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

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

FEDERAL BUREAU OF INVESTIGATION

of the

DEPARTMENT OF JUSTICE

Revision of a Currently Approved Collection-CJIS Name Check Form (1-791)

[OMB Number 1110-0060]

January 8, 2018

By notice published November 8, 2017 the Department of Justice's Federal Bureau of Investigation ("FBI") proposed information collection request concerning name checks for noncriminal justice purposes in the Next Generation Identification ("NGI") system.[1] The Name Check Form (1-791) allows the FBI to conduct a name-based background check after applicant fingerprints have been rejected twice for quality so that applicants are not denied employment, benefits, or licensing.

The Electronic Privacy Information Center ("EPIC") supports this form and would like to encourage the FBI to expand usage of the form to allow applicants to select name-based

[1] *Notice of request for public comment on "Revision of a Currently Approved Collection-CJIS Name Check Form (1-791),"* 82 Fed. Reg. 51643 (Nov. 8, 2017) (hereafter "Notice"), *available at* https://www.federalregister.gov/documents/2017/11/07/2017-24208/agency-information-collection-activities-proposed-ecollection-ecomments-requested-revision-of-a.

background checks in lieu of fingerprint-based background checks. The name-based background check accomplishes the same purpose as the fingerprint-based background check without requiring the collection of sensitive biometric information.

Names should be used instead of fingerprints to conduct background checks for noncriminal purposes whenever possible. Fingerprints are some of the most sensitive information about an individual because they are personally identifiable and cannot be changed. If the NGI database were ever compromised, the breach of fingerprints would pose a greater risk of harm. The FBI's lengthy retention policy increases the exposure of a potential data breach by retaining the fingerprints of individuals well beyond the purpose of collection and heightens the risk of data breach by collecting so much sensitive information in one database.

Pursuant to the agency's request for comments, EPIC submits these comments to express support for the use of the Name Check Form (1-791) and urge the FBI to allow any individual submitting to a background check for noncriminal purposes to select this form rather than requiring the submission of fingerprints.

I. EPIC's Interest

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in privacy safeguards for information systems operated by the federal government. Since NGI's inception, EPIC has repeatedly called for increased oversight of the program. In addition to multiple coalition letters to Congress and the Attorney General,[2] EPIC submitted comments to the FBI in

[2] 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; Letter from Coalition of Civil Liberties groups to Eric Holder, U.S. Attorney General (June 24,

2016.[3] EPIC has also pursued a series of Freedom of Information Act requests to determine the accuracy and reliability of the NGI records system.[4]

II. FBI's Collection and Retention Policies Create Unnecessary Privacy Risks

The FBI retains records in the NGI system for an unreasonably long period of time. Once the fingerprints are entered into the database, the records are kept by the FBI until individual turns 110, or seven years after notification of their death.[5] Individuals cannot get their records purged unless they have a court order.[6] Additionally, employers often give individuals no choice but to submit their fingerprints for a background check in order to secure a particular job.[7] EPIC supports giving applicants the option to submit the Name Check Form in lieu of a fingerprint-based background check.

By contrast, NGI's predecessor—Integrated Automated Fingerprint Identification System ("IAFIS")—routinely deleted fingerprints collected for noncriminal purposes after they were

---

2014), https://www.privacycoalition.org/Ltr-to-Review-FBI-NGI-Program.pdf; Letter from EPIC to Chairman Grassley and Ranking Member Leahy of the S. Jud. Comm. (Jan. 9, 2015), https://epic.org/foia/fbi/ngi/EPIC-to-SJC-re-NGI.pdf; Letter from Coalition Privacy, Transparency, Civil Rights, Human Rights, and Immigrant groups to Senators Grassley and Leahy, and Representatives Goodlatte, Chaffetz, Conyers, and Cummings (June 23, 2016), https://epic.org/privacy/fbi/NGI-Congressional-Oversight-Letter.pdf.

[3] Comments of EPIC to FBI, *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.

[4] *See, e.g.*, EPIC, *EPIC v. FBI – Next Generation Identification*, http://epic.org/foia/fbi/ngi/.

[5] Ernest J. Babcock, *Privacy Impact Assessment: Next Generation Identification (NGI) - Retention and Searching of Noncriminal Justice Fingerprint Submissions*, FBI (Feb. 20, 2015), https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/next-generation-identification-ngi-retention-and-searching-of-noncriminal-justice-fingerprint-submissions.

