The American-Arab Anti-Discrimination Committee

Comments to the

U.S. Department of Justice
Privacy & Civil Liberties Office

on the

Federal Bureau of Investigation (FBI) Implementation of the Next Generation Identification-Interstate Photo System (NGI-IPS) and its Proposed Exclusion from Certain Provisions of the Privacy Act of 1974

Yolanda Rondon, Esq., ADC Staff Attorney
American-Arab Anti-Discrimination Committee
1990 M Street NW Suite 610
Washington, DC 20036
Phone: (202) 244-2990
Fax: (202) 333-3980
E-mail: legal@adc.org
Web: www.adc.org

CPCLO Order NO. 003-2016
DOJ FRDOC 0001-0173
DOJ-OPCL-2016-0008-0001
81 FR 27288

July 6, 2016

VIA ELECTRONIC EMAIL

Ms. Erika Brown Lee
Attn: Privacy Analyst
U.S. Department of Justice
Privacy & Civil Liberties Office
National Place Building
1331 Pennsylvania Ave. NW, Suite 1000
Washington, D.C. 20530-0001

RE: Concerns Regarding the FBI's Implementation of the NGI-IPS and its Proposed Exemption from Vital Provisions of the Privacy Act of 1974

Dear Ms. Lee:

I am writing to you on behalf of the American-Arab Anti-Discrimination Committee (ADC), the country's largest Arab-American organization. Founded in 1980 by U.S. Senator James Abourezk, ADC consists of members from all 50 states and has multiple chapters nationwide. ADC is committed to protecting civil rights, promoting mutual understanding, and preserving Arab cultural heritage. ADC has protected the Arab-American community's civil rights for over thirty-five years against discrimination, racism, and stereotyping. ADC has a standing commitment to protecting the Arab-American community's constitutional rights and right to privacy. ADC respectfully takes this opportunity to address the Department of Justice regarding its proposed rulemaking to exempt the FBI's utilization of the Next Generation Identification-Interstate Photo System (NGI-IPS) from essential provisions of the Privacy Act of 1974 in addition to the agency's disturbing disregard and blatant negligence of the system's lack of accuracy which targets minority communities and puts citizens' privacy rights at risk.

NGI-IPS Concerns

ADC has serious concerns about NGI-IPS and the FBI's proposal to exclude its vast system of various biometrics from key provisions of the Privacy Act of 1974. Since 2008, the FBI has been collecting biometric information belonging to millions of American citizens. This collection of biometric data includes fingerprints, iris scans, palm prints, facial recognition, and other materials retrieved not only during arrests, but for non-criminal purposes like immigration purposes from U.S. Department of State database, background checks like with the U.S. Department of Defense, and

drivers' licenses.[1] Although the system utilizes some of the most advanced technology in order to more quickly identify criminals, it is deeply flawed in that it has been implemented in a secretive and nontransparent manner which threatens the protections of the Privacy Act, provides results lacking in accuracy, and disproportionately targets minority populations.[2]

While our national security and the FBI's dedication to preventing, prosecuting, and determining crimes is of absolute importance, the FBI's proposal utilizes the premise of national security as a façade which shields its violation of the American citizen's right to privacy and First Amendment protections.

Dismissal of Protections Granted by the Privacy Act

In its proposed rulemaking, the FBI seeks to exempt NGI from Privacy Act protections which allow people to find out whether they are in NGI database, whether their profile has been shared with other parts of the government, and whether their profile is accurate or incorrect.

The FBI has requested exemption from several subsections of 5 U.S.C. § 552a(e), including those which require: maintenance of only material that is relevant in order to accomplish the purpose of the agency; collecting information directly from an individual when it may result adversely determine their rights, benefits, or privileges under federal programs; inform the person from whom it seeks information of their authority, purpose, routine, and effects; publishing in the Federal Register the categories of sources as well as agency procedures where someone may request to be notified if the agency has a record about him; and notifying someone when their information is shared with another person or government agency. The implications of these exemptions are deeply troubling and infringe upon the essence of the Privacy Act itself – to ensure that American citizens are protected and allowed to live life as they wish.

