred to other federal agencies, who will have access to this sensitive personal information, or for what purposes the data will be used.

14. The State Department collects and maintains personal data on U.S. and non-U.S. persons in the CCD system, including highly sensitive, personally identifiable information, including names, addresses, birthdates, gender, race, nationality, biometric data (fingerprints and facial images), unique identification numbers (e.g., social security numbers, and alien registration numbers), medical information, family information, and even social media identifiers.⁸

15. The biometric data contained in the CCD is especially sensitive because “biometrics... are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.”⁹ Besides their immutability, facial images are especially sensitive data because they can be used by facial recognition systems to detect and identify human faces.

16. Further, the State Department, using the CCD system, enables a “repository of data flows” to other federal agencies.¹⁰ For example, the State Department transfers personally identifiable information from the CCD to the Department of Homeland Security, the Department of Commerce, the Department of Defense, the Department of Justice, the Government Printing Office, the Office of Personnel Management, the Federal Bureau of Investigation, as well as “[o]ther [i]nteragency [p]artners[.]”¹¹

⁸ CCD PIA, *supra* note 2, at 3.

⁹ 740 Ill. Comp. Stat. 14/5(c).

¹⁰ CCD PIA, *supra* note 2, at 2.

¹¹ *Id.* at 12-13.

17. The CCD Privacy Impact Assessment states that “[a]ll external agencies that share information with the CCD are required to sign an MOU or MOA, which generally define a set of responsibilities and requirements.”¹²

18. The public, the Congress, and the individuals whose personal biometric information is gathered by the State Department and managed in the CCD cannot meaningfully assess what happens to the biometric data, submitted only for the purposes of obtaining a passport or visa, until the State Department releases these agreements between the agency and the entities that obtain the data.

19. None of the application forms, currently available, specifically discuss the use of facial images submitted for purposes unrelated the processing of passport or visa applications. The *Privacy Act Statement* sections on *Purpose* and *Routine Uses*, which are nearly identical on each form,¹³ do not mention biometric data at all. The explanation of the *Purpose* for the collection reads simply: “We are requesting this information in order to determine your eligibility to be issued a U.S. passport. Your Social Security number is used to verify your identity.”¹⁴ The *Routine Uses* section also does not specifically address the sharing of biometric data either:

This information may be disclosed to another domestic government agency, a private contractor, a foreign government agency, or to a private person or private employer in accordance with certain approved routine uses. These routine uses include, but are not limited to, law enforcement activities, employment verification, fraud prevention, border security, counterterrorism, litigation activities, and activities that meet the Secretary of State's responsibility to protect U.S. citizens

¹² *Id.* at 11.

¹³ Form DS-82 for passport renewals contains a sentence not found in the others at the beginning of the *Routine Uses* section: “Your Social Security number will be provided to the Department of the Treasury and may be used in connection with debt collection, among other purposes authorized and generally described in this section.”

¹⁴ U.S. Dep’t of State, *U.S. Passport Application*, Form DS-11 (June 2016), <https://eforms.state.gov/Forms/ds11.pdf>; U.S. Dep’t of State, Form DS-82, *U.S. Passport Renewal Application for Eligible Individuals*, (Jan. 2017), <https://eforms.state.gov/Forms/ds82.pdf>; U.S. Dep’t of State, Form DS-5504, *Application for a U.S. Passport*, (June 2016), <https://eforms.state.gov/Forms/ds5504.pdf>.

and non-citizen nationals abroad. More information on the Routine Uses for the system can be found in System of Records Notices State-05, Overseas Citizen Services Records and State-26, Passport Records.¹⁵

20. Given the lack of specific information in these forms, American passport applicants have little-to-no warning that the personal information they provide for the clearly stated purpose of determining eligibility for a passport will then be transferred to other agencies to test and implement facial recognition technology, such as CBP's unregulated¹⁶ airport facial recognition roll-out.

21. The State Department routinely transfers biometric data from the CCD to CBP for use at airports and other ports of entry. There is no way for visa and passport applicants to opt-out of the disclosures the State Department makes to CBP and other agencies. The CBP has still not completed a public rulemaking concerning the use of facial recognition. It is not known which other agencies receive this personal data from the State Department, for what other purposes it is used, or whether the necessary regulatory requirements have been completed.

22. The terms of the transfer (e.g, restrictions on use, security, and subsequent dissemination of the information) to CBP and other agencies would likely be included in the MOUs EPIC seeks.

¹⁵ *Id.*

¹⁶ Sens. Edward J. Markey (D-MA) and Mike Lee (R-Utah), *Senators Markey and Lee Call for Transparency on DHS Use of Facial Recognition Technology* (Mar. 12, 2019), <https://www.markey.senate.gov/news/press-releases/senators-markey-and-lee-call-for-transparency-on-dhs-use-of-facial-recognition-technology>, (“Since the Department of Homeland Security began scanning travelers’ faces at U.S. airports, we have repeatedly called on the agency to honor their personal commitment to complete a rulemaking to establish privacy and security rules of the road... Despite these commitments, DHS has failed to follow through and appears to be expanding the program... DHS should pause their efforts until American travelers fully understand exactly who has access to their facial recognition data, how long their data will be held, how their information will be safeguarded, and how they can opt out of the program altogether.”).

23. EPIC seeks to inform the public and the Congress about the current practices of the State Department concerning the collection and disclosure of sensitive personal information.

