June 24, 2014

The Honorable Eric H. Holder, Jr.
United States Attorney General
Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

Re: FBI Next Generation Identification System (NGI)

Dear Attorney General Holder,

We write today to urge the Department of Justice (DOJ) to quickly complete an updated Privacy Impact Assessment (PIA) for the Federal Bureau of Investigation's Next Generation Identification System (NGI) as part of a broader effort to examine the goals and impact of NGI. The previous PIA on NGI's face recognition component dates back to 2008.[1] Since that time the program has undergone a radical transformation—one that raises serious privacy and civil liberties concerns.

The FBI recognizes this transformation and, at a July 2012 Senate hearing, committed to updating its privacy assessment of the agency's use of facial recognition.[2] Jerome Pender, Deputy Assistant Director of the FBI's Criminal Justice Information Service Division, stated in his statement for the record that "[a]n updated PIA is planned and will address all evolutionary changes since the preparation of the 2008 IPS PIA."[3] Furthermore, Assistant Director Pender said the updated privacy assessment would have "an emphasis on Facial Recognition."[4] Nearly two years later an updated privacy assessment has not been completed.[5]

PIAs are an important check against the encroachment on privacy by the government. They allow the public to see how new programs and technology utilized by the government affect their privacy and assess whether the government has done enough to mitigate the privacy risks. As the DOJ's own guidelines on PIAs explains, "[t]he PIA also gives the public notice of this analysis

[1] FBI, *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System (IPS)* (June 9, 2008), *available at* http://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system.

[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 for the record of Jerome Pender, Deputy Assistant Director, FBI), *available at* http://www.judiciary.senate.gov/pdf/12-7-18PenderTestimony.pdf.

[3] *Id.*

[4] *Id.*

[5] *See* FBI Response to EPIC FOIA Request (Mar. 19, 2014) (stating the FBI is still drafting the Privacy Threshold Analysis and Privacy Impact Assessment for facial recognition), *available at* http://epic.org/foia/fbi/FBI.Response.PIA.FR.pdf.

and helps promote trust between the public and the Department by increasing transparency of the Department's systems and missions."[6]

The PIA, as the DOJ's guidelines state, is not optional:

> A PIA is an analysis required by the E-Government Act of how information in identifiable form is handled to ensure compliance with applicable legal, regulatory, and policy requirements regarding privacy, to determine the risks and effects of collecting, maintaining, and disseminating such information in an electronic information system, and to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[7]

Additionally, PIAs should be conducted during the development of any new system "with sufficient lead time to permit final Departmental approval and public website posting on or before the commencement of any system operation (including before any testing or piloting.)"[8] The FBI's NGI program has instituted multiple pilots using biometric identifiers including facial recognition and iris recognition without completing a proper privacy assessment.[9] And despite the fact that FBI has so far failed to produce a PIA for NGI, the Bureau has stated it plans for NGI's face recognition component "to be at Full Operating Capacity (FOC) in fiscal year 2014."[10]

The capacity of the FBI to collect and retain information, even on innocent Americans, has grown exponentially. It is essential for the American public to have a complete picture of *all* the programs and authorities the FBI uses to track our daily lives, and an understanding of how those programs affect our civil rights and civil liberties.

The FBI's NGI system is a massive biometric database that includes iris scans, palm prints, and face recognition. NGI builds on the Integrated Automated Fingerprint Identification System, the FBI's legacy fingerprint database, which already contains well over 100 million individual records—equal to nearly one third of the U.S. population.[11] NGI combines these biometric data in each individual's file, linking them to personal and biographic information like name, home address, ID number, immigration status, age, race, etc. This immense database is shared with other federal agencies and with the approximately 18,000 tribal, state and local law enforcement agencies across the United States.

[6] OPCL DOJ, Privacy Impact Assessments Official Guidance, 3 (Rev. March 2012).

[7] *Id.* (footnotes omitted).

[8] *Id.* at 4.

[9] *See Federal Government Approaches to Issuing Biometrics IDs: Part II: Hearing Before the Subcomm. on Government Operations of the H. Comm. on Oversight & Government Reform*, 113th Cong. 4 (2013) (statement for the record of Steve M. Martinez, Executive Assistant Director Science and Technology Branch Federal Bureau of Investigation), *available at* http://oversight.house.gov/wp-content/uploads/2013/06/Martinez-Testimony-Final.pdf..

[10] *See* FBI record released in response to EFF FOIA Request, *Interstate Photo System Face Recognition Operational Prototype Project Plan*, CJIS Document Number - NGI-DOC-27239-2.0, 1 (Sept. 28, 2011) *available at* https://www.eff.org/document/fbi-ngi-2011-face-recognition-operational-prototype-plan.

