

1 Jennifer Lynch (SBN 240701)
jlynch@eff.org
2 ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
3 San Francisco, CA 94109
Telephone: (415) 436-9333
4 Facsimile: (415) 436-9993

5 David L. Sobel (*pro hac vice pending*)
sobel@eff.org
6 ELECTRONIC FRONTIER FOUNDATION
1818 N Street, N.W.
7 Suite 410
Washington, DC 20036
8 Telephone: (202) 797-9009 x104
Facsimile: (202) 707-9066

9 Attorneys for Plaintiff
10 ELECTRONIC FRONTIER FOUNDATION

11
12 UNITED STATES DISTRICT COURT
13 FOR THE NORTHERN DISTRICT OF CALIFORNIA

14 SAN FRANCISCO DIVISION

15 ELECTRONIC FRONTIER FOUNDATION,

16 Plaintiff,

17 v.

18 DEPARTMENT OF JUSTICE,

19 Defendant.

20
21
22
23
24
25
26
27
28
LB
CV 13 2946
COMPLAINT FOR INJUNCTIVE
RELIEF FOR VIOLATION OF THE
FREEDOM OF INFORMATION ACT,
5 U.S.C. § 552

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1. This is an action under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, for injunctive and other appropriate relief. Plaintiff seeks the release of records that Plaintiff requested from Defendant Department of Justice and its component, Federal Bureau of Investigation, concerning the agency's efforts to build out its biometrics systems and specifically its face recognition capabilities.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

PARTIES

2. Plaintiff Electronic Frontier Foundation (EFF) is a not-for-profit corporation established under the laws of the Commonwealth of Massachusetts, with offices in San Francisco, California and Washington, DC. EFF is a donor-supported membership organization that works to inform policymakers and the general public about civil liberties issues related to technology and to act as a defender of those liberties. In support of its mission, EFF uses the FOIA to obtain and disseminate information concerning the activities of federal agencies.

3. Defendant Department of Justice (DOJ) is a Department of the Executive Branch of the United States Government. DOJ is an “agency” within the meaning of 5 U.S.C. § 552(f). The Federal Bureau of Investigation (FBI) is a component of Defendant DOJ.

JURISDICTION

4. This Court has both subject matter jurisdiction over this action and personal jurisdiction over the parties pursuant to 5 U.S.C. §§ 552(a)(4)(B) and 552(a)(6)(C)(i). This Court also has jurisdiction over this action pursuant to 28 U.S.C. § 1331.

VENUE AND INTRADISTRICT ASSIGNMENT

5. Venue is proper in this district under 5 U.S.C. § 552(a)(4)(B) and 28 U.S.C. § 1391(e).

6. Assignment to the San Francisco division is proper pursuant to Local Rule 3-2(c) and (d) because a substantial portion of the events giving rise to this action occurred in this district and division, where Plaintiff is headquartered.

FACTUAL ALLEGATIONS

The FBI is Building “Bigger, Faster and Better” Biometrics Systems

7. The FBI has maintained a national criminal biometrics repository since 1924 and now controls one of the largest biometrics databases in the world.¹ This database, called the Integrated Automated Fingerprint Identification System (IAFIS), contains more than 100 million

¹ FBI, *Integrated Automated Fingerprint Identification System*, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis (last visited June 24, 2013) (hereinafter “FBI, *Integrated Automated Fingerprint Identification System*”).

1 fingerprints. 34 million of those are civil prints, which are collected as part of background checks
2 for sensitive positions and from US service members, applicants for federal jobs, and others. More
3 than 70 million of the prints in IAFIS are criminal and collected as a result of arrest, incarceration,
4 or another criminal justice purpose.² The database also contains biographic data such as name,
5 identification number and address; “criminal histories; mug shots; scars and tattoo photos; physical
6 characteristics like height, weight, and hair and eye color; and aliases.”³

