



August 11, 2015

VIA CERTIFIED MAIL

Freedom of Information Act Appeal  
Office of Information Policy  
U.S. Department of Justice  
Suite 11050  
1425 New York Avenue, N.W.  
Washington, DC 20530-0001

1718 Connecticut Ave NW

Suite 200

Washington DC 20009

USA

+1 202 483 1140 [tel]

+1 202 483 1248 [fax]

www.epic.org

Re: Freedom of Information Act Appeal - Request of April 2, 2015

Dear FOIA Officer:

This letter constitutes an appeal under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and is submitted to the Office of Information Policy by the Electronic Privacy Information Center ("EPIC"). EPIC is appealing the Federal Bureau of Investigation's ("FBI's") failure to make a determination within the statutory deadline.

### Background

The FBI currently employs a biometric identification program known as "Next Generation Identification" ("NGI").<sup>1</sup> NGI grew out of the FBI's "Automated Fingerprint Identification System" ("IAFIS"), a "national fingerprint and criminal history system."<sup>2</sup> 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

<sup>1</sup> *Next Generation Identification: Bigger-Better-Faster*, FEDERAL BUREAU OF INVESTIGATION (last visited

Aug. 11, 2015), [https://www.fbi.gov/about-us/cjis/fingerprints\\_biometrics/ngi](https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi).

<sup>2</sup> *Integrated Automated Fingerprint Identification System*, FEDERAL BUREAU OF INVESTIGATION (last visited Aug. 11, 2015), [http://www.fbi.gov/about-us/cjis/fingerprints\\_biometrics/iafis](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." FBI, *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System (IPS)* (June 9, 2008) [hereinafter PRIVACY ASSESSMENT], available at [http://www.fbi.gov/foialprivacy-impact\\_assessments/interstate-photo-system](http://www.fbi.gov/foialprivacy-impact_assessments/interstate-photo-system).

separate civil file with an additional 34 million subjects.<sup>3</sup> 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 iris scans and face-prints.<sup>4</sup> According to a story released by the FBI on fbi.gov in September 2014, NGI is now at “full operational capability.”<sup>5</sup>

In addition to providing new ways to store data, under the NGI program the FBI will expand the number of uploaded photographs and provide investigators with “automated facial recognition search capability.”<sup>6</sup> 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 just 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).<sup>7</sup> 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.<sup>8</sup>

Widespread deployment of facial recognition technology carries with it a number of privacy and security concerns.<sup>9</sup> Facial recognition data is personally identifiable information and improper collection, storage, and use of this information can result in identity theft or inaccurate identifications.<sup>10</sup> 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.<sup>11</sup> Ubiquitous and near-effortless identification eliminates individuals' ability to control their identities, posing special risk to protestors

---

<sup>3</sup> FBI, *Integrated Automated Fingerprint Identification System*, [https://www.fbi.gov/about-us/cjis/fingerprints\\_biometrics/iafis/iafis](https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis).

<sup>4</sup> *Supra*, note 1.

<sup>5</sup> FBI, *FBI Announces Biometrics Suite's Full Operational Capability*, (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>.

<sup>6</sup> *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>.

<sup>7</sup> PRIVACY ASSESSMENT.

<sup>8</sup> *Id.*

<sup>9</sup> 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-capability-for-next-generation-identification-system](http://www.fbi.gov/news/pressrel/press_releases/fbi-announces-initial-operating-capability-for-next-generation-identification-system).

<sup>10</sup> EPIC, *Biometric Identifiers*, (last visited Aug. 11, 2015), <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>.

<sup>11</sup> *Id.* at III.C.

engaging in lawful, anonymous free speech.<sup>12</sup> The U.S. Supreme Court has repeatedly upheld the right to engage in political speech anonymously.<sup>13</sup> For these reasons, it is vital that the deployment of facial recognition technology be done transparently and thoughtfully.

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

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.<sup>18</sup> One of the systems the FBI already has, or seeks to achieve, interoperability with is the Automated Biometric Identification System (ABIS).<sup>19</sup> 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.

### Procedural History

---

<sup>12</sup> 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\\_american\\_targets\\_critics\\_say.html](https://www.pcworld.com/article/120292/electronic_passports_may_make_traveling_american_targets_critics_say.html).

<sup>13</sup> See Jeffrey Rosen, *Protect Our Right to Anonymity*, N.Y. Times, Sept. 12, 2011.

<sup>14</sup> 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).

<sup>15</sup> *Id.*

<sup>16</sup> *Id.*

<sup>17</sup> *Supra*, Note 5.

<sup>18</sup> 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](http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/files/facial-recog-forum-110211b.pdf).

<sup>19</sup> *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>.

