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 21, 2019

The Honorable Elijah E. Cummings, Chairman
The Honorable Jim Jordan, Ranking Member
U.S. House Committee on Oversight and Government Reform
2157 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Cummings and Ranking Member Jordan:

We write to you in advance of the hearing on "Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties."[1] We appreciate your interest in the civil liberties implications of facial recognition technology. The Electronic Privacy Information Center ("EPIC") has litigated this issue and made specific recommendations regarding the protection of privacy.[2] We welcome your leadership on this critical issue and look forward to working with you and your staff.

EPIC filed a lawsuit yesterday to compel the State Department to release information about the transfer of facial images, gathered from visa and passport applicants, to other federal agencies.[3] Through the State Department's Consular Consolidated Database, facial images are disclosed to the Department of Homeland Security, the Department of Defense, and the Federal Bureau of Investigation (FBI). The FBI, in particular, has a history of ignoring the privacy implications of facial recognition technology and EPIC urges the Committee to consider the FBI's Next Generation Identification program, which makes use of biometric identifiers and raises serious privacy issues.

<u>The FBI's Next Generation Identification Program</u>

In 2014, EPIC prevailed in a Freedom of Information Act (FOIA) case against the FBI concerning the NGI program.[4] In finding for EPIC's claim that the publication of information about the FBI's identification system, U.S. District Judge Tanya Chutkan stated:

[1] *Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties*, House Comm. on Oversight and Gov't Reform, 116th Cong. (May 22, 2019), https://oversight.house.gov/legislation/hearings/facial-recognition-technology-part-1-its-impact-on-our-civil-rights-and.

[2] *See EPIC v. FBI*, 72 F.Supp.3d 338 (D.D.C. 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] *EPIC v. Dept. of State,* No. 1:19-cv-1468 (D.D.C. filed May 20, 2019); *See* EPIC, *EPIC Sues State Department About Secret Facial Recognition Database* (May 20, 2019), https://epic.org/2019/05/epic-sues-state-department-abo.html.

[4] *EPIC v. FBI*, 72 F.Supp.3d 338 (D.D.C. 2014) (records regarding Next Generation Identification).

> 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 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. Another FOIA lawsuit for the Bureau's biometric agreements with the Department of Defense yielded several agreements between the FBI and DoD and one that included that State Department that detailed the dissemination of biometric data between the agencies for a broad set of purposes.[10]

The increasing use and dissemination of biometric data by the FBI requires oversight particularly after the GAO's recent report on the FBI's use of facial recognition.[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] Three years later, the GAO reports that the FBI has still not implemented all of the agency's recommendations to address the issues with the FBI's use of facial recognition, including recommendations "to ensure privacy and accuracy of the FBI's face recognition capabilities."[13]

[5] *Id.* at 346.

[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] EPIC, *FBI Performs Massive Virtual Line-up by Searching DMV Photos* (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,* No. 16-2237 (filed Nov. 10, 2016 D.D.C.) *(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.

[13] Letter from Gene L. Dodaro, Comptroller General of the United States, to William P. Barr, Attorney General for the United States, 2 (Apr. 10, 2019), https://www.gao.gov/assets/700/698610.pdf.

The risks of NGI and the large-scale collection, use, retention, and sharing of biometrics, especially facial images, are well understood by the privacy and civil liberties community. Several years ago, EPIC led the way in calling for greater oversight on the FBI's NGI database. In 2011, 70 organizations joined EPIC and urged the Inspector General of the Department of Justice to investigate the privacy and civil liberties implications of the FBI's NGI program.[14] 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.[15] EPIC sent a letter to Congress in January 2015 urging greater oversight of NGI.[16] In 2016, a coalition of 46 groups sent a letter to Congress demanding oversight of the FBI's vast biometric database—NGI.[17]

The increasing use of biometrics, particularly facial recognition, by law enforcement raises serious for the public. The 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.

In the context of consumer protection, EPIC had urged the FTC to establish a moratorium on facial recognition techniques until adequate privacy safeguards were established.[18] We also objected to Facebook's use of facial recognition, which is prohibited by many countries outside of the United States.[19] And after 9-11, EPIC objected to Admiral John Poindexter's proposal for "Total Information Awareness," which relied in part on techniques such as facial recognition to capture identity.[20]

There is little a person in the United States could to do to prevent the capture of their image by a federal agency or a private company. Participation in society necessarily exposes one's images in public spaces. But ubiquitous and near effortless identification eliminates the individual's

[14] 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.
[15] 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.
[16] 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.
[17] 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.
[18] Comments of EPIC to FTC, *Face Facts: A Forum on Facial Recognition* (Jan. 31. 2012), https://epic.org/privacy/facerecognition/EPIC-Face-Facts-Comments.pdf.
[19] *In re Facebook and the Facial Identification of Users*, EPIC, https://epic.org/privacy/facebook/facebook_and_facial_recognitio.html (EPIC's Complaint to the FTC in the matter of Facebook and the Facial Identification of Users is available at https://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf.)
[20] *Total Information Awareness*, EPIC, https://www.epic.org/privacy/profiling/tia/.

ability to control the disclosure of their identities to others 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 Constitutionally protected right, virtually impossible.[21]

EPIC urges the Committee to explore how the FBI is currently using facial recognition, the agency's plans future use, and how the agency is mitigating the substantial risks to the public of this technology.

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/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

/s/ *Jeramie Scott*
Jeramie Scott
EPIC Senior Counsel

[21] *See McIntyre v. Ohio Elections Commission,* 514 U.S. 334, 337 (1995) ("Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society.")