ADC has serious concerns that the FBI seeks to exempt NGI from 5 U.S.C. § 552a(g), which provides U.S. citizens with the right to due process and/or enforcement of a Privacy Act violation. Under the FBI's proposal, the FBI could violate rules like 5 U.S.C. § 552a(e)(7), which largely bars

[1] Sam Thielman, *FBI using vast public photo data and iffy facial recognition tech to find criminals* , THE GUARDIAN,, June 15, 2016, https://www.theguardian.com/us-news/2016/jun/15/fbi-facial-recognition-software-photo-database-privacy; *see also* Coalition Letter Request for Oversight Hearing to Senators Grassley and Leahy and Representatives Goodlatte, Chaffetz, Conyers, and Cummings, The FBI's Use of Facial Recognition and Proposal to Exempt the Bureau's Next Generation Identification Database from Privacy Act Obligations, dated June 23, 2016, https://epic.org/privacy/fbi/NGI-Congressional-Oversight-Letter.pdf.

[2] *See* Coalition Letter to FBI Requesting More Time to Respond to Proposed Privacy Act Exemptions for Next Generation Identification, dated May 27, 2016, https://www.eff.org/document/2016-letter-fbi-re-NGI.

the government from creating databases about the political activities of American citizens, without any accountability because the person has not notice or substantive way to discover the violation and dispute its use. If this were to pass, private citizens could never take the government to court and there would be no accountability. Exemptions are necessary in certain circumstances, but they should not make the Privacy Act and the protections it provides completely moot.

ADC is alarmed that the FBI has created a centralized database of biometrics, especially where the FBI is exposing millions of citizens to potential data breach by retaining masses of pieces of this personal identifying information. Biometrics cannot be changed; millions of people cannot change their fingerprints, facial structure, or irises. Data breaches are becoming increasingly common, an important example being when the Office of Personnel Management was breached in June 2015.[3] By keeping far more information than it could possibly need in a surely congested and far too expansive system, the FBI hinders its own investigations and the privacy rights of American citizens.

Exemptions to these protections are justified in certain circumstances, and it is understandable that the FBI cannot be fully transparent as it conducts its law enforcement duties. However, to completely bar people from accessing their records and preventing them from correcting inaccurate data is concerning, as that means people would no longer be able to know what information the FBI has about them, and whether that information is correct. There is no accountability with such a policy, and the FBI would be free to collect any information – correct or incorrect, civil or criminal, legal or illegal – that it wishes.

Lack of Accuracy

While the FBI argues that it is impossible to ensure that all of the information included in NGI system is accurate, the consequences of such a policy are worrisome. Inaccurate information may victimize innocent American citizens, and the prospect of erroneous allegations circulating between agencies with no recourse or burden for the agency responsible goes against what our laws endeavor to protect.

In 2013, 50% of the FBI's criminal records failed to include information on the final outcome of a case. This means that it is quite possible that many records of cases where a person was proven

[3] *See* Coalition Letter Request for Oversight Hearing to Senators Grassley and Leahy and Representatives Goodlatte, Chaffetz, Conyers, and Cummings, *supra* note 1.

innocent or never even charged at all do not indicate the innocence of that person. If an arrest record indicates only an arrest but not the final conviction, an innocent person is quite likely to be falsely perceived as a criminal. A recent investigation shows that on a yearly basis thousands of people undergoing fingerprint-based background checks cannot secure work due to inaccurate FBI records.

While the FBI has stated that civil photos will be separate from criminal photos in the database, citizens' First Amendment rights could be threatened nonetheless. In certain instances, like if someone is arrested during a protest, civil photographs will be combined with one's criminal record. Furthermore, as the FBI has shared, at least 15% of the time NGI may produce a false match and implicate a person as a suspect in a crime that they did not commit. The FBI has not properly established safeguards to ensure that search results do not display non-criminal offenders - innocent people. The FBI has only conducted limited testing which is not nearly enough to establish sufficient accuracy.

Targeting of Minority Populations

NGI does not affect everyone equally. It is incredibly likely that it targets minority populations such as immigrant, Latino, and African American communities. Research indicates that some of NGI's biometric identifying capabilities, like facial recognition, possibly incorrectly analyze African Americans, young people, and women at higher rates than Caucasians, elders and men.4 Furthermore, due to disproportionately high arrest rates, a large amount of people affected by the FBI's inaccurate or out of date records are people of color.

