epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

VIA FACSIMILE

October 12, 2018

Kellie Robinson, Public Liaison
U.S. Department of State
Office of Information Programs and Services
A/GIS/IPS/RL
SA-2, Suite 8100
Washington, D. C. 20522-0208
Fax Number: (202) 261-8579

Dear FOIA Officer:

This letter constitutes an request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and is submitted on behalf of the Electronic Privacy Information Center ("EPIC") to the Department of State's ("DOS") Bureau of Administration.

EPIC seeks documents related to the Bureau of Consular Affairs's ("CA") Consular Consolidated Database ("CCD"). There is good reason to believe that the records exist and that the Bureau of Administration has them because these records are referred to in a Privacy Impact Assessment ("PIA") for the CCD published on July 17, 2015 by the DOS, and the Bureau of Administration is listed as the contact for this PIA.[1]

Documents Requested

(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;

[1] *See* U.S. Dep't of State, *Consular Consolidated Database (CCD) Privacy Impact Assessment (PIA)* (July 17, 2015), https://www.state.gov/documents/organization/242316.pdf [hereinafter CCD PIA].

(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.

Background

The CCD is a data warehouse that stores current and archived data about U.S. persons (i.e., citizens and legal permanent residents) and non-U.S. persons (i.e., foreign nationals). All data is pulled from applications for visas, passports, and American Citizen Services, and includes names, addresses, birthdates, biometric data (fingerprints and facial images), race, identification numbers (e.g., social security numbers and alien registration numbers) and country of origin.

Initially created to increase the efficiency of consular activity and to provide up-to-date information on transactions at domestic and post databases, the CCD functions as the "central consolidated storage facility" for the Bureau of Consular Affairs.[2] The CCD also interfaces with other internal DOS facial recognition systems, such as the Automated Biometric Identification System ("ABIS") and Integrated Biometric System ("IBS"). Both ABIS and IBS are "enterprise-level, facial-recognition matching" programs, and receive data from visa and passport applications via the CCD and disseminate facial recognition matching results with external agencies via the CCD.[3] One of the uses of the data stored within the CCD is "[r]egistration of applicant facial images for Facial Recognition."[4]

The CCD also serves as the "repository of data flows" between the DOS and external federal agencies that provide input to passport and visa approval systems.[5] The CCD is integrated with and serves as a "gateway" to DHS OBIM's Automated Biometric Identification System ("IDENT"), which performs automated fingerprint checking, and "other Federal biometric systems."[6] External data dissemination via the CCD is of interest to EPIC given its concerns with external agencies' use of biometric data, such as CBP's biometric entry/exit tracking system,[7] which recently entered Phase II of the technical demonstration testing facial recognition and iris imaging capabilities at certain U.S. airports.[8] CBP's biometric entry/exit program uses facial photos collected by the DOS.[9]

---

[2] *Id.* at 3.
[3] *See* U.S. Dep't of State, *Automated Biometric Identification System (ABIS) Privacy Impact Assessment (PIA)* (Aug. 8, 2013), https://www.state.gov/documents/organization/242309.pdf; U.S. Dep't of State, *Integrated Biometric System (IBS) Privacy Impact Assessment (PIA)* (July 9, 2015), https://www.state.gov/documents/organization/246821.pdf.
[4] CCD PIA, *supra* note 1, at 6.
[5] *Id.* at 3.
[6] *Id.* at 2.
[7] *See* Complaint for Injunctive Relief, *EPIC v. CBP*, No. 17-1438 (D.D.C. filed July 19, 2017).
[8] *See* U.S. Dep't of Homeland Sec., DHS/CBP/PIA-030(e), *Privacy Impact Assessment Update for the Traveler Verification Service (TVS): CBP-TSA Technical Demonstration Phase II* (Aug. 14, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030e-tvs-august2018_0.pdf.
[9] *Id.* at 1 n.3, 4.

Facial recognition systems are computer-based security systems that are able to automatically detect and identify human faces.[10] Facial recognition technology can be deployed "covertly, even remotely, and on a mass scale," and there is little an individual can do to prevent collection of his or her image.[11] Facial images and other types of biometric data are especially sensitive because, "unlike other means of identification . . . it cannot be changed."[12] That external agency facial recognition programs receive data from and disseminate results through the CCD raises serious privacy and civil liberties concerns.

The CCD PIA 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."[13] EPIC is pursuing this FOIA request to mitigate privacy concerns by making public these information-sharing access agreements.

Request for Expedition

EPIC is entitled to expedited processing of this request under the FOIA and the DOS's FOIA regulations because there is a "compelling need" for the information. 5 U.S.C. § 552(a)(6)(E)(v)(II); 22 C.F.R. § 171.11(f). Specifically, (1) there is an "urgency to inform the public concerning actual or alleged Federal Government activity," and (2) EPIC is "primarily engaged" in publishing and disseminating information "to the public in general." 22 C.F.R. § 171.11(f)(2).