7 8. For the last several years, the FBI has been working with private, federal, state and
8 local partners to build a “bigger, faster and better”⁴ biometrics system to replace IAFIS.⁵ In 2008,
9 the FBI awarded a contract estimated at 1 billion dollars to Lockheed Martin, the contractor that
10 developed the original IAFIS, to build the new system.⁶ This system, called Next Generation
11 Identification or NGI, is designed to be “multimodal” and will eventually include many “forms of
12 biometric identification like palm prints, iris scans, facial imaging, scars, marks, and tattoos—in
13 one searchable system.”⁷ NGI is also designed to be scalable to allow it to accommodate advanced
14 forms of biometrics like voice and gait as they become available in the future.⁸

15 NGI’s Facial Recognition Component

16 9. Although IAFIS has allowed the submission of some photographs since its inception
17 in 1999, this capability has been limited.⁹ Agencies are only able to submit a limited number of
18 criminal, “mug shot”-style photographs. These photographs are linked to the fingerprints and

19 ² FBI, *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate*
20 *Photo System (IPS)*, (June 9, 2008) [http://www.fbi.gov/foia/privacy-impact-assessments/interstate-](http://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system)
21 *photo-system* (hereinafter “FBI, *PIA for the NGI IPS*”); FBI, *Integrated Automated Fingerprint*
Identification System.

22 ³ FBI, *Integrated Automated Fingerprint Identification System*.

23 ⁴ FBI, *Beyond Fingerprints: Our New Identification System*,
https://www.fbi.gov/news/stories/2009/january/ngi_012609 (last visited June 24, 2013) (hereinafter
24 “FBI, *Beyond Fingerprints: Our New Identification System*”).

25 ⁵ FBI, *Next Generation Identification*, [https://www.fbi.gov/about-](https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi)
26 *us/cjis/fingerprints_biometrics/ngi* (last visited June 24, 2013).

27 ⁶ Alice Lipowicz & Ben Bain, *FBI Awards NGI Contract to Lockheed Martin*, Federal Computer
28 Week (Feb. 12, 2008) [http://fcw.com/articles/2008/02/12/fbi-awards-ngi-contract-to-lockheed-](http://fcw.com/articles/2008/02/12/fbi-awards-ngi-contract-to-lockheed-martin.aspx)
martin.aspx.

⁷ FBI, *Beyond Fingerprints: Our New Identification System*.

⁸ *Id.*

⁹ FBI, *Integrated Automated Fingerprint Identification System*.

1 biographic data with which they are submitted, and, as IAFIS currently has no face recognition
2 capabilities, the system is not able to search through the photographs independently from the prints
3 or data. Further, FBI does not accept photographs with civil fingerprint submissions.

4 10. NGI will change almost everything about how the FBI treats photograph
5 submissions. For example, NGI will allow “the increased capacity to retain photographic images,
6 additional opportunities for agencies to submit photographic images, and additional search
7 capabilities, including automated searches via the NCIC.”¹⁰ The proposed new system would also
8 allow law enforcement “to collect and retain other images (such as those obtained from crime
9 scene security cameras” and from friends and family)¹¹ and would allow submission of “civil
10 photographs along with civil fingerprint submissions that were collected for noncriminal
11 purposes.”¹²

12 11. NGI will also apply face recognition algorithms¹³ to the photographs, creating a
13 unique “face print” for each person. This will allow users to upload a photo of an unknown person
14 to the system, and the system will search through the database of face prints to find possible
15 matches.

16 12. Since late 2011, the FBI has been working with several states as part of a pilot
17 program to develop the face recognition capabilities of NGI.¹⁴ The pilot program will allow
18 participants that already have facial recognition capabilities within their own state criminal
19 database systems to upload face recognition-ready photographs to NGI and to search through a
20 database of mug shot photos.¹⁵ The goals of the pilot program are to “test the facial recognition
21

22 ¹⁰ FBI, *PIA for the NGI IPS*.

23 ¹¹ *Id.*

24 ¹² *Id.*

25 ¹³ See, e.g., FBI Biometric Center of Excellence, *Face Recognition*,
26 <http://www.biometrics.gov/Documents/FaceRec.pdf#page=2> (last visited June 24, 2013)
(discussing various face recognition algorithms).

27 ¹⁴ *Staff Paper: Next Generation Identification (NGI) Program Implementation and Transition*
28 *Update*, 6, CJIS Advisory Policy Board (APB) Spring 2012 Advisory Process Meetings
<https://www.eff.org/file/35292#page/6/mode/1up> (last visited June 20, 2013)(hereinafter “*Staff*
Paper: NGI Program Implementation and Transition Update”).

