June 23, 2016

Senator Chuck Grassley, Chairman
Committee on the Judiciary
437 Russell Senate Office Building
Washington, DC 20510

Senator Patrick J. Leahy, Ranking Member
Committee of the Judiciary
437 Russell Senate Office Building
Washington, DC 20510

Congressman Bob Goodlatte, Chairman
Committee on the Judiciary
2138 Rayburn House Office Building
Washington, DC 20515

Congressman John Conyers, Ranking Member
Committee on the Judiciary
2138 Rayburn House Office Building
Washington, DC 20515

Congressman Jason Chaffetz, Chairman
Committee on Oversight and Government Reform
2157 Rayburn House Office Building
Washington, DC 20515

Congressman Elijah Cummings, Ranking Member
Committee on Oversight and Government Reform
2157 Rayburn House Office Building
Washington, DC 20515

Re: The FBI's Use of Facial Recognition and Proposal to Exempt the Bureau's Next Generation Identification Database from Privacy Act Obligations

Dear Senators Grassley and Leahy and Representatives Goodlatte, Chaffetz, Conyers, and Cummings:

Thank you for your continued oversight of the Federal Bureau of Investigation ("FBI") programs that impact the privacy, civil liberties, and human rights of Americans and lawful permanent residents. Oversight hearings promote transparency and accountability and help ensure that the FBI fulfills its mission while upholding American values and constitutional freedoms.

We, the undersigned privacy, transparency, civil rights, human rights, and immigrant rights organizations, write today to bring your attention to the FBI's recent proposal to exempt the Bureau's massive biometric database known as Next Generation Identification ("NGI") from the protections provided by the Privacy Act of 1974, and the FBI's extensive use of facial recognition technology without proper oversight. We urge you to hold an oversight hearing on the NGI program and the FBI's use of biometric data.

NGI is a massive biometric database that was launched in 2008 and went fully operational in Fall 2014.[1] The database contains the biometric data on millions of US citizens

[1] FBI Press Release, *FBI Announces Full Operational Capability of the Next Generation Identification System* (Sept. 15, 2014), https://www.fbi.gov/news/pressrel/press-releases/fbi-announces-full-operational-capability-of-the-next-generation-identification-system.

and immigrants.[2] NGI incorporates numerous biometrics including fingerprints, facial recognition, and iris recognition.[3] The database contains profiles on arrestees and people with records as well as individuals with no connection to the criminal justice system, and NGI is used for both law enforcement and non-law enforcement purposes.[4] Through NGI's Interstate Photo System ("NGI-IPS"), the FBI runs a face recognition service with over 30 million photos from 16.9 million individuals that is accessed by various state and local law enforcement agencies.[5]

Additionally, the FBI has agreements with 16 states to request facial recognition searches of state repositories of photos consisting mostly of driver license photos.[6] From 2011 to 2015, the FBI ran over 36,000 facial recognition searches of *well over 170 million driver's license photos* – photos of law-abiding drivers unconnected to the criminal justice system.[7] The FBI is currently negotiating with 18 other states to include their driver's license photos in these searches.[8] All of these searches have been conducted without any judicial oversight or internal audits.

Per the Systems of Record Notice, NGI will collect personal information, including biometric data, for the purposes of employment, licensing, military service, volunteer service, background checks, immigration benefits, lawful detention, criminal inquiries, or civil law violations, and through sharing agreements with foreign countries or international organizations.[9] The default retention of these records is until the individual turns 110 years old or seven years after the FBI has been notified of the individual's death regardless of whether the original purpose for the collection has come to an end or not.[10]

The FBI is unnecessarily retaining vast amounts of personal and biometric information and exposing millions of people to a potential data breach. In light of the increasing number of data breaches, and in particular the Office of Personnel Management's data breach, there is no excuse for unnecessarily retaining personal information on millions of people. Biometric data cannot be changed if it is compromised. The collecting of biometric data raises numerous