First, there is a "compelling need" for the information because there is an "urgency to inform the public concerning actual or alleged Federal government activity." 22 C.F.R. § 171.11(f)(2). The "actual" federal government activity is the DOS's dissemination of biometric data for facial recognition purposes with external agencies via the CCD. The DOS published the CCD PIA and expressly lists "[r]egistration of applicant facial images for Facial Recognition" as a use of CCD data.[14] The DOS's CCD PIA also identifies the DHS, DOD, and FBI as external agencies with which the CCD disseminates data to.

There is an "urgency to inform the public" about the DOS's dissemination of data to external agencies given the sensitive nature of biometric data and the substantial privacy concerns regarding government use of facial recognition technology. Further, the speed at which the government is developing, implementing, and expanding biometric identification technology like CBP's biometric entry/exit program[15] has prompted vocal bipartisan concern from

[10] EPIC, *Face Recognition*, https://epic.org/privacy/facerecognition/.
[11] EPIC, *In the Matter of Facebook, Inc. and the Facial Identification of Users (EPIC Complaint, Request for Investigation, Injunction, and Other Relief)* (April 6, 2018), https://www.epic.org/privacy/facebook/FTC-Facebook-FR-Complaint-04062018.pdf.
[12] 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.
[13] CCD PIA, *supra* note 1, at 11.
[14] *Id.* at 6, 11.
[15] *See* Chris Burt, *U.S. Biometric Entry/Exit Program Moves on to Phase II*, Biometric Update (Sept. 6, 2018), https://www.biometricupdate.com/201809/u-s-biometric-entry-exit-program-moves-on-to-phase-ii.

Congress.[16] The broad language used in the CCD PIA, "[r]egistration of applicant facial images for Facial Recognition," without accompanying MOUs, MOAs, or other information-sharing access agreements, does not provide adequate information on the procedures and safeguards deployed by the DOS to ensure protection of applicants' biometric data.[17] It is urgent that the DOS release more information about the CCD.

Second, EPIC is an organization whose "primary activity involves publishing or otherwise disseminating information to the public in general." 22 C.F.R. § 171.11(f)(2). As the Court explained in *EPIC v. DOD*, "EPIC satisfies the definition of 'representative of the news media,'" entitling it to preferred fee status under FOIA. 241 F. Supp. 2d 5, 15 (D.D.C. 2003). EPIC's mission is to focus public attention on emerging privacy and civil liberties issues, and routinely disseminates documents obtained under the FOIA on its website.[18] EPIC's FOIA work is extensively covered by national news media organizations.[19] EPIC does not publish information specifically for one segment or group of people.

In submitting this request for expedited processing, I certify that this explanation is true and correct to the best of my knowledge and belief. 5 U.S.C. § 552(a)(6)(E)(vi).

Request for "News Media" Fee Status and Fee Waiver

EPIC is a "representative of the news media" for fee classification purposes. *EPIC v. DOD*, 241 F. Supp. 2d at 6. Based on EPIC's status as a "news media" requester, EPIC is entitled to receive the requested record with only duplication fees assessed. 5 U.S.C. § 552(a)(4)(A)(ii)(II).

Moreover, any duplication fees should also be waived because (1) disclosure "is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government" and (2) disclosure "is not primarily in the commercial interest of the requester." 5 U.S.C. § 552(a)(4)(A)(iii); 22 C.F.R. § 171.16(a)(1)–(2).

(1) Disclosure of the information is likely to contribute to public understanding of the operations or activities of the government.

Disclosure of the requested documents is "in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government." 22 C.F.R. § 171.16(a)(1). DOS components evaluate four considerations to determine whether this requirement is met: (i) the "subject of the request must concern

---

[16] *See* Mack DeGeurin, *Facial Recognition Concerns Gain Political Legitimacy*, Medium (Sept. 20, 2018), https://medium.com/@bmd329/facial-recognition-concerns-gain-political-legitimacy-734da41162a7; Devin Coldewey, *Sen. Harris Tells Federal Agencies to Get Serious About Facial Recognition Risks*, TechCrunch (Sept. 18, 2018), https://techcrunch.com/2018/09/18/sen-harris-tells-federal-agencies-to-get-serious-about-facial-recognition-risks/; Press Release, Senator Ed Markey (D-Mass.), Senators Markey and Lee Release Statement on Facial Recognition Technology Use at Airports (June 22, 2018), https://www.markey.senate.gov/news/press-releases/senators-markey-and-lee-release-statement-on-facial-recognition-technology-use-at-airports.
[17] CCD PIA, *supra* note 1, at 6.
[18] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html; EPIC, *EPIC FOIA Cases*, https://epic.org/foia/.
[19] *See* EPIC, *EPIC in the News*, https://epic.org/news/epic_in_news.php/.