¹⁵ *Id.*

1 processes, resolve policy and processing issues, solidify privacy protection procedures, and address
2 user concerns.”¹⁶

3 13. As part of the pilot program, the FBI has executed Memoranda of Understanding
4 (MOUs) with several states that already have existing “Face/Photo search capability.” As of Spring
5 2012, these states included Maryland, Hawaii, and Michigan.¹⁷ As of Summer 2012, other states,
6 including South Carolina, Ohio, and New Mexico were “engaged in the MOU review process” to
7 participate in the pilot program, while Kansas, Arizona, Tennessee, Nebraska, and Missouri had
8 expressed interest in the program.¹⁸

9 14. Once the pilot program concludes, the FBI will roll out NGI access to states that do
10 not already have their own face recognition capabilities.¹⁹ The FBI appears to be developing new
11 software, called “Universal Face Workstation,” to enable this access.²⁰

12 15. The FBI also has access to many states’ Department of Motor Vehicles (DMV) face
13 recognition databases. As reported by the *Washington Post*, 37 states use facial recognition in their
14 DMV databases, and “at least 26 of those allow state local or federal law enforcement agencies to
15 search — or request searches.”²¹ The FBI has formal agreements with at least 10 of those states,²²
16 and has been working directly with one state—North Carolina—for at least four years.²³

17
18
19 ¹⁶ Jerome M. Pender, FBI, *Statement Before the Senate Judiciary Committee, Subcommittee on*
20 *Privacy, Technology, and the Law* (July 18, 2012) available at
<http://www.fbi.gov/news/testimony/what-facial-recognition-technology-means-for-privacy-and-civil-liberties>.

21 ¹⁷ *Staff Paper: NGI Program Implementation and Transition Update*, 6.

22 ¹⁸ Pender, FBI, *Statement Before the Senate Judiciary Committee, Subcommittee on Privacy,*
Technology, and the Law.

23 ¹⁹ *Id.*

24 ²⁰ *Staff Paper: NGI Program Implementation and Transition Update*, 6.

25 ²¹ Craig Timberg & Ellen Nakashima, *State Photo-ID Databases Become Troves for Police*, Wash.
26 *Post* (June 16, 2013) http://www.washingtonpost.com/business/technology/state-photo-id-databases-become-troves-for-police/2013/06/16/6f014bd4-ced5-11e2-8845-d970ccb04497_story.html.

27 ²² *Id.*

28 ²³ Mike Baker, *FBI Uses Facial Recognition Technology on DMV Photos*, USA Today (October
13, 2009) http://usatoday30.usatoday.com/tech/news/2009-10-13-fbi-dmv-facial-recognition_N.htm.

1 16. The FBI's plans for face recognition appear to be broader than mug shot and DMV
2 photos. The Face Recognition Pilot Program MOU between FBI and Hawaii states that full
3 implementation of the program will "permit photo submissions independent of arrests" and "permit
4 bulk submission of photos being maintained at state and federal repositories."²⁴ The FBI has also
5 stated in a public presentation given at a national biometrics conference that it wants to use its
6 facial recognition system to "identify[] unknown persons of interest from images" and "identify[]
7 subjects in public datasets."²⁵ In the same presentation, the FBI included a graphic image that
8 implied the Bureau wanted to use facial recognition to be able to track people from one political
9 rally to another.²⁶

10 17. The Bureau states that NGI's face recognition system is "scheduled for full
11 operational capability in the summer of 2014."²⁷ Upon deployment, "the repository will contain 12
12 million searchable frontal photos."²⁸

13 18. FBI has released very little information to the public about how it uses face
14 recognition, NGI's face recognition capabilities, or about its state pilot program.

15 Data Sharing and Database Interoperability

16 19. IAFIS and NGI have been designed to allow non-FBI users to access the systems
17 through data sharing and database interoperability.

