



VIA FACSIMILE & EMAIL

March 9, 2018
Federal Bureau of Investigation
Attn: FOI/PA Request
Record/Information Dissemination Section
170 Marcel Drive
Winchester, VA 22602-4843
Email: foiparequest@ic.fbi.gov
Fax: (540) 868-4391/4997

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 Next Generation Identification (NGI) Monthly Fact Sheets to inform the public about how the NGI program operates.

Background

The Federal Bureau of Investigation employs NGI, a biometric identification system. The program grew out of the FBI’s Automated Fingerprint Identification System (“IAFIS”), a fingerprint database described by the FBI as “the world’s largest person-centric database.”¹ The program was first initiated in 1999. The FBI has since built NGI over the groundwork IAFIS provided, first deploying NGI in 2011. NGI vastly exceeds the original scope of IAFIS, encompassing additional types of biometric data,

¹ FBI, *Next Generation Identification (NGI)*, FBI.GOV (Sept. 7, 2016), <https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi>.

quick and easy search capabilities, and notification systems.² Today, NGI includes fingerprints, iris scans, palm prints, photos, and voice data, made available to state and federal agencies.³ Biometric records held in the database are frequently linked with other identifying data such as detailed biographic information, including criminal histories, physical characteristics of the individual, and employer name and contact information.⁴ Furthermore, the database logs the personal information of a wide variety of individuals, reaching beyond merely those formally accused of criminal conduct.⁵ As to program's scale, NGI housed over 30 million photos as of May 2016.⁶

FBI's collection of the personal information of millions of individuals via the NGI program, including the information of those without any link to the criminal justice system, raises significant security and civil liberties concerns. For example, as recent headline-making government data breaches ranging from the Office of Personnel Management to the Internal Revenue Service have shown, substantial caches of personal information are consistently inadequately protected when in government hands and subject to an increasing number of data breaches.⁷ Moreover, while anonymous speech

² *Id.*; FBI, *FBI Announces Biometrics Suite's Full Operational Capability*, 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>.

³ *FBI's Next Generation Identification Biometrics Database*, ELECTRONIC FRONTIER FOUNDATION (Sept. 7, 2016), <https://www.eff.org/foia/fbis-next-generation-identification-biometrics-database>.

⁴ NGI SORN at 27,285; Richard W. Vorder Bruegge, *Facial Recognition and Identification Initiatives*, FBI BIOMETRIC CENTER FOR EXCELLENCE (Sept. 7, 2016), https://www.eff.org/files/filenode/vorder_bruegge-facial-recognition-and-identification-initiatives_0.pdf.

⁵ NGI SORN at 27,285 (describing records maintained in the NGI database, including data maintained relating to civil actions, received from foreign countries or international organizations pursuant to sharing agreements, and logged pursuant to an individual's request or consent, among others); FBI, *NGI Rap Back Service Overview*, NATIONAL COUNCIL OF STATE BOARDS OF NURSING (May 21, 2014), https://www.ncsbn.org/NGI_Rap_Back_Overview_Presentation_for_National_Council_of_State_Boards_of_Nursing_2014_05_21.pdf (a presentation document to this entity explaining the benefits of the NGI Rap-Back service, in which employers voluntarily sign up to collect and submit fingerprints to facilitate ongoing background checks of civil applicants, employees, volunteers, and licensees).

⁶ U.S. Gov't Accountability Office, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, GAO (May 16, 2016), <http://www.gao.gov/products/GAO-16-267>.