identifiable operations or activities of the Federal Government, with a connection that is direct and clear, not remote or attenuated"; (ii) disclosure "must be meaningfully informative about government operations or activities in order to be 'likely to contribute' to an increased public understanding of those operations or activities"; (iii) "disclosure must contribute to the understanding of a reasonably broad audience of persons interested in the subject, as opposed to the individual understanding of the requester," and (iv) "[t]he public's understanding of the subject in question must be enhanced by the disclosure to a significant extent." *Id.*

First, the subject of the request concerns "identifiable operations or activities of the Federal Government." 22 C.F.R. § 171.16(a)(1)(i). The DOS's CCD PIA expressly identifies which external agencies the CCD disseminates data to and lists "[r]egistration of applicant facial images" for facial recognition as a use of the data within the CCD.[20]

Second, disclosure would be "meaningfully informative" and "'likely to contribute' to an increased understanding of government operations or activities," 22 C.F.R. § 171.16(a)(1)(ii), because little new information is known about the program other than what has been released. The release of this information would meaningfully inform the public about the DOS's use and dissemination of the biometric data it collects from visa and passport applicants with external agencies.

Third, disclosure will "contribute to the understanding of a reasonably broad audience of persons interested in the subject" because, as provided in the DOS FOIA regulations, the DOS components will "presum[e] that a representative of the news media will satisfy this consideration." 22 C.F.R. § 171.16(a)(1)(iii).

Fourth, the public's understanding of the DOS's use of biometric data will "be enhanced by the disclosure to a significant extent." 22 C.F.R. § 171.16(a)(1)(iv). The federal government's use of biometric data for facial recognition purposes has drawn growing public attention and criticism.[21] The public, which includes all visa and passport applicants, is currently unaware of the extent of the DOS's dissemination of biometric data with external agencies. The MOUs, MOAs, and other agreements detailing the information-sharing processes and safeguards the DOS has in place with external agencies will provide insight into the way their personal data is handled, privacy and security risks associated with the dissemination of the data externally, and steps the DOS is taking to mitigate such risks.

---

[20] CCD PIA, *supra* note 1, at 6, 11.

[21] *See* Lori Aratani, *Facial-Recognition Scanners at Airports Raise Privacy Concerns*, Wash. Post (Sept. 15, 2018), https://www.washingtonpost.com/local/trafficandcommuting,/facial-recognition-scanners-at-airports-raise-privacy-concerns/2018/09/15/a312f6d0-abce-11e8-a8d7-0f63ab8b1370_story.html?; Morgan Wright, *Our Government is Moving Toward Facial Recognition Technology, But Where Will It Take Us?*, The Hill (Aug. 26, 2018), https://thehill.com/opinion/technology/403394-our-government-is-moving-toward-facial-recognition-technology-but-where; 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; Asma Khalid, *Facial Recognition May Boost Airport Security But Raises Privacy Worries*, Nat'l Pub. Radio (June 26, 2017), https://www.npr.org/sections/alltechconsidered/2017/06/26/534131967/facial-recognition-may-boost-airport-security-but-raises-privacy-worries.

(2) Disclosure of the information is not primarily in the commercial interest of the requester.

The "[d]isclosure of the information is not primarily in the commercial interest" of EPIC. 22 C.F.R. § 171.16(a)(2). The DOS components evaluate two considerations in assessing this requirement: (i) "whether the requester has a commercial interest that would be furthered by the requested disclosure"; and, if so, (ii) "whether disclosure is primarily in the commercial interest of the requester." *Id.*

First, EPIC has no "commercial interest . . . that would be furthered by the requested disclosure." 22 C.F.R. § 171.16(a)(2)(i). EPIC is a registered non-profit organization committed to privacy, open government, and civil liberties.[22]

Second, disclosure is not "primarily in the commercial interest of the requester." 22 C.F.R. § 171.16(a)(2)(ii). Again, EPIC has no commercial interest in the requested records and has established that there is significant public interest in the requested records.

For these reasons, a fee waiver should be granted to EPIC's request.

Conclusion

Thank you for your consideration of this request. I anticipate your determination on EPIC's request within ten calendar days. 5 U.S.C. § 552(a)(6)(E)(ii)(I). For responses to or questions regarding this request contact Enid Zhou at 202-483-1140 x104 or FOIA@epic.org.

Respectfully submitted,

/s Casey Matsumoto
Casey Matsumoto
EPIC Law Clerk

/s Jeramie D. Scott
Jeramie D. Scott
EPIC National Security Counsel

/s Enid Zhou
Enid Zhou
Open Government Counsel

[22] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.