[11] *See* Jennifer Lynch, *FBI Ramps Up Next Generation ID Roll-Out—Will You End Up in the Database?*, EFF (Oct. 19, 2011) https://www.eff.org/deeplinks/2011/10/fbi-ramps-its-next-generation-identification-roll-out-winter-will-your-image-end.

The facial recognition component of NGI poses real threats to privacy for all Americans, and could, in the future, allow us to be monitored and tracked in unprecedented ways.[12] NGI will include criminal and non-criminal photos, and the FBI projects that by 2015, the database could include as many as 52 million face images.[13] 4.3 million of those would be taken for non-criminal purposes, such as employer background checks. It appears FBI plans to include these non-criminal images every time a law enforcement agency performs a criminal search of the database.[14]

According to an FBI study, the quality of images in the database is inconsistent and often of low resolution.[15] Partly for this reason, the FBI doesn't promise accuracy in its search results. Instead, it ensures only that "the candidate will be returned in the top 50 candidates" 85% of the time "when the true candidate exists in the gallery."[16] In fact, the overwhelming number of matches will be false. This false-positive risk could result in even greater racial profiling by disproportionately shifting the burden of identification onto certain ethnicities. The false-positive risk can also alter the traditional presumption of innocence in criminal cases by placing more of a burden on the suspect to show he is not who the system identifies him to be. And this is true even if a face recognition system such as NGI offers several results for a search instead of one, because each of the people identified could be brought in for questioning, even if he or she has no relationship to the crime.[17]

The use of facial recognition technology allows the government to track Americans on an unprecedented level. Despite FBI statements to the media that NGI will merely be a mug shot database, the Bureau's plans for its face recognition capabilities are much broader. According to an FBI presentation on facial recognition and identification initiatives at a biometrics conference in 2010, one of the FBI's goals for NGI is to be able to track people as they move from one location to another.[18]

The extensive collection and sharing of biometric data at the local, national, and international level raises significant concerns for Americans. Data accumulation and sharing can be good for solving crimes across jurisdictions or borders, but can also perpetuate racial and ethnic profiling, social stigma, and inaccuracies throughout all systems and can allow for government tracking and surveillance on a level not before possible.

[12] "The FBI's Next Generation Identification Program: Big Brother's ID System?" Electronic Privacy Information Center, December 2013, *available at* http://epic.org/privacy/surveillance/spotlight/ngi.html.

[13] Jennifer Lynch, "FBI Plans to Have 52 Million Photos in its NGI Face Recognition Database by Next Year." Electronic Frontier Foundation, April 14, 2014*, available at* https://www.eff.org/deeplinks/2014/04/fbi-plans-have-52-million-photos-its-ngi-face-recognition-database-next-year.

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] *What Facial Recognition Technology Means for Privacy and Civil Liberties: hearing before the S. Committee on the Judiciary Subcommittee of Privacy, Technology, and the Law*, 112th Congress (2012) (statement of Jennifer Lynch, Electronic Frontier Foundation), *available at* https://www.eff.org/files/filenode/JenniferLynch_EFF-Senate-Testimony-Face_Recognition.pdf.

[18] Richard W. Vorder Bruegge, Federal Bureau of Investigation, *Facial Recognition and Identification Initiatives*, (pdf, pp. 4-5), *available at* http://biometrics.org/bc2010/presentations/DOJ/vorder_bruegge-Facial-Recognition-and-Identification-Initiatives.pdf; Biometric Consortium Conference, September 21-23, 2010, Program, *available at* http://www.biometrics.org/bc2010/program.pdf.

Given the serious and wide ranging scope of NGI we urge the Department to review the goals of the program and ensure that information collection is solely of individuals who are part of the criminal justice system and does not become a tool for surveillance of innocent Americans. Completion of a comprehensive Privacy Impact Assessment is the first step of what we hope will be a robust assessment and review.

Sincerely,

American Civil Liberties Union
Bill of Rights Defense Committee (BORDC)
Brennan Center for Justice
Center for Digital Democracy
Center for Democracy & Technology
Center for Financial Privacy and Human Rights
Center for National Security Studies
The Constitution Project
Constitutional Alliance
Consumer Action
Consumer Federation of America
Consumer Watchdog
Council on American-Islamic Relations
Council for Responsible Genetics
Cyber Privacy Project
Defending Dissent Foundation
Demand Progress
DownsizeDC.org
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Friends of Privacy USA
Government Accountability Project
Liberty Coalition
NAACP
National Association of Criminal Defense Lawyers
National Urban League
OpenTheGovernment.org
Patient Privacy Rights
Privacy Rights Clearinghouse
Privacy Times
R Street Institute
World Privacy Forum

cc: Erika Brown Lee
DOJ Chief Privacy and Civil Liberties Officer

Senator Al Franken, Chairman
U.S. Senate Subcommittee on Privacy, Technology and the Law

Senator Jeff Flake, Ranking Member
U.S. Senate Subcommittee on Privacy, Technology and the Law