epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

May 1, 2017

Senator Chuck Grassley, Chairman
Senator Dianne Feinstein, Ranking Member
United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510-6050

Dear Chairman Grassley and Ranking Member Feinstein:

We write to you regarding the upcoming hearing on "Oversight of the Federal Bureau of Investigation."[1] EPIC respectfully requests, once again, that you to ask the FBI Director about the Next Generation Identification ("NGI") systems, which is quickly becoming one of the largest biometric databases in the world. EPIC has pursued FOIA litigation to promote accountability for the NGI and we have made specific recommendations regarding the protection of privacy for biometric identification systems.[2] EPIC believes that the NGI system raises profound questions of privacy, civil liberties, and security for all Americans.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC participates in a wide range of activities, including research and education, litigation, and advocacy. EPIC is currently pursuing Freedom of Information Act matters related to the FBI's use of facial recognition and other biometric identifiers as part of the FBI's Next Generation Identification program. EPIC has also prepared amicus briefs for the US Supreme Court in cases concerning the civil liberties implications of new investigative techniques.[3]

---

[1] *Oversight of the Federal Bureau of Investigation*, 115th Cong. (2017), S. Comm. on the Judicary, https://www.judiciary.senate.gov/meetings/05/03/2017/oversight-of-the-federal-bureau-of-investigation (May 3, 2017).

[2] *See EPIC v. FBI*, No. 2013 -cv- 00442 (D.D.C. Nov. 5, 2014), http://epic.org/foia/fbi/ngi/; Comments of EPIC to Federal Bureau of Investigation, *Privacy Act of 1974; Systems of Record Notice of a Modified System of Records Notice* (July 6, 2016), https://epic.org/apa/comments/EPIC-CPCLO-FBI-NGI-Comments.pdf.

[3] Brief of *Amicus Curiae* EPIC, *Riley v. California*, 573 U.S. ___ (2014), https://epic.org/amicus/cell-phone/riley/; Brief of *Amicus Curiae* EPIC, *Maryland v. King*, 569 U. S. ___ (2013), https://epic.org/amicus/dna-act/maryland/EPIC-Amicus-Brief.pdf; Brief of *Amicus Curiae* EPIC, *Florida v. Harris*, 568 U. S. ___ (2013), https://epic.org/amicus/harris/EPIC-Amicus-Brief.pdf; Brief of *Amicus Curiae* EPIC, *U.S. v. Jones,* 565 U. S. ___ (2012), https://epic.org/amicus/jones/EPIC_Jones_amicus_final.pdf.

In 2014, EPIC prevailed in a Freedom of Information Act (FOIA) case against the FBI concerning the NGI program.[4] EPIC had sought information about the reliability and accuracy of the database system maintained by the FBI. In finding for EPIC's public interest claim, U.S. District Judge Tanya Chutkan stated:

> There can be little dispute that the general public has a genuine, tangible interest in a system 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.[5]

The documents EPIC obtained in this FOIA lawsuit showed that the FBI accepted a twenty percent error rate for the facial recognition technology used with NGI.[6] Through a previous FOIA request, EPIC obtained numerous agreements between the FBI and state DMVs that allowed the FBI to use facial recognition to compare subjects of FBI investigations with the millions of license and identification photos retained by participating state DMVs.[7]

More recently, EPIC obtained nearly two years of monthly stat sheets for NGI. These documents revealed that the FBI's use of facial recognition searches is increasing.[8] The NGI monthly stat sheets also showed that the NGI database is now predominantly used for non-criminal purposes.[9] The FBI has stated in the past that the Bureau does not run facial recognition searches using the civilian data in NGI, but there is currently no legal requirement preventing the FBI from reversing this position—and doing so without informing the public. EPIC is currently litigating a FOIA lawsuit for the Bureau's biometric agreements with the Department of Defense. Through that FOIA lawsuit, EPIC obtained several agreements between the FBI and DoD and one that included that State Department that detailed the dissemination of biometric data between the agencies.[10]

The GAO's recent report on the FBI's use of facial recognition underscores the need for NGI oversight.[11] The GAO report detailed the FBI's failure to conduct a privacy audit of the agency's use of facial recognition or adequately test the accuracy of the technology.[12]