Facial recognition technology is known for being flawed in its recognition – or lack thereof – of brown and black populations. In 2015, Google Photos faced huge backlash when its software identified black people as gorillas despite accurately identifying objects such as skyscrapers and airplanes or ceremonies like graduation.[5] In another instance, a camera misinterpreted smiling Asian eyes as blinking.[6] In 2010, HP computers had webcams that would recognize as human and follow

[4] Jennifer Lynch, *New Report: FBI Can Access Hundreds of Millions of Face Recognition Photos*, June 15, 2016, https://www.eff.org/deeplinks/2016/06/fbi-can-search-400-million-face-recognition-photos.
[5] Charles Pulliman Moore, *Google Photos identified black people as 'gorillas,' but racist software isn't new*, June 11, 2016, http://fusion.net/story/159736/google-photos-identified-black-people-as-gorillas-but-racist-software-isnt-new/.
[6] Adam Rose, *Are Face-Detection Cameras Racist?*, TIME, Jan. 22, 2010, http://content.time.com/time/business/article/0,8599,1954643,00.html .

white subjects but not black subjects, and in 2015 Flickr released tagging software that labeled a black man and white woman as apes.[7]

While the FBI has stated that NGI will be used to provide a list of suspects rather than positively identify anyone, ADC is still concerned given that someone conducting a search can request a listing anywhere between 2 to 50 subjects. There is still a chance that an non-criminal offender – an innocent person will be listed as a possible suspect, and even more so, the utilized technology may more likely incriminate a person of color.[8]

Lack of Transparency

ADC is disturbed with the lack of transparency in this rulemaking, indicative of the FBI's pattern of practice and disregard to the abrogation U.S. citizens rights' without their knowledge. The Privacy Act requires a Systems of Records Notice (SORN) and/or a Privacy Impact Assessment (PIA), which must be published when the FBI creates or significantly changes any database that collects and utilizes American citizens' personal information.

When the FBI began working on this system in 2008, it released a PIA, but that PIA was not updated until late 2015 after major changes, more than half a decade later. The FBI also did not release a PIA about the facial recognition technology until 2015, or three years after starting to use the technology. The FBI did not release a relevant SORN until May 2016. When the FBI finally did, it requested that the system be exempted from certain parts of the Privacy Act and initially only allowed 21 days for groups to review its request for exemption.[9] The FBI failed to give public notice through updated PIAs of the privacy implications of its program and to protect the privacy protections Americans are entitled to possess.

Additionally, the FBI has been secretive about its future plans for NGI. In a 2012 congressional testimony, a FBI official stated NGI would only utilize criminal mug shot photos – but the FBI indicated in 2015 that it planned to allow law enforcement officers to submit data from the field such as fingerprints, iris scans, and face recognition directly to NGI.[10] Furthermore, the FBI

---

[7] *See* Jenna McLaughlin, The Use of FBI's Facial Recognition Is Growing, Despite Rampant Inaccuracy and Privacy Concerns, The Intercept, June 16, 2016, https://theintercept.com/2016/06/16/audit-criticizes-fbi-facial-recognitions-poor-privacy-protections-accuracy/.
[8] Daniel Rivero, *The FBI wants to exempt its next-level policing software from public scrutiny*, June 1, 2016, http://fusion.net/story/308680/fbi-policing-software-privacy/.
[9] *Id.*
[10] Jennifer Lynch, FBI Wants to Remove Privacy Protections from its Massive Biometrics Database, May 31, 2016, https://www.eff.org/deeplinks/2016/05/fbi-ngi-privacyact.

indicated in a 2010 presentation that it was interested in using the system to follow movements to and from "critical events", to identify people in "public datasets," and to utilize photos to determine "unknown persons of interest".[11]

A powerful system containing millions of pieces of personal data requires a checks-and-balances system. A database containing the personal biometrics of millions of citizens grants to the FBI the limitless power to identify individuals without probable cause, reasonable suspicion, or any other legal standard otherwise obligatory under law. However, the FBI's elusive actions indicate that it is moving in the opposite direction, one of secrecy and vast authority, namely without any clear restraints on use and sharing of this biometrics data, and substantive oversight. The FBI seeks to exempt its system from the right given by the Privacy Act to Americans to see what information about them the government possesses. Given that NGI has millions of pieces of biometric data, a number of which belong to citizens who have not been convicted or involved with any sort of crime, and it is impossible that all people within the system will be investigated. The FBI already excludes portions of information from the Privacy Act based on nine exemptions. The FBI should thus allow those who are not under investigation to access their files as citizens have the right to know what the government knows about them. By doing so, people will be able to practice their right to correct any inaccurate information the FBI may possess about them.

Conclusion

ADC is deeply concerned about the FBI's proposed rulemaking to exempt NGI-IPS from certain provisions of the Privacy Act. Based on the above, ADC request that the NGI-IPS not to be exempt under the designated Privacy Act provisions, and that the NGI-IPS system not be implemented and utilized.

Respectfully submitted,

Yolanda C. Rondon, Esq.
Staff Attorney, Legal & Policy Department
American-Arab Anti-Discrimination Committee

[11] *Id.*