EPIC's FOIA Request

24. On October 12, 2018, EPIC submitted a FOIA request ("EPIC's FOIA Request") to the State Department's FOIA Division via facsimile.

25. EPIC's FOIA Request sought records about the Bureau of Consular Affairs' Consular Consolidated Database. Specifically, EPIC sought:

- (1) All Memorandums of Understanding ("MOUs"), Memorandums of Agreement ("MOAs"), and other information-sharing access agreements and documents between the DOS and the Department of Homeland Security ("DHS"), and any office, agency, or division within the DHS regarding access to the CCD, including, but not limited to the Office of Biometric Identity Management ("OBIM"), U.S. Citizenship and Immigration Services ("USCIS"), and U.S. Customs and Border Protection ("CBP");
- (2) All MOUs, MOAs, and other information-sharing access agreements and documents between the DOS and the Department of Defense ("DOD"), and any office, agency, or division within the DOD that accesses the CCD;
- (3) All MOUs, MOAs, and other information-sharing access agreements and documents between the DOS and the Federal Bureau of Investigation ("FBI"), and any office, agency, or division within the FBI regarding access to the CCD;
- (4) Any other MOUs, MOAs, or other information-sharing access agreements between the DOS and any other local, state, or federal entity—specifically those agreements that address the access or use of biometric data contained within the CCD; and
- (5) Any MOUs, MOAs, or other agreements the DOS has with any local, state, or federal entity for DOS access to databases that contain biometric data.

26. 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).

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

28. EPIC received no acknowledgement letter from the State Department.

29. On November 29, 2018, EPIC contacted the State Department's FOIA office to inquire about the status of the request and for the request's tracking number. The State Department FOIA officer confirmed delivery of EPIC's FOIA request and tracking number, F-2019-00429. The officer stated that the request is still opened and is being processed.

30. On February 12, 2019, EPIC contacted the State Department's FOIA office again to inquire about the status of the request. The FOIA officer could not provide more detail of where the request was in the processing stage. The FOIA officer stated that she can follow up with EPIC after she has a better idea of where the request is in the processing stage.

31. On March 1, 2019, EPIC contacted the State Department's FOIA office again to inquire about the status of the request. The FOIA officer could not provide more detail of where the request was in the processing stage but offered to consult with her colleagues. The FOIA officer stated that she would follow up with EPIC regarding where exactly EPIC's FOIA Request was in the processing stage and provide an estimated date of completion.

32. As of May 20, 2019 there has been no update from the State Department's FOIA office to provide an estimated date of completion or information on the status of EPIC's FOIA Request.

EPIC's Constructive Exhaustion of Administrative Remedies

33. Today is the 219th day since the State Department received EPIC's FOIA Request.

34. The State Department has failed to make a determination regarding EPIC's FOIA Request for expedited processing within the time period prescribed by 5 U.S.C. § 552(a)(6)(E)(ii)(I).

35. Additionally, the State Department has failed to make a determination regarding EPIC's FOIA Request within the time period required by 5 U.S.C. § 552(a)(6)(A)(i).

36. EPIC has 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

37. Plaintiff asserts and incorporates by reference paragraphs 1–36.
38. Defendant State Department has failed to make a determination regarding EPIC’s FOIA Request for 219 days. Thus, the State Department has thus violated the deadlines under 5 U.S.C. §§ 552(a)(6)(E)(ii)(I), (a)(6)(A)(ii).
39. Plaintiff has constructively exhausted all applicable administrative remedies under 5 U.S.C. § 552(a)(6)(C)(i).

Count II

Violation of FOIA: Failure to Grant Request for Expedited Processing

40. Plaintiff asserts and incorporates by reference paragraphs 1–36.
41. Defendant’s failure to grant plaintiff’s request for expedited processing violated the FOIA, 5 U.S.C. § 552(a)(6)(E)(i).
42. Plaintiff is entitled to injunctive relief with respect to an agency determination on EPIC’s request for expedited processing.

Count III

Violation of FOIA: Unlawful Withholding of Agency Records

43. Plaintiff asserts and incorporates by reference paragraphs 1–36.
44. Defendant State Department has wrongfully withheld agency records requested by Plaintiff.
45. Plaintiff has exhausted all applicable administrative remedies under 5 U.S.C. § 552(a)(6)(C)(i).

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

Count IV

Claim for Declaratory Relief

47. Plaintiff asserts and incorporates by reference paragraphs 1–36.

48. Plaintiff is entitled under 28 U.S.C. § 2201(a) to a declaration of the rights and other legal relations of the parties with respect to the claims set forth in Counts I–IV.

Requested Relief

WHEREFORE, Plaintiff requests this Court:

- A. Order Defendant to immediately conduct a reasonable search for all responsive records;
- B. Order Defendant to take all reasonable steps to release non-exempt records;
- C. Order Defendant to disclose promptly to Plaintiff all responsive, non-exempt records;
- D. Order Defendant to produce the records sought without the assessment of search fees;
- E. Order Defendant to grant EPIC’s request for a fee waiver;
- F. Award EPIC costs and reasonable attorney’s fees incurred in this action; and
- G. 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

/s/ Jeramie D. Scott
JERAMIE D. SCOTT, D.C. Bar # 1025909
EPIC Senior 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: May 20, 2019