18 20. FBI exchanges data regularly with more than 18,000 national, state, local and tribal
19 law enforcement agencies.²⁹ These agencies contribute fingerprints, mug shots, biographic data and
20

21 _____
22 ²⁴ *MOU between the FBI and the State of Hawaii Dept. of the Attorney Gen. for the Interstate*

23 *Photo System Facial Recognition Pilot, 2, available at*

24 *https://www.eff.org/file/35296#page/2/mode/1up* (last visited June 20, 2013).
²⁵ Richard Vorder Bruegge, *Facial Recognition and Identification Initiatives*, FBI, 5,

25 *https://www.eff.org/file/35308#page/5/mode/1up* (last visited June 20, 2013).

26 ²⁶ *Id.* at 4, available at *https://www.eff.org/file/35308#page/4/mode/1up*.
²⁷ Pender, FBI, *Statement Before the Senate Judiciary Committee, Subcommittee on Privacy,*

27 *Technology, and the Law*.

28 ²⁸ *Staff Paper: NGI Program Implementation and Transition Update*, 6.
²⁹ *FBI Announces Initial Operating Capability for Next Generation Identification System* (March 8,
2011) *http://www.fbi.gov/news/pressrel/press-releases/fbi-announces-initial-operating-capability-*
for-next-generation-identification-system (last visited June 18, 2012).

1 criminal histories to IAFIS and are able to query the database 24 hours per day and 365 days per
2 year.³⁰

3 21. In the last few years, FBI has been working with various federal agencies, including
4 Department of Homeland Security (DHS), Department of State, and Department of Defense (DOD)
5 to enable the agencies' respective biometrics databases to share data.³¹ As noted in a Privacy
6 Impact Assessment (PIA) discussing the plans for interoperability between IAFIS/NGI and DHS's
7 IDENT database, interoperability will achieve "1) enhanced access to, and in some cases
8 acquisition of, the IAFIS/NGI information by the IDENT and its users and 2) the reciprocal
9 enhanced access to, and in some cases acquisition of, the IDENT information by the IAFIS/NGI
10 and its users."³²

11 22. Federal database interoperability does not just affect the federal agencies
12 maintaining the individual databases. As of December 31, 2011, 43 states and the territory of
13 Puerto Rico were also able to take advantage of IDENT/IAFIS interoperability.³³

14 23. The FBI also shares biometric data with at least 77 countries through formal and
15 informal relationships.³⁴ The Bureau is in the process of partnering with several "Visa Waiver
16 Program countries" such as Ireland, Spain and Australia to allow each country automatic access to
17 the other's biometric database.³⁵

18 _____
19 ³⁰ *Id.*

20 ³¹ Biometrics Identity Management Agency, "The Biometrics Triad: Working to Seamlessly
21 Integrate Biometric Data," *The Biometric Scan*, (Jan.–March 2010)
http://www.biometrics.dod.mil/Newsletter/issues/2010/Jan/v6issue1_a4.html (last visited June 24,
2013).

22 ³² FBI, *Privacy Impact Assessment: Integrated Automated Fingerprint Identification System*
(IAFIS)/Next Generation Identification (NGI) Biometric Interoperability,
23 <https://www.fbi.gov/foia/privacy-impact-assessments/iafis-ngi-interoperability-1> (last visited June
24, 2013).

24 ³³ *Staff Paper: State Participation in Automated Biometric Identification System*
(IDENT)/Integrated Automated Fingerprint Identification System (IAFIS) Interoperability, CJIS
25 Advisory Policy Board (APB) Spring 2012 Advisory Process Meetings
<https://www.eff.org/file/35291#page/88/mode/1up> (last visited June 20, 2013).

26 ³⁴ *Staff Paper: Biometric Information Sharing Update*, CJIS Advisory Policy Board (APB) Spring
27 2012 Advisory Process Meetings <https://www.eff.org/file/35294#page/2/mode/1up> (last visited
28 June 20, 2013).

