epic.org

March 29, 2013

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

VIA ELECTRONIC MAIL

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

RE: Freedom of Information Act Request

Dear FOIA Officer:

This letter constitutes as 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 Investigations ("FBI").

EPIC seeks records related to the FBI's Facial Analysis Comparison and Evaluation (FACE) Services Unit.

Background

On July 18, 2012, the Senate Subcommittee on Privacy, Technology and the Law held a hearing on "What Facial Recognition Technology Means for Privacy and Civil Liberties."[1] At that hearing, Jerome Pender, the Deputy Assistant Director of the Information Services Branch for the Criminal Justice Information Services Division of the FBI, was one of the witnesses. In his statement for the record, Mr. Pender spoke of the FBI's Facial Recognition Pilot that permitted authorized law enforcement agencies to leverage the FBI's national repository of mug shots for facial recognition queries.[2]

At the time of the hearing, the FBI had executed MOUs with Michigan, Hawaii, and Maryland.[3] Several states were in the process of reviewing MOUs for the Facial Recognition Pilot, including South Carolina, Ohio, and New Mexico.[4] Additionally, Kansas, Arizona, Tennessee, Nebraska, and Missouri had expressed interest in the pilot.[5] Through Open Records

---

[1] http://www.judiciary.senate.gov/hearings/hearing.cfm?id=daba530c0e84f5186d785e4894e78220.
[2] *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Comm. on the Judiciary*, 112th Cong. 3 (2012) (statement of Jerome Pender, Deputy Assistant Director, FBI) [hereinafter *Pender Statement*].
[3] *Id.* at 4.
[4] *Id.*
[5] *Id.*

requests, some of the MOUs for the Facial Recognition Pilot have been obtained and posted online.[6]

In a follow-up question after the hearing, Senator Franken asked Mr. Pender about plans to expand the FBI's use of facial recognition technology to compare photos of fugitives to driver license photos held by state DMVs.[7] Senator Franken was referring to what Mr. Pender described as the FBI's "Project Facemask."[8] According to Mr. Pender, "'Project Facemask' was initiated in 2007 as a collaborative effort by the FBI and the North Carolina (NC) Department of Motor Vehicles (DMV) to use the NC DMV's facial recognition program as a means of locating fugitives and missing persons."[9]

After the conclusion of Project Facemask pilot in 2010, the capabilities of the pilot were evaluated.[10] The evaluation of the capabilities of Project Facemask lead the FBI to create the Facial Analysis Comparison and Evaluation (FACE) Services Unit.[11] Once the FACE Services Unit was created, it began "establishing Memoranda of Understanding (MOUs) with the DMVs of states whose laws allow them to share DMV information for law enforcement purposes."[12] The MOU process was "being carried out in coordination with the Office of the General Counsel and the FBI's Records Management Division."[13]

The increasing expansion of facial recognition technology carries with it a number of privacy and security concerns.[14] Facial recognition data is personally identifiable information and improper collection, storage, and use of this information can result in identity theft or inaccurate identifications.[15] 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.[16] Finally, ubiquitous and near-effortless identification eliminates individuals' ability to control their identities, posing special risk to protesters

---

[6] Memorandum of Understanding between the Federal Bureau of Investigation and the Maryland Department of Public Safety and Correctional Services Information Technology and Communications Division, *available at* https://www.eff.org/sites/default/files/filenode/Maryland_NGI_MOU_Face-recognition-BulkSubmission.pdf; Memorandum of Understanding between the Federal Bureau of Investigation and the State of Hawaii Department of the Attorney General, *available at* https://www.eff.org/sites/default/files/filenode/Hawaii_MOU_NGI_face-recognition.pdf.

[7] *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Comm. on the Judiciary*, 112th Cong. 1 (2012) (question for the record of Jerome Pender, Deputy Assistant Director, FBI) [hereinafter *Pender Question*].

[8] *Id.*

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] *Biometric Identifiers*, Elec. Privacy Info. Ctr. (last visited March 21, 2013), 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.

[15] Electronic Privacy Information Center Comments to the Federal Trade Commission, Face Facts: A Forum on Facial Recognition at III.C., Jan. 31, 2012.

[16] *See* Erik Larkin, *Electronic Passports May Make Traveling Americans Targets, Critics Say*, PC World (Apr. 11, 2005), http://www.pcworld.com/article/120292/article.html.

engaging in lawful, anonymous free speech.[17] The U.S. Supreme Court has repeatedly upheld the right to engage in political speech anonymously.[18] For these reasons, it is vital that the deployment of facial recognition technology be done transparently and thoughtfully.

The FBI recognizes these risks, at least to some extent. Mr. Pender states that procedures to protect privacy and civil liberties have been created for the FACE team to ensure proper disposal of personally identifiable information.[19] The MOUs between the FACE Services Unit and participating states include requirements for the state to protect privacy.[20] Additionally, communications between the FBI and DMVs regarding facial recognition services are logged for, at least in part, audit purposes.[21]

Documents Requested

1. The original MOU or agreement with the North Carolina DMV for "Project Facemask."
2. All MOUS or agreements with state DMVs established by the FACE Services Unit.
3. The procedures established to protect privacy and civil liberties with respect to the activities of the FACE team.
4. Any audits conducted of the FACE Services Unit's work with respect to facial recognition services.

Request for Expedited Processing

This request warrants expedited processing because it is made by "a person primarily engaged in disseminating information . . ." and it pertains to a matter about which there is an "urgency to inform the public about an actual or alleged federal government activity."[22] EPIC is "primarily engaged in disseminating information."[23]

There is particular urgency for the public to obtain information about the FBI's development and implementation of a program to run facial recognition queries on the databases of state DMVs. There is specific urgency for citizens who have or plan to obtain a state ID from a state DMV already participating in the FBI's facial recognition program. It is important for the public to be able to make informed decisions when deciding to acquire an ID, and it is vital to ensure privacy and security concerns are mitigated early in the development cycle. This requires fostering public discussions and engaging with decision-makers as soon as possible. For these reasons, EPIC is requesting expedited processing.

---

[17] *See* Jeffrey Rosen, *Protect Our Right to Anonymity*, N.Y. Times, Sept. 12, 2011.
[18] *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).
[19] *Pender Question* at 2.
[20] *Id.* n.1.
[21] *Pender Question* at 2.
[22] 5 U.S.C. § 552(a)(6)(E)(v)(II) (2008); *Al-Fayed v. CIA*, 254 F.3d 300, 306 (D.C. Cir. 2001).
[23] *American Civil Liberties Union v. Dep't of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004).

Request for "News Media" Fee Status

EPIC is a "representative of the news media" for fee waiver purposes.[24] 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.[25]

Conclusion

Thank you for your consideration of this request. As provided in 5 U.S.C. § 552(6)(e)(2), I will anticipate your determination of our request for expedited processing within 10 business days. For questions regarding this request, I can be contacted at 202-483-1140 x108 or foia@epic.org.

Respectfully Submitted,

Jeramie D. Scott
EPIC National Security Fellow

Ginger McCall
Director, EPIC Open Government Project

[24] *EPIC v. Dep't of Defense*, 241 F. Supp. 2d 5 (D.D.C. 2003).
[25] 5 U.S.C. § 552(a)(6)(E)(v)(II) (2008); *Al-Fayed v. CIA*, 254 F.3d 300, 306 (D.C. Cir. 2001).