On April 2, 2015 EPIC requested, via facsimile (540.868.4391) and an email (foiparequest@ic.fbi.gov), the following records:

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.

On April 2, 2015, the FBI, via email, confirmed receipt of EPIC’s FOIA request.

Though over 90 business days have elapsed since EPIC submitted its request by email,<sup>20</sup> EPIC has received no determination concerning its request.

#### EPIC Appeals the FBI’s Failure to Make a Determination within Statutory Timeline

EPIC hereby appeals the FBI’s failure to make determinations regarding the release of documents according to the FOIA’s statutory timeline.

Upon receipt of a FOIA request, an agency has twenty working days to determine whether it will release or deny a record, notify the requestor of that determination, articulate its reasoning for reaching this decision, and inform the requestor of her right to appeal any adverse determination.<sup>21</sup>

Under unusual circumstances, an agency may notify the requestor in writing that it intends to seek an extension of no more than ten additional working days to make a determination;<sup>22</sup> however, the time period for the FBI to seek this extension

---

<sup>20</sup> The observed date of Independence Day (July 3, 2015), a legal public holiday, has been excluded from these calculations. 5 U.S.C. § 552(a)(6)(A)(i).

<sup>21</sup> 5 U.S.C. § 552(a)(6)(A); *see also* 32 C.F.R. § 286.23(e)(1) (stating “[w]henver possible, initial determinations to release or deny a record normally shall be made and the decision reported to the requester within 20 working days after receipt of the request by the official designated to respond”).

<sup>22</sup> 5 U.S.C. § 552(a)(6)(B)(i).

has also passed.<sup>23</sup> Additionally, the agency must afford the requestor an opportunity to modify or limit the scope of the request so that it may be processed within the statutory time limit.<sup>24</sup>

A requestor has “constructively exhausted administrative remedies” and may file an action in district court when an agency fails to make a determination of whether to release documents responsive to a FOIA request or administrative appeal within the statutory time limit.<sup>25</sup>

As noted above, the FBI is beyond the twenty working day time limit. The FBI has neither made a determination of whether it will release documents responsive to EPIC’s FOIA request, nor provided EPIC with an opportunity to narrow the scope of its original request so that it may be processed in a timely fashion. Therefore, EPIC submits this appeal prior to seeking judicial review.

The FBI’s failure to make such determinations of the initial FOIA request and this administrative appeal will grant EPIC a cognizable claim to file suit in district court.<sup>26</sup>

#### EPIC Notes That No Fees May Be Assessed

Because the FBI has failed to make a determination or seek an extension within the required twenty-day period, no search or duplication fees may be assessed.<sup>27</sup>

Even absent the FBI’s failure to meet the twenty-day deadline, EPIC is entitled to “news media” fee status. EPIC is a non-profit, educational organization that routinely and systematically disseminates information to the public. Therefore, it is a “representative of the news media” for fee waiver purposes.<sup>28</sup>

#### Conclusion

EPIC appeals the FBI’s failure to make determinations regarding the release of documents according to the FOIA’s statutory timeline. Thank you for your prompt response to this appeal. I anticipate that you will produce responsive documents within 10 working days. For questions regarding this request I can be contacted at 202-483-1140 x108 or FOIA@epic.org.

---

<sup>23</sup> The observed date of Independence Day (July 3, 2015), a legal public holiday, has been excluded from these calculations. 5 U.S.C. § 552(a)(6)(A)(i).

<sup>24</sup> 5 U.S.C. § 552(a)(6)(B)(ii).

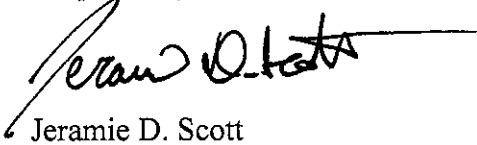
<sup>25</sup> *Nat’l Sec. Counselors v. C.I.A.*, 931 F. Supp. 2d 77, 95 (D.D.C. 2013) (citing *Judicial Watch, Inc. v. Rossotti*, 326 F.3d 1309, 1310 (D.C. Cir. 2003)); *Toensing v. U.S. Dep’t of Justice*, 890 F. Supp. 2d 121, 132 (D.D.C. 2012).

<sup>26</sup> *Nat’l Sec. Counselors*, 931 F. Supp. 2d at 95.

<sup>27</sup> 5 U.S.C. § 552(a)(4)(A)(vii), (ii)(II).

<sup>28</sup> *EPIC v. Department of Defense*, 241 F. Supp. 2d 5 (D.D.C. 2003).

Respectfully Submitted,

A handwritten signature in black ink, appearing to read "Jeramie D. Scott", with a long horizontal flourish extending to the right.

Jeramie D. Scott  
EPIC National Security Counsel