---

[2] FBI, *Next Generation Identification (NGI) Monthly Fact Sheet* (Dec. 2015), https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi/december-2015-ngi-fact-sheet.pdf.
[3] FBI, *Next Generation Identification*, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi.
[4] *See Id*.
[5] GAO, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, 10 (May 2016).
[6] *Id.* at 50. The FBI also recently ran a pilot to run facial recognition searches on the vast repository of passport photos maintained by the State Department. GAO, F*ace Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, 48 (May 2016).
[7] *Id.* at 47-49.
[8] *Id.* at 50.
[9] Notice of Privacy Act System of Records, 81 Fed. Reg. 27284, 27284-85 (May 5, 2016) (Notice of Privacy Act System of Records modified extension, 81 Fed. Reg. 36350 (June 6, 2016)).
[10] *See* Privacy Impact Assessment for the Next Generation Identification (NGI) Interstate Photo System, § 3.4 (Sept. 15, 2015), https://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system; *see also* Privacy Impact Assessment Next Generation Identification (NGI) – Retention and Searching of Noncriminal Justice Fingerprint Submissions, § 3.4 (Feb. 20, 2015).

privacy and civil liberties issues. For many communities, it also raises serious religious concerns.[11]

The collection of biometric data on millions of people gives law enforcement the ability to identify individuals without probable cause, reasonable suspicion, or any other legal standard that might otherwise be required for law enforcement to obtain traditional identification. Through the use of biometric identifiers like facial recognition, law enforcement can covertly and remotely identify people on a mass scale.

The FBI has a unit dedicated to the use of facial recognition. The Facial Analysis, Comparison, and Evaluation ("FACE") Services Unit "receives facial probe images from the field, conducts a face search of all available facial recognition (FR) systems, and provides results back to the requesting agent."[12] Furthermore the FBI's Biometric Center of Excellence continues to explore "the use of new and enhanced biometric technologies and capabilities for integration into operations"[13] with minimal transparency.

The FBI's use of facial recognition through NGI and its FACE Services Unit lacks proper public oversight. A recent GAO report determined that the "FBI has not completed audits to oversee the use of NGI-IPS or FACE services."[14] The GAO report concluded that "without conducting audits to determine whether users are conducting face image searches in accordance with CJIS policy requirements, FBI officials cannot be sure they are implementing face recognition capabilities in a manner that protects individuals' privacy."[15] Furthermore, the FBI has failed to timely update the public through Privacy Impact Assessments required by law.[16] These privacy assessments are essential to informing the public on how the FBI mitigates the privacy risks associated with its information systems.[17]

Congress often holds oversight hearings of the FBI, but more often than not the FBI's NGI database and its use of biometrics receives too little scrutiny. The last time NGI and specifically the FBI's use of face recognition were a predominant focus of a congressional hearing was in July 2012 before the Senate Judiciary subcommittee on Privacy, Technology and

---

[11] Many individuals have significant religious objections to the collection, retention, and/or sharing of their biometric data.
[12] Standard Operating Manual: Facial Analysis, Comparison, and Evaluation (FACE) Service Unit (Version 1.0 Apr. 9, 2013), https://epic.org/foia/fbi/faces/FBI-SOP-FACES-Unit.pdf.
[13] FBI, *Biometric Center of Excellence*, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/.
[14] GAO, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, 23 (May 2016), http://www.gao.gov/assets/680/677098.pdf.
[15] *Id.* at 33.
[16] *Id.* at 18-19.
[17] *See* DOJ Office of Privacy and Civil Liberties, *Privacy Impact Assessments: Official Guidance*, 4 (Revised July 2015), https://www.justice.gov/opcl/file/631431/download.

the Law.[18] In his statement for the record, Senator Franken expressed the risks of the use of facial recognition by the FBI without proper oversight, stating:

> I fear that the FBI pilot could be abused to not only identify protestors at political events and rallies, but to target them for selective jailing and prosecution, stifling their First Amendment rights . . . . I also fear that without further protections, facial recognition technology could be used on unsuspecting civilians innocent of any crime—invading their privacy and exposing them to potential false identifications.[19]

The risks of NGI and the large-scale collection, use, retention, and sharing of biometrics are well understood by the privacy and civil liberties community. Because of these risks, public interest organizations have repeatedly called for the review of NGI.[20] In 2011, 70 organizations urged the Inspector General of the Department of Justice to investigate the privacy and civil liberties implications of the FBI's NGI program.[21] In 2014, as NGI neared full operational capacity, a coalition of civil liberties groups urged Attorney General Eric Holder to review the NGI program and release an updated Privacy Impact Assessment as a first step to robust review of the program.[22] Since that letter, NGI has gone fully operational with minimal oversight.

