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.** **FEDERAL BUREAU OF INVESTIGATION** **Washington, D.C. 20230** **Defendant.**	)	**Civil Action No. _____**

COMPLAINT FOR INJUNCTIVE RELIEF

1. This is an action under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552(a) (2009), for injunctive and other appropriate relief, seeking the release of agency records requested by Plaintiff Electronic Privacy Information Center ("EPIC") from Defendant United States Federal Bureau of Investigation ("FBI").

2. EPIC challenges the failure of the FBI to disclose non-exempt records in response to EPIC's FOIA request ("EPIC's FOIA Request") for records pertaining to biometric and identity management data agreements between the FBI and the Department of Defense ("DOD"). EPIC now seeks an injunctive order requiring disclosure, as soon as practicable, of all responsive, non-exempt records.

Jurisdiction and Venue

3. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 and 5 U.S.C. §§ 552(a)(4)(A)(vii), (a)(4)(B), and (a)(6)(c)(i). This Court has personal jurisdiction over Defendant FBI.

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

Parties

5. Plaintiff EPIC is a public-interest research organization incorporated as a 501(c)(3) non-profit corporation in Washington, D.C. EPIC conducts government oversight and analyzes the impact of government programs on civil liberties and privacy interests. EPIC publishes books, reports, and a bi-weekly newsletter. EPIC also maintains a popular website, epic.org, where EPIC publishes educational resources about emerging privacy and civil liberties issues, including documents obtained from federal agencies under the FOIA. 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.

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

Facts

Biometric and Identity Data Memoranda of Understanding

7. The FBI developed and maintains a biometric identification program called "Next Generation Identification" ("NGI"). The Bureau describes NGI as "the world's largest and most efficient electronic repository of biometric and criminal history information."[1] The FBI developed NGI as a successor to the Integrated Automated Fingerprint Identification System

[1] *Next Generation Identification (NGI),* Federal Bureau of Investigation (last visited Nov. 2, 2016), https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi.

("IAFIS"), a program started in July 1999 that provided to law enforcement "automated tenprint [fingerprint] and latent fingerprint searches, electronic image storage, electronic exchanges of fingerprints and responses, as well as text-based searches based on descriptive information."[2]

8. In NGI, the FBI incorporated all of the capabilities and data of IAFIS, along with additional capabilities such as the ability to quickly and easily store and search for new forms of biometric data, including iris scans and face-prints.[3]

9. Since 2014, the FBI has been using NGI at "full operational capability."[4]

10. With NGI, the FBI will expand the number of uploaded photographs and provide investigators with "automated facial recognition search capability."[5] The FBI intends to do this by eliminating restrictions on the number of submitted photographs (including photographs that are not accompanied by tenprint fingerprints) and allowing the submission of non-facial photographs (e.g. scars or tattoos).[6]

11. The FBI also widely disseminates this NGI data. According to the FBI's latest NGI fact sheet, 24,510 local, state, tribal, federal and international partners submitted queries to NGI in September 2016.[7]

12. Widespread deployment of facial recognition technology presents a number of significant privacy and security issues.[8] Facial recognition data is personally identifiable information and

---

[2] *Id.*
[3] *Id.*
[4] *FBI Announces Biometrics Suite's Full Operational Capability*, Federal Bureau of Investigation (Sept. 23, 2014), https://www.fbi.gov/news/stories/fbi-announces-biometrics-suites-full-operational-capability/fbi-announces-biometrics-suites-full-operational-capability.
[5] *What Facial Recognition Technology Means for Privacy and Civil Liberties:* Before the Subcommittee on Privacy, *Technology* and the Law, S. Jud. Comm., 112th Cong. (2012) (Testimony of Jerome Pender, Deputy Assistant Director of the *Criminal* Justice Information Services Division of the *FBI) available at* https://www.judiciary.senate.gov/imo/media/doc/12-7-18PenderTestimony.pdf.
[6] *Privacy Impact Assessment for the Next Generation Identification System (NGI) Interstate Photo System*, Federal Bureau of Investigation (Sept. 2015), https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/interstate-photo-system [hereinafter "NGI PIA"].
[7] *Next Generation Identification (NGI) Monthly Fact Sheet*, Federal Bureau of Investigation (last visited Nov. 2, 2016), https://www.fbi.gov/file-repository/ngi-monthly-fact-sheet.

