epic.org

April 2, 2015

1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA
+1 202 483 1140 [tel]
+1 202 483 1248 [fax]
www.epic.org

VIA FACSIMILE and EMAIL

Federal Bureau of Investigation
Record/Information Dissemination Section
170 Marcel Drive
Winchester, VA 22602-4483
Fax: (540) 868-4391
Email: foiparequest@ic.fbi.gov

RE: Freedom of Information Act Request

Dear FOIA Officer:

This letter constitutes a 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 Federal Bureau of Investigation ("FBI").

EPIC seeks all documents and communications related to any memorandum of understanding between the FBI and the Department of Defense ("DOD") for sharing of biometric and other identity management information.

Background

The FBI currently employs a biometric identification program known as "Next Generation Identification" ("NGI").[1] NGI grew out of the FBI's "Automated Fingerprint Identification System" ("IAFIS"), a "national fingerprint and criminal history system."[2] The FBI has described IAFIS as "the largest biometric database in the world," with a criminal master file of more than 70 million subjects and a separate civil file with an additional 32 million subjects.[3] NGI includes 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 identifiers, including

[1] *Next Generation Identification: Bigger-Better-Faster,* FEDERAL BUREAU OF INVESTIGATION (last visited Jan. 17, 2012), http://www.fbi.gov/about-uslcjis/fingerprints biometrics/ngi/ngi-overview.
[2] *Integrated Automated Fingerprint Identification System,* FEDERAL BUREAU OF INVESTIGATION (last visited Jan. 17, 2012), http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis. Currently IAFIS stores information including "names, addresses, social security numbers, telephone numbers email addresses, biometric identifiers, unique identifying numbers, gender, race, dates of birth geographic indicators, license numbers, vehicle identifiers including license plates and other descriptors and information collected as a result of an arrest or incarceration." FEDERAL BUREAU OF INVESTIGATIONS PRIVACY IMPACT ASSESSMENT (PIA) FOR THE NEXT GENERATION IDENTIFICATION (NGI) INTERSTATE PHOTO SYSTEM (IPS) (June 9, 2008), *available at* http://www.fbi.gov/foialprivacy-impact_assessments/interstate-photo-system.
[3] Id.

iris scans and face-prints.[4] According to a story released by the FBI on fbi.gov in September 2014, NGI is now at "full operational capability."[5]

In addition to providing new ways to store data, under NGI the FBI will expand the number of uploaded photographs and provide investigators with "automated facial recognition search capability."[6] The FBI lists several ways to accomplish this, including by eliminating restrictions on the number of submitted photographs, allowing the submission of photographs of subjects included in the database for civil rather than criminal matters, including photographs that are not accompanied by ten-print fingerprints, and allowing the submission of non-facial photographs (e.g. scars or tattoos).[7] Furthermore, this information will be widely shared; "more than 18,000 law enforcement agencies and other authorized criminal justice partners" will have access to NGI.[8]

Widespread deployment of facial recognition technology carries with it a number of privacy and security concerns.[9] Facial recognition data is personally identifiable information and improper collection, storage, and use of this information can result in identity theft or inaccurate identifications.[10] 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.[11] Ubiquitous and near-effortless identification eliminates individuals' ability to control their identities, posing special risk to protestors engaging in lawful, anonymous free speech.[12] The U.S. Supreme Court has repeatedly upheld the right to engage in political speech anonymously.[13] For these reasons, it is vital that the deployment of facial recognition technology be done transparently and thoughtfully.

---

[4] *Supra*, note 1.

[5] Federal Bureau of Investigation, FBI Announces Biometrics Suite's Full Operational Capability, http://www.fbi.gov (Sep. 23, 2014), http://www.fbi.gov/news/stories/2014/september/fbi-announces-biometrics-suites-full-operational-capability/fbi-announces-biometrics-suites-full-operational-capability.

[6] *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* http://www.judiciary.senate.gov/pdf/12-7-18PenderTestimony.pdf.

[7] FEDERAL BUREAU OF INVESTIGATIONS, PRIVACY IMPACT ASSESSMENT (PIA) FOR THE NEXT GENERATION INDENTIFICATION (NGI) INTERSTATE PHOTO SYSTEM (IPS) (June 9, 2008) [hereinafter PRIVACY ASSESSMENT], *available at* http://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system.

[8] *Id.*

[9] 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.

[10] *Biometric Identifiers,* ELEC. PRIVACY INFO. CTR. (last visited Jan. 17, 2012), *http://epic.org/privacy/* biometrics/; Electronic Privacy Information Center 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.

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

[12] 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.

[13] *See* Jeffrey Rosen, *Protect Our Right to Anonymity*, N.Y. Times, Sept. 12, 2011.

The FBI recognized several of these risks associated with increased use of facial recognition technology in its Privacy Impact Assessment.[14] 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."[15] To help mitigate these risks, the FBI proposed "aggressive training," "strong security features," and "both State and Federal audits to ensure accuracy."[16] In recognizing the privacy concerns involved, the FBI has also indicated that it would conduct thorough privacy impact assessments for each enhancement under NGI.[17]

The FBI has indicated that one of its initiatives is to achieve biometric-based information sharing by making the Department of Justice (DOJ) FBI Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification interoperable with other repositories in order to exchange information in real or near-real time.[18] One of the systems the FBI already has, or seeks to achieve, interoperability with is the Automated Biometric Identification System (ABIS).[19] The FBI has indicated that a memorandum of understanding between the FBI and the DOD relating to the sharing of biometric and other identity management information exists.

Documents Requested

EPIC hereby request the following documents:

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;
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.

---

[14] *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).
[15] *Id.*
[16] *Id.*
[17] *Supra*, Note 5.
[18] Criminal Justice Information Services Division Interoperability Initiatives Unit, Biometric Interoperability, http://www.fbi.gov (Nov. 2, 2011), http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/files/facial-recog-forum-110211b.pdf.
[19] *Id;* United States Government Accountability Office, DEFENSE BIOMETRICS, DOD Can Better Conform to Standards and Share Biometric Information with Federal Agencies, http://www.gao.gov (March 2011), http://www.gao.gov/assets/320/317368.pdf.

Request for "News Media" Fee Status

EPIC is a "representative of the news media" for fee status and waiver purposes.[20] As such, EPIC is entitled to receive the requested record for the cost of duplication only. Because disclosing this information will "contribute significantly to public understanding of the operations or activities of the government," any duplication fees should be waived.[21]

Conclusion

Thank you for your consideration of this request. As provided in 5 U.S.C. § 552(a)(6)(E)(ii)(I), we will anticipate your response within 20 business days. Should you require additional information, please contact Jeramie Scott at 202-483-1140 x108 or foia@epic.org.

Respectfully Submitted,

/s/
Jeramie D. Scott
EPIC National Security Counsel

/s/
Jared Galanis
EPIC Law Clerk

[20] *EPIC v. Dep't of Defense*, 241 F. Supp. 2d 5 (D.D.C. 2003).
[21] 5 U.S.C. § 552(a)(6)(E)(v)(II) (2008); *Al-Fayed v. CIA*, 254 F.3d 300, 306 (D.C. Cir. 2001).