³⁵ *Id.*

1 Civil and Criminal Records

2 24. In the past, civil and criminal biometric and biographic data were kept separate in
3 IAFIS.³⁶ This meant that a query to one database would not necessarily produce records from the
4 other.³⁷

5 25. The FBI appears poised to link or combine the civil and criminal records in NGI
6 under a “Master Name” or unique identifier.³⁸ At a 2012 meeting, the Criminal Justice Information
7 Services (CJIS) Advisory Board—a body “responsible for reviewing appropriate policy, technical,
8 and operational issues” related to programs such as IAFIS³⁹—discussed plans to link the records,
9 which could allow system users to search criminal and civil records at the same time. The Board
10 stated that although “all information about a person in the system” would be maintained “as a
11 single record,” the system itself would be designed to ensure that “retained civil submissions
12 remain untainted by criminal submissions.”⁴⁰

13 26. FBI has not explained to the public how NGI or IAFIS’s system design would
14 ensure that civil submissions are not “tainted” by criminal submissions or explained why it is
15 necessary to combine the two types of data.

16 Privacy Concerns with IAFIS and NGI

17 27. Governmental use of face recognition—and the potential for misuse—raises many
18 privacy concerns. As Senator Al Franken noted at a hearing of the Senate Judiciary Subcommittee
19 on Privacy, Technology and the Law last year,

20 facial recognition creates acute privacy concerns that fingerprints do not.
21 Once someone has your fingerprint, they can dust your house or your
22 surroundings to figure out what you’ve touched. Once someone has your
23 faceprint, they can get your name, they can find your social networking

23 ³⁶ *Staff Paper: Implementation of the Next Generation Identification (NGI) Enhanced Repository*,
24 CJIS Advisory Policy Board (APB) Spring 2012 Advisory Process Meetings
25 https://www.eff.org/sites/default/files/filenode/FBI-CJIS-AB_NGI_Master_Name_2012.pdf (last
26 visited June 20, 2013)(hereinafter “*Staff Paper: Implementation of the NGI Enhanced*
27 *Repository*”).

28 ³⁷ *Id.*

³⁸ *Id.*

³⁹ FBI, *The CJIS Advisory Process: A Shared Management Concept*, <http://www.fbi.gov/about-us/cjis/advisory-policy-board> (last visited June 20, 2013).

⁴⁰ *Staff Paper: Implementation of the NGI Enhanced Repository*.

1 account and they can find and track you in the street, in the stores you
2 visit, the government buildings you enter, and the photos your friends post
3 online.⁴¹

4 Franken went on to note, “I fear that without further protections, this technology could be used on
5 unsuspecting civilians innocent of any crime, or could be used to instantly identify someone
6 walking down the street. I urge the FBI . . . to do more to protect people’s privacy so that this new
7 technology isn’t abused.”⁴²

8 28. The Privacy Impact Assessments (PIAs) for IAFIS and NGI have not kept pace with
9 these programs’ development. Five years ago, on June 9, 2008, the FBI published a PIA
10 concerning “enhancements” to the IAFIS Interstate Photo System (IPS).⁴³ This was only a few
11 months after FBI awarded the NGI contract to Lockheed Martin and well before the FBI developed
12 the face recognition component of NGI as it exists today.

13 29. Nevertheless, the PIA recognized several privacy risks posed by the enhancements.
14 For example, for some photos, “the subjects may not have been aware of being photographed, and
15 their identities may not yet be known or established.” Nevertheless, the PIA noted these photos
16 would still be included in the database. Photographs that could not be identified when submitted
17 would be “maintained in a common photo file.” If the individual in the photo is later identified, the
18 photo may later be associated with that individual’s file.⁴⁴ This means people may have their
19 photograph—and their unique face print—in a government-maintained criminal database without
20 their knowledge. And a certain percentage of these people likely are not engaged in criminal
21 activity.

22 30. The FBI recognizes that the 2008 Interstate Photo System PIA is outdated and
23 testified before Congress in July 2012 that “an updated PIA is planned and will address all
24

25 ⁴¹ Press Release, *Sen. Franken Presses Facebook, Government to Safeguard Privacy As Facial*
26 *Recognition Technology Quickly Advances*, (July 18, 2012)

http://www.franken.senate.gov/?p=press_release&id=2144.

27 ⁴² *Id.*

⁴³ FBI, *PIA for the NGI IPS*.

28 ⁴⁴ *Id.*

1 evolutionary changes since the preparation of the 2008 Interstate Photo System PIA.”⁴⁵ However,
2 although the Bureau appears to be accepting photographs from each of the states involved in the
3 pilot program and plans to achieve full deployment of its face recognition program next year, it has
4 yet to release a new PIA.