improper collection, storage, and use of this information can result in identity theft or inaccurate identifications.[9] Additionally, an individual's ability to control access to his or her identity, including determining when to reveal it, is an essential aspect of personal security that facial recognition technology erodes.[10] Ubiquitous and near-effortless identification eliminates individuals' ability to control their identities, posing special risk to protestors engaging in lawful, anonymous free speech.[11] The U.S. Supreme Court has repeatedly upheld the right to engage in political speech anonymously.[12] For these reasons, it is vital that the deployment of facial recognition technology be done in a transparent way to ensure adequate public oversight.

13. The FBI recognized several risks associated with increased use of facial recognition technology in a Privacy Impact Assessment.[13] The FBI stated that "[i]ncreased collection and retention of personally identifiable information (PII) presents a correspondingly increased risk that the FBI will then be maintaining more information that might potentially be subject to loss or unauthorized use" and that, because "photographs may now be submitted without accompanying ten-print fingerprints," the accompanying photo "may be associated with the wrong identity."[14]

---

[8] Press Release, Federal Bureau of Investigation, *FBI Announces Initial Operating Capability for Next Generation Identification System* (Mar. 8, 2011), *available at* http://www.fbi.gov/news/pressrel/press_releases/fbi-announces-initial-operating-capabililty-for-next-generation-identification-system.

[9] *Biometric Identifiers,* EPIC (last visited Jan. 17, 2012), http://epic.org/privacy/biometrics/; EPIC Comments to the Federal Trade Commission, Face Facts: A Forum on Facial Recognition, Jan. 31, 2012, *available at* http://www.ftc.gov/os/comments/facialrecognitiontechnology/00083-82624.pdf.

[10] *Id*. at III.C.

[11] See Erik Larkin, *Electronic Passports May Make Traveling Americans Targets, Critics Say*, PC World (Apr. 11, 2005 4:00 AM), https://www.pcworld.com/article/120292/electronic_passports_may_make_traveling_americans_targets_critics_say.html; *see* Jeffrey Rosen, *Protect Our Right to Anonymity*, N.Y. Times, Sept. 12, 2011.

[12] *See, e.g.*, *Buckley v. American Constitutional Law Foundation*, 525 U.S. 182 (1999); *Talley v. California*, 362 U.S. 60 (1960); *NAACP v. Alabama*, 357 U.S. 449 (1958).

[13] *See* NGI PIA.

[14] *Id.*

14. By notice published May 5, 2016, the FBI proposed to exempt the NGI database from several significant provisions of the Privacy Act of 1974.[15]

15. EPIC filed comments on the FBI's proposal to exempt NGI from the Privacy Act on July 6, 2016.[16]

16. One of the FBI's stated initiatives is for the Bureau, through NGI, to exchange information with other data repositories in real or near-real time.[17] NGI is currently capable of such information transfers with the Automated Biometric Identification System ("ABIS"), a biometric program run by the DOD.[18]

17. The FBI has acknowledged the existence of a memorandum of understanding, dated September 10, 2009, between the FBI and the DOD pertaining to the transfer of biometric data and other identity management information.[19]

EPIC's FOIA Request

18. On April 2, 2015, EPIC submitted a FOIA Request to the FBI's Record/Information Dissemination Section via fax and email.

19. EPIC's FOIA Request sought records pertaining to all memoranda of understanding between the FBI and DOD relating to biometric data transfers. Specifically, EPIC sought:

1. All memoranda of understanding, memoranda of agreement, or equivalent documents between the FBI and Department of Defense ("DOD") for sharing of biometric and other identity management information;

---

[15] Notice of Proposed Rulemaking, 81 Fed. Reg. 27,288 (proposed May 5, 2016).
[16] EPIC, *Comments on Docket CPCLO Order No. 003-2016: Privacy Act of 1974; Implementation* (July 6, 2016), https://epic.org/apa/comments/EPIC-CPCLO-FBI-NGI-Comments.pdf.
[17] *Biometric Interoperability*, Criminal Justice Information Services Division Interoperability Initiatives Unit, Federal Bureau of Investigation (Nov. 2, 2011), http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/files/facial-recog-forum-110211b.pdf.
[18] *Id; Defense Biometrics: DOD Can Better Conform to Standards and Share Biometric Information with Federal Agencies*, United States Government Accountability Office (Mar. 2011), http://www.gao.gov/assets/320/317368.pdf.
[19] *Biometric Interoperability*, Criminal Justice Information Services Division, Federal Bureau of Investigation 4 (Nov. 2, 2011), https://www.fbi.gov/file-repository/about-us-cjis-fingerprints_biometrics-biometric-center-of-excellences-facial-recog-forum-110211b.pdf.