---

[4] *EPIC v. FBI*, No. 2013 -cv- 00442 (D.D.C. Nov. 5, 2014).
[5] *Id.* at 10.
[6] DEPT. OF JUSTICE, FEDERAL BUREAU OF INVESTIGATION, NEXT GENERATION IDENTIFICATION (NGI) SYSTEM REQUIREMENTS DOCUMENT VERSION 4.4 at 244 (Oct. 1, 2010), https://epic.org/foia/fbi/ngi/NGI-System-Requiremets.pdf.
[7] *FBI Performs Massive Virtual Line-up by Searching DMV Photos*, EPIC (June 17, 2013), https://epic.org/2013/06/fbi-performs-massive-virtual-l.html.
[8] FEDERAL BUREAU OF INVESTIGATION, NEXT GENERATION IDENTIFICATION MONTHLY FACT SHEETS (Nov. 2014 – Aug. 2016), *available at* http://epic.org/foia/fbi/EPIC-16-09-08-FBI-FOIA-20161219-NGI-Monthly-Fact-Sheets.pdf.
[9] *Id.*
[10] *EPIC v. FBI (Biometric Data Transfer Agreements)*, EPIC, https://epic.org/foia/fbi/biometric-mou/. (The Memorandum of Understanding obtained by EPIC via FOIA request is available at https://epic.org/foia/fbi/biometric-mou/16-cv-02237-FBI-Biometric-MOUs-FBI-and-DOD.pdf).
[11] U.S. Gov't Accountability Office, GAO-16-267, FACE RECOGNITION TECHNOLOGY: FBI SHOULD BETTER ENSURE PRIVACY AND ACCURACY (2016), http://www.gao.gov/assets/680/677098.pdf.
[12] *Id.* at 33.

The risks of NGI are widely shared in the civil liberties community. In 2011, EPIC, joined by 70 organizations, urged the Inspector General of the Department of Justice to investigate the NGI program.[13] In 2014, as NGI neared full operational capacity, a broad 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.[14] EPIC sent a letter to Congress in January 2015 urging for greater oversight of NGI.[15] Most recently, a coalition of 46 organizations sent a letter to this Committee demanding oversight of the FBI's vast biometric database—NGI.[16]

The increasing use of biometrics, particularly facial recognition, by law enforcement raises substantial privacy, civil liberties, and security risks. Improper collection, storage, and use of this information can result in identity theft, inaccurate identifications, and infringement on constitutional rights. An individual's ability to control access to his or her identity, including determining when to reveal it, is an essential aspect of personal security and privacy. The use of facial recognition technology erodes that ability. The collection of facial images into the FBI's NGI database raises privacy issues because of the surveillance potential of facial recognition, the collection of personally identifiable information into a centralized database, and the prospects of secondary uses of the data. Additionally, facial recognition technology can be done covertly, even remotely, and on a mass scale.

There is little one can do prevent the collection of one's image. Participation in society – working, traveling, shopping, political organizing -- involves exposing one's face. Ubiquitous and near effortless identification eliminates individual's ability to control the disclosure of their identities and poses a special risk to the First Amendment rights of free association and free expression, particularly to those who engage in lawful protests. With the FBI's increasing database of biometrics on civilians, the NGI program could render anonymous free speech, a right well established by the US Supreme Court and central to our nation's founding, virtually impossible.

Justice Sandra Day O'Connor anticipated this problem. In *Arizona v. Evans* she wrote:

> In recent years, we have witnessed the advent of powerful, computer-based recordkeeping systems that facilitate arrests in ways that have never before been possible. The police, of course, are entitled to enjoy the substantial advantages this technology confers. They may not, however, rely on it blindly. With the

[13] 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.
[14] 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.
[15] Letter from EPIC to Sen. Chuck Grassley and Sen. Patrick Leahy, S. Comm. on the Judiciary (Jan. 9, 2015), https://epic.org/foia/fbi/ngi/EPIC-to-SJC-re-NGI.pdf.
[16] Letter from EPIC, Coalition of civil rights, privacy, and transparency groups to S. Comm. on the Judiciary (June 23, 2016), https://epic.org/privacy/fbi/NGI-Congressional-Oversight-Letter.pdf.

benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities.[17]

EPIC again urges the Committee to ask Director Comey about the Next Generation Identification system.

- Are the privacy and security safeguards for NGI adequate?
- Has the specific threat of remote hacking of NGI been assessed?
- Have all the necessary NGI Privacy Impact Assessments been completed?
- Why aren't individuals given the ability to access their own biometric profile which is available to more than one million people across federal, state, and local governments?
- What limitations exist on the use of NGI for non-law enforcement purposes, and specifically for Constitutionally protected activity, such as political rallies?

We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Committee on these issues of vital importance to the American public.

Sincerely,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Jeramie Scott
Jeramie Scott
EPIC National Security Counsel

/s/ Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Policy Director

[17] 514 U.S. 17-18 (1995) (O'Connor, J., concurring); *See also* EPIC, Sandra Day O'Connor's Legacy, https://epic.org/privacy/justices/oconnor/.