5 Technical Limitations of Face Recognition

6 31. Researchers and government officials have noted that face recognition is not
7 infallible, and is in fact “highly dependent on the quality of images enrolled in the system.”⁴⁶ It
8 performs well with consistent lighting conditions and poses. However, with variable lighting,
9 shadows, backgrounds, poses or expressions, the error rates are significant.⁴⁷ Other factors, such as
10 age of the subject, gender, and race also affect accuracy.⁴⁸ Further, as facial recognition databases
11 increase in size, the risk of false positives—such as a person being misidentified as the perpetrator
12 of a crime—increases as well.⁴⁹

13 32. The FBI recognizes this problem and has proposed to address it in several ways. In
14 the 2008 Interstate Photo System PIA, the FBI noted it planned to analyze and specify “critical
15

16 ⁴⁵Pender, FBI, *Statement Before the Senate Judiciary Committee, Subcommittee on Privacy,*
17 *Technology, and the Law.*

18 ⁴⁶ *Staff Paper: NGI Program Implementation and Transition Update*, 6; see also FBI Biometric
19 Center of Excellence, *Face Recognition*,
20 <http://www.biometriccoe.gov/Modalities/facialRecognition.htm> (last visited June 24, 2013) (noting
21 that “the need for higher accuracy [in face recognition] remains”).

22 ⁴⁷ See, e.g., P. Jonathon Phillips, et al., *An Introduction to the Good, the Bad, & the Ugly Face*
23 *Recognition: Challenge Problem*, National Institute of Standards & Testing (Dec. 2011), available
24 at www.nist.gov/itl/iad/ig/upload/05771424.pdf (noting only 15% accuracy for face image pairs
25 that are “difficult to match”). Security researcher Bruce Schneier has noted that even a 90%
26 accurate system “will sound a million false alarms for every real terrorist” and that it is “unlikely
27 that terrorists will pose for crisp, clear photos.” Bruce Schneier, *Beyond Fear: Thinking Sensibly*
28 *About Security in an Uncertain World*, 190 (2003).

⁴⁸ Patrick J. Grother, et al., *Report on the Evaluation of 2D Still-Image Face Recognition*
Algorithms, NIST Interagency Report 7709, 4 (Aug. 24, 2011) available at
http://www.nist.gov/customcf/get_pdf.cfm?pub_id=905968.

⁴⁹ See, e.g., Lucas D. Introna & Helen Nissenbaum, *Facial Recognition Technology: A Survey of*
Policy and Implementation Issues, 3, N.Y.U. (April 2009), available at
http://www.nyu.edu/ccpr/pubs/Niss_04.08.09.pdf; see also Grother, *Report on the Evaluation of 2D*
Still-Image Face Recognition Algorithms, 26 (“the chance of one or more false matches increases
with the population size”).

1 performance parameters . . . through functional and system requirements analysis.”⁵⁰ It would also
2 “promulgate policies and procedures to emphasize that photographic matches are not to be
3 considered ‘positive’ identifications, and searches of the photographs will merely result in a ranked
4 listing of candidates.”⁵¹ Further, “[u]sers will be trained on system limitations, and to recognize
5 that the aging process and intentional lifestyle choices will reduce the effectiveness of image
6 searching.”⁵²

7 33. The FBI has not made this technical information or any of its proposed policies for
8 addressing NGI face recognition’s limitations available to the public.

9 **Plaintiff’s FOIA Requests**

10 34. Between June 25, 2012 and July 5, 2012, Plaintiff sent three FOIA requests via
11 email to Defendant concerning Defendant’s use of facial recognition and development of its Next
12 Generation Identification (NGI) system.

13 35. Each of these requests sought search, review and duplication fee waivers based on
14 EFF’s status as a news media requester and based on the fact that disclosure of the requested
15 information is in the public interest within the meaning of 5 U.S.C. § 552(a)(4)(A)(ii)-(iii). In the
16 requests, EFF presented facts to support its fee waiver requests.