2. All memoranda of understanding, memoranda of agreement, or equivalent documents between the FBI and DOD regarding interoperability or the facilitation of interoperability between FBI and DOD databases that contain biometric data.
3. All documents and communications related to any memorandum of understanding (or equivalent document) between the FBI and the DOD for sharing of biometric and other identity management information.
4. All documents and communications related to any memorandum of understanding (or equivalent document) between the FBI and the DOD regarding interoperability or the facilitation of interoperability between FBI and DOD databases that contain biometric data.

20. EPIC sought "news media" fee status under 5 U.S.C. § 552(4)(A)(ii).

21. EPIC also sought a waiver of all duplication fees under 5 U.S.C. § 552(a)(4)(A)(iii).

22. In an email dated April 2, 2015, FBI Public Information Officer, David P. Sobonya, acknowledged receipt of EPIC's FOIA Request.

23. In a letter dated April 13, the FBI again acknowledged EPIC's FOIA Request and assigned it FOIPA Request number 1326085-000. The Bureau also indicated that it was searching for responsive records and that EPIC's fee waiver request was under consideration.

24. On August 11, after receiving no word from the FBI, EPIC submitted an administrative appeal to the DOJ's Office of Information Policy noting the FBI's failure to make a determination as to EPIC's FOIA Request.

25. In a letter dated August 21, the Office of Information Policy acknowledged receipt of EPIC's administrative appeal.

26. In a letter dated August 31, the Office of Information Policy wrote that the Office was not required to act on EPIC's administrative appeal because the FBI had not yet made an adverse determination.

27. In a letter dated September 1, 2015, the FBI informed EPIC that 35 pages of responsive records were located, but released no records. According to the FBI, because the records "originated with, or contained information concerning, other Government Agencies [OGA]," the

Bureau had to consult with other agencies before releasing any records. The FBI concluded with a promise to correspond with EPIC when it completed the consultation.

28. To date, the FBI has not made any determination as to EPIC's FOIA Request.

EPIC's Constructive Exhaustion of Administrative Remedies

29. It has been 587 days since the DOJ received EPIC's FOIA Request.

30. The DOJ has failed to make a determination regarding EPIC's FOIA Request within the time period prescribed by 5 U.S.C. §§ 552(a)(6)(A)(i), (ii) and (a)(6)(E)(iii).

31. The DOJ's failure to make a determination within the statutory limit violates the FOIA.

32. 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

33. Plaintiff asserts and incorporates by reference paragraphs 1-26.

34. Defendant DOJ has failed to make a determination regarding EPIC's FOIA Request within twenty business days, and has thus violated the deadline under 5 U.S.C. § 552(a)(6)(A)(i) and 28 C.F.R. § 16.5.

35. Plaintiff has constructively exhausted all applicable administrative remedies with respect to EPIC's FOIA Request.

Count II

Violation of FOIA: Unlawful Withholding of Agency Records

36. Plaintiff asserts and incorporates by reference paragraphs 1-26.

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

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

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

Requested Relief

WHEREFORE, Plaintiff requests that this Court:

A. Order Defendant to conduct a reasonable search for all responsive records;

B. Order Defendant to disclose to Plaintiff, as soon as practicable, all responsive, non-exempt records;

C. Order Defendant to produce a *Vaughn* Index identifying any records or portions of records withheld, if such records exist, stating the statutory exemption claimed and explaining how disclosure would damage the interests protected by the claimed exemption;

D. Order Defendant to produce the records sought without the assessment of search fees;

E. Order Defendant to grant Plaintiff's request for a fee waiver;

F. Award Plaintiff 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

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

By: */s/ Jeramie D. Scott*
Jeramie D. Scott, D.C. Bar # 1025909

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

Dated: November 10, 2016