[6] *Id.*

[7] *Id.* ("Civil applicants may decline to submit fingerprints; however, a fingerprint-based background check is often a prerequisite for employment and licensing.")

processed.[8] The IAFIS retention policy allowed the purpose for the fingerprint collection to be completed without subjecting individuals to the unnecessary risk of breach, misuse, or mission creep for the rest of their lives. A shorter retention period is more important now than ever.

The rise of government data breaches is a major concern. The Government Accountability Office ("GAO") has made about 2,500 recommendations to federal agencies to improve the security of their systems and information, but as of February 2017 about 1,000 of the recommendations have not been implemented.[9] According to GAO, "Federal information systems and networks are inherently at risk. They are highly complex and dynamic, technologically diverse, and often geographically dispersed."[10]

The 2015 Office of Personnel Management (OPM) data breaches compromised the personal information of 21.5 million people, including 1.8 million people who did not apply for a background check.[11] The fingerprints of 5.6 million people were stolen in the data breach.[12] More recently, the IRS and Department of Education faced threats from identity thieves exploiting their financial aid application[13] and a government cybersecurity contractor fell prey to

[8] *Id.*
[9] U.S. Gov't Accountability Office, *Cybersecurity Actions Needed to Strengthen U.S. Capabilities* at 5 (Feb. 14, 2017), *https://www.gao.gov/assets/690/682756.pdf.*
[10] *Id.* at 2.
[11] Dan Goodin, *Call it a "Data Rupture": Hack Hitting OPM Affects 21.5 Million*, ARSTECHNICA (July 9, 2015), http://arstechnica.com/security/2015/07/call-it-a-data-rupture-hack-hitting-opm-affects-21-5- million/.
[12] Andrea Peterson, *OPM Says 5.6 Million Fingerprints Stolen in Cyberattack, Five Times as Many as Previously Thought*, WASH. POST (Sept. 23, 2015), https://www.washingtonpost.com/news/the- switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/.
[13] Christopher Krebs, *Student Aid Tool Held Key for Tax Fraudsters,* Krebs on Security (Mar. 21, 2017), https://krebsonsecurity.com/2017/03/student-aid-tool-held-key-for-tax-fraudsters/.

a phishing scam, releasing employee W-2 tax information.[14]

While the OPM breach compromised the fingerprints of 5.6 million people, the NGI database contains over 56 million fingerprints and the database continues to grow.[15] The increasing aggregation of biometric data in one spot makes the NGI database an enticing target for criminals— especially given the rise of the use of biometrics for secure access and their immutable property.

A breach of the NGI database would be catastrophic for millions of Americans because biometric identifiers cannot be changed in the event of a breach. Reverting to the retention policy under IAFIS for noncriminal submissions would improve the security of the records. The longer information is stored, the more likely it is to be compromised. The NGI database needlessly exposes millions to data breaches. Barring a shorter retention period, the FBI should minimize the sensitive data collected and allow applicants to opt for name-based background checks. Conducting noncriminal background checks using names instead of fingerprints would mitigate some of the privacy risk.

III. Conclusion

EPIC supports use of the Name Check Form for all individuals submitting to background checks for noncriminal purposes. The FBI currently offers this form only to individuals whose fingerprints have been rejected twice, but EPIC urges the FBI to make the Name Check Form available to all individuals in lieu of fingerprint-based background checks for noncriminal

[14] Christopher Krebs, *Govt. Cybersecurity Contractor Hit in W-2 Phishing Scam,* Krebs on Security (Mar. 17, 2017), https://krebsonsecurity.com/2017/03/govt-cybersecurity-contractor-hit-in-w-2-phishing-scam/.
[15] FBI, NGI Monthly Fact Sheet (Oct. 2017), https://www.fbi.gov/file-repository/ngi-monthly-fact-sheet/view.

purposes. Relying on name checks rather than fingerprint checks would reduce the privacy risks inherent in the NGI system.

Sincerely,

/s/ Jeramie Scott
Jeramie Scott
EPIC National Security Counsel

/s/ Christine Bannan
Christine Bannan
EPIC Administrative Law and Policy Fellow