17 36. Each of these requests also asked that documents be produced in their native file
18 format. Specifically, EFF requested:

- 19 a. that files stored in electronic format be produced in electronic format;
- 20 b. that files be produced either in their native format (likely appropriate for
21 spreadsheets and database files—for example, Microsoft Excel files produced as .xls
22 electronic files) or as text-searchable pdf formatted files (likely appropriate for word
23 processing documents, letters, memos, or emails);
- 24 c. that files preserve the “parent / child” relationship between records (for example, if
25 an email has an attachment, that attachment—or, if appropriate, information

26 _____
27 ⁵⁰ FBI, *PIA for the NGI IPS*.

28 ⁵¹ *Id.*

⁵² *Id.*

1 regarding the attachment's withholding—should accompany or follow the pdf of the
2 email); and that the beginning and ending of individual records is clearly indicated.

3 First Request — FBI/State Facial Recognition Partnerships

4 37. The first request, dated June 25, 2012, sought records related to the FBI's plans to
5 partner with states to build out its facial recognition database. The request sought all agency
6 records, including electronic records, created from January 1, 2010 to the present concerning FBI's
7 plans to incorporate facial recognition capabilities and face-recognition-ready photographs into
8 NGI. Specifically, it sought records related to:

- 9 a. memoranda of understanding (MOUs) or other similar contracts or
10 agreements between the FBI and any states concerning submitting facial
11 recognition photographs to and retrieving or accessing photographs from the
12 Next Generation Identification database;
- 13 b. discussions between the FBI and any states regarding the state's
14 participation in a program to submit and/or retrieve facial recognition
15 photographs to the FBI's Next Generation Identification (NGI) database;
- 16 c. records related to a "Face Report Card," possibly created by FBI's Next
17 Generation Identification Program Office to "provide feedback to individual
18 agencies regarding the quality of images submitted" to the FBI's Next
19 Generation Identification database.

20 38. The FBI acknowledged receipt of Plaintiff's request via email dated June 26, 2012
21 and letter dated July 2, 2012. In the July 2 letter, the FBI stated it had begun the search and was
22 considering EFF's fee waiver request. Defendant also assigned Plaintiff's FOIA request, FOIA
23 Request No. 1193642.

24 39. In a letter dated October 5, 2012, the FBI stated it had located approximately "7380
25 pages which are potentially responsive to the FOIA." FBI also noted that EFF's fee waiver request
26 was still under review and requested that EFF convey its "willingness to pay the estimated search
27 and duplication costs" of "\$215.00 (15 CD's at \$15.00 less \$10.00) to receive the release on a CD."
28

- 1 a. any studies, reports, notes, comments, or other records on the reliability of
2 facial recognition biometric data in the NGI database and/or the Face
3 Recognition Pilot (FRP) project in the NGI database. These studies, reports,
4 etc, could include information on the ability of the database to accurately
5 identify a person in a photograph submitted to the database and/or data on
6 the false-accept rate (FAR) and false-reject rate (FRR) of the database;
- 7 b. any information on the total current number of face recognition capable
8 records and/or searchable frontal photographs in the database and the
9 proposed number at deployment;
- 10 c. any studies, reports, notes, comments, or other records that discuss specific
11 image quality metrics, best practices, and recommendations regarding
12 quality of images submitted to or enrolled in the system.

13 46. The FBI acknowledged receipt of Plaintiff's request via email dated July 6, 2012.

14 47. FBI has not produced any records in response to EFF's third request.

15 48. Defendant has exceeded the generally applicable twenty-day deadline for the
16 processing of FOIA requests.

17 49. Plaintiff has exhausted the applicable administrative remedies with respect to all of
18 its FOIA requests referenced herein.

19 50. Defendant has wrongfully withheld the requested records from Plaintiff.

20 CAUSES OF ACTION

21 **Violation of the Freedom of Information Act for Wrongful Withholding of Agency Records**

22 51. Plaintiff repeats and realleges paragraphs 1-50.

23 52. Defendant has wrongfully withheld agency records requested by Plaintiff by failing
24 to comply with the statutory time limit for the processing of FOIA requests.

25 53. Plaintiff has exhausted the applicable administrative remedies with respect to
26 Defendant's wrongful withholding of the requested records.