Most recently a coalition of public interest organizations called upon the Department of Justice to extend the public comment period for the FBI's proposal to exempt NGI from many of the most important protections provided by the Privacy Act of 1974.[23] The letter urged more time to "allow the public the opportunity for a careful, step-by-step examination of both the NGI System of Records Notice and the FBI's proposal to render that system largely secret."[24]

In a public interest case against the FBI, U.S. District Judge Tanya Chutkan stated, "There can be little dispute that the general public has a genuine tangible interest in a system

---

[18] *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. (2012).
[19] *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. 2 (2012) (statement for the record of Senator Al Franken).
[20] EPIC previously called for a congressional hearing on FBI's NGI database. Letter from EPIC to Senators Chuck Grassley and Patrick Leahy (Jan. 9, 2015), https://epic.org/foia/fbi/ngi/EPIC-to-SJC-re-NGI.pdf.
[21] Letter from Coalition of Civil Liberties groups to Cynthia A. Schnedar, DOJ Acting Inspector General (Sept. 11, 2011), https://epic.org/privacy/secure_communities/DOJ-S-Comm-Letter.pdf.
[22] Letter from Coalition of Civil Liberties groups to Eric Holder, U.S. Attorney General (June 24, 2014), https://www.privacycoalition.org/Ltr-to-Review-FBI-NGI-Program.pdf.
[23] Letter from Coalition of Civil Liberties groups to Erika Brown Lee, DOJ Chief Privacy and Civil Liberties Officer (May 27, 2016), https://epic.org/privacy/fbi/coalition-letter-urges-public-comment-extension-on-NGI.pdf.
[24] *Id.*

designed to store and manipulate significant quantities of its own biometric data, particularly given the great numbers of people from whom such data will be gathered."[25]

We urge the Committees to take up this issue as soon as possible and hold oversight hearings to assess the privacy, civil liberties, and human right issues raised by the FBI's massive biometric database and the Bureau's use of facial recognition technologies to search its own database, other federal department databases, and databases of state driver's license photos. We also urge the committees to require the FBI's compliance with the Privacy Act of 1974 and ensure ongoing public reports on the FBI's use, collection, retention, and disclosure of biometric data.

Sincerely,

18MillionRising.org
Advocacy for Principled Action in Government
American-Arab Anti-Discrimination Committee
American Civil Liberties Union
American Library Association
Amnesty International USA
Arab American Institute
Asian Americans Advancing Justice - Asian Law Caucus
Bill of Rights Defense Committee/Defending Dissent Foundation
Center for Democracy & Technology
Center for Digital Democracy
Center for Financial Privacy and Human Rights
Center for Media Justice
Center on Privacy & Technology at Georgetown Law
ColorOfChange.org
Constitutional Alliance
The Constitution Project
Consumer Action
Consumer Watchdog
Council on American-Islamic Relations
Cyber Privacy Project
Demand Progress
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Fight for the Future
Free Press Action Fund
Freedom of the Press Foundation
Government Accountability Project

[25] *EPIC v. FBI*, 72 F. Supp. 3d 338, 346 (D.D.C. Nov. 5, 2014). The case was a Freedom of Information Act lawsuit against the FBI for records about the Bureau's NGI database.

Immigrant Legal Resource Center
Media Mobilizing Project
MPower Change
National Association of Criminal Defense Lawyers
National Consumers League
National Day Laborer Organizing Network
National Employment Law Project
National Immigration Law Center
National Immigration Project of the National Lawyers Guild
National LGBTQ Task Force Action Fund
New America's Open Technology Institute
OpenTheGovernment.org
Patient Privacy Rights
Privacy Rights Clearinghouse
Privacy Times
Restore the Fourth
Sunlight Foundation
World Privacy Forum