⁷ *Thales: U.S. Federal Government Agencies Experience More Than 20% Increase in Data Breaches*, CISION (Feb. 22, 2018, 3:00 PM), <https://www.prnewswire.com/news-releases/thales-us-federal-government-agencies-experience-more-than-20-increase-in-data-breaches-300602532.html>. See also Herb Weisbaum, *Data Breaches Happening at Record Pace, Report Finds*, NBC (July 24, 2017, 10:18 AM), <https://www.nbcnews.com/business/consumer/data-breaches-happening-record-pace-report-finds-n785881> (reporting a 29% increase in the number of data breaches in the U.S. overall in the first half of 2017); Riley Walters, *Federal Cyber Breaches in 2017*, THE HERITAGE FOUNDATION (Jan. 3, 2018), <https://www.heritage.org/sites/default/files/2018-01/IB4804.pdf>; Nafeesa Syeed, *White House Report Finds Cybersecurity Gaps at Federal Agencies*, BLOOMBERG (Mar. 10, 2017, 5:02 PM), <https://www.bloomberg.com/news/articles/2017-03-10/white-house-report-finds-cybersecurity-gaps-at-federal-agencies>; Josue Ledesma, *How Big is the U.S. Government Cybersecurity Problem?*, SECURITYSCORECARD INSIGHTS & NEWS (Apr. 14, 2016), <http://blog.securityscorecard.com/2016/04/14/big-us-government-cybersecurity-problem/>.

has long been championed by the Supreme Court as vital to the democratic process,⁸ the pervasive use of biometrics that defines NGI risks infringing these core Free Speech rights of Americans and chilling political expression.

Finally, while existing privacy protections in U.S. law might otherwise moderate some of these risks generated by NGI, the FBI broadly exempts the program from the Privacy Act. The FBI claims NGI's exemption from §§ 552a(c)(3)–(4); (d)(1)–(4); (e)(1)–(3); (e)(4)(G)–(I); (e)(5); and (e)(8)(f)–(g) of the Act, sections which, among other essential protections, provide for limits on collection and promote accountability and accuracy through disclosure requirements.

In light of the privacy concerns raised by collection of the sensitive personal information of millions of individuals via the FBI's NGI program, transparency in its operation of NGI is vital to maintain trust and accountability.

The NGI Monthly Fact Sheet for December 2017 is publicly available on the FBI's website.⁹ This document details "December 2017 Monthly Statistics," including data such as volume statistics, repository counts, photo counts, and more. These monthly stat sheets provide necessary public transparency regarding the extent of the use of NGI, but only the December 2017 Monthly Fact Sheet is available, and there is no comprehensive repository of prior monthly fact sheets. All such NGI fact sheets should be made public.

Documents Requested

- (1) All Next Generation Identification (NGI) Monthly Fact Sheets from September 2016 to present.

Request for "News Media" Fee Status and Fee Waiver

EPIC is a "representative of the news media" for fee status and waiver purposes.¹⁰ 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.¹¹

Duplication fees should also be waived because the disclosure of these requested documents will "contribute significantly to public understanding of the operations or

⁸ See, e.g., *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995).

⁹ FBI, *Next Generation Identification (NGI) Monthly Fact Sheet: December 2017 Monthly Statistics*, FBI.GOV (Dec. 2017), <https://www.fbi.gov/file-repository/ngi-monthly-fact-sheet/view>.

¹⁰ *EPIC v. Dep't of Def.*, 241 F. Supp. 2d 5 (D.D.C. 2003).

¹¹ 5 U.S.C. § 552(a)(6)(E)(v)(II) (2008); *Al-Fayed v. CIA*, 254 F.3d 300, 306 (D.C. Cir. 2001).

activities of the government.”¹² As a request for disclosure of FBI operational information, the requested documents of the FBI concern “the operations or activities of the government.”¹³ Further, these documents are “likely to contribute significantly to public understanding of those operations or activities,”¹⁴ by developing the public’s comprehension of the policies and processes involved in the FBI’s NGI program. Additionally, the requested documents are of interest to the large numbers of the public who may be affected by the program’s monitoring, whether directly as a subject or indirectly, as an employer for example. Transparency in the program also is of interest to American citizens generally, who have a stake in preserving accountable, open government institutions. Thus, these requested documents would “contribute to a reasonably broad audience of persons interested in the subject,” although the agency “shall [] presume[] that a representative of the news media will satisfy this consideration.”¹⁵

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,

Jeramie D. Scott
EPIC National Security Counsel

Sara Wolovick
EPIC Legal Clerk

¹² § 552(a)(4)(A)(iii).

¹³ See 28 C.F.R. § 16.10(k)(1)(i).

¹⁴ § 16.10(k)(2)(ii).

¹⁵ See 28 C.F.R. § 16.10(k)(2)(ii)(B).