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

TRANSPORTATION SECURITY ADMINISTRATION

Intent to Request Revision from OMB of One Current Public Collection of Information: TSA Pre-Check Application Program

Docket No. TSA-2014-0001

July 3, 2017

By notice published May 4, 2017 the Transportation Security Administration ("TSA") requests comment on the agency's intent "to expand enrollment options and the potential use of biographical and biometric (*e.g.*, fingerprints, iris scans, and/or photo) information."[1] The revision would allow for security threat assessments done as part of the Pre-Check enrollment process to be used for programs with comparable requirements.[2] Additionally, applicant's biometric information may be used in TSA's Biometric Authentication Technology ("BAT") effort, which will use biometrics is in place of boarding passes to authenticate the identity of TSA Pre-Check applicants at airport security checkpoints.[3]

Pursuant to the agency's request, the Electronic Privacy Information Center ("EPIC") submits these comments to (1) highlight the increased privacy and security risk of expanding the use and continued dissemination of biometric information; (2) call attention to the rising

[1] *Intent to Request Revision From OMB of One Current Public Collection of Information: TSA Pre-Check Application Program,* 82 Fed. Reg. 20,910 (May 4, 2017) [hereafter "Pre-Check Revision"]
[2] *Id.* at 20,911.
[3] *Id.* at 20,911.

potential for mission creep; and (3) propose an alternative course of action for storage of biometrics for Pre-Check applicants.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and protect privacy, the First Amendment, and constitutional values.[4] EPIC has a particular interest in preserving the right of people to engage in First Amendment protected activities without the threat of government surveillance.

EPIC has repeatedly called to limit the information kept in government databases and advocated for data minimization.[5] The TSA is proposing to increase the use of biometrics collected for the TSA Pre-Check program and continue to disseminate biometric information for retention in FBI and DHS databases.[6] TSA sends Pre-Check applicant information to the Federal Bureau of Investigation's ("FBI's") Next Generation Identification ("NGI") database and the Department of Homeland Security's ("DHS's") Automated Biometrics Identification System ("IDENT")[7] where individual's biometric data will be kept for decades beyond what is necessary for the stated purpose of collection. EPIC has previously highlighted the risks associated with biometric databases like NGI and the security risks of government databases in general.[8] The

---

[4] EPIC, About EPIC (2017), https://epic.org/epic/about.html.

[5] Comments of EPIC to the Department of Homeland Security, *Privacy Act of 1974; Department of Homeland Security/ALL—038 Insider Threat Program System of Record Notice of Privacy Act System of Records and Notice of Proposed Rulemaking,* Mar. 28, 2016, https://epic.org/apa/comments/EPIC-DHS-Inisder-Threat-Comments.pdf; Comments of EPIC to the Department of Defense, *DUSDI 01_DoD, Department of Defense (DoD) Insider Threat Management and Analysis Center (DITMAC) and DoD Component Insider Threat Records System,* Jun. 20, 2016, https://epic.org/apa/comments/EPIC-Comments-DoD-Insider-Threat-Database.pdf; Comments of EPIC to the Department of Justice, *Privacy Act of 1974; System of Records and Implementation Notice of a New System of Records and Notice of Proposed Rulemaking*, Sep. 19, 2016.

[6] Pre-Check Revision at 20,911.

[7] *Id.*

[8] EPIC Statement to House Committee on Oversight and Government Reform, 115th Cong. (2017), Mar. 22, 2017, https://epic.org/testimony/congress/EPIC-HCOGR-FacialRecognition-Mar2017.pdf [hereafter "EPIC Facial Recognition Statement"]; Comments of EPIC to the Federal Bureau of Investigation, *Privacy Act of 1974; Systems of Record Notice of a Modified System of Records Notice CPCLO Order No. 002-2016*; Jul. 6, 2016, https://www.epic.org/apa/comments/EPIC-CPCLO-FBI-NGI-Comments.pdf [hereafter "EPIC NGI Comments"].

expanded collection and dissemination of biometric information under Pre-Check substantially increases the privacy and security risks for applicants as well as the potential for mission creep.

I. The Increased Use and Continued Dissemination of Biometric Information increases privacy and security risks and the potential for mission creep

The TSA disseminates the biographical and biometric information from Pre-Check applicants to the FBI's NGI database and the DHS' IDENT database. The FBI and DHS can then use that information as they please and retain the data well beyond what is required for the original purpose of collection. Signing up for Pre-Check exposes the biographical and biometric information of applicants to a lifetime in various government databases guaranteeing that their information will be used well beyond the stated collection purpose.

The information stored in the NGI database is kept for an excessively long time, 110 years or until 7 years after a person dies. This means that individuals whose information is included in the database have it stored there for the rest of their lives and it is incredibly difficult to get their information removed. NGI is used by both federal and select state law enforcement agencies to support criminal investigations by providing a repository of biometric and biographical information.[9] This is the case despite the fact the information is provided voluntarily by individuals suspected of no wrongdoing that warrants their information being stored by a law enforcement agency.

IDENT is a DHS-wide system that stores and processes biometric data and links biometrics with biographical information to confirm individual identities.[10] The biometrics obtained via TSA Pre-Check are not only used to conduct a one-time security threat assessment,

[9] U.S. Gov't Accountability Office, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy,* May 2016, http://www.gao.gov/assets/680/677098.pdf.
[10] *Privacy Impact Assessment for the Automated Biometric Identification System (IDENT),* TSA, Dec. 7, 2012.

they are kept and repeatedly used for immigration, law enforcement, and intelligence purposes.[11] The information contained in IDENT is kept for 75 years.[12] Information in IDENT can be accessed by domestic and international agencies.[13]

A. The Increased Use and Continued Dissemination of Biometrics Increase the Risks of a Security Breach

Recent high-profile government data breaches indicate that federal agencies are incapable of adequately protecting sensitive information from improper disclosure. Indeed, GAO recently released a report on widespread cybersecurity weaknesses throughout the executive branch, aptly titled "Federal Agencies Need to Better Protect Sensitive Data."[14] According to the report, a majority of federal agencies, "have weaknesses with the design and implementation of information security controls …."[15] In addition, most agencies "have weaknesses in key controls such as those for limiting, preventing, and detecting inappropriate access to computer resources and managing the configurations of software and hardware."[16] The GAO report concluded that, due to widespread cybersecurity weaknesses at most federal agencies, "federal systems and information, as well as sensitive personal information about the public, will be at an increased risk of compromise from cyber-based attacks and other threats."[17]

Data breaches have directly impacted DHS information systems in recent years. For example, in 2014, a DHS contractor conducting background investigations for the agency

---

[11] *Id. at* 2.
[12] *Id.* at 10.
[13] *Id.* at 3.
[14] 3 U.S. Gov't Accountability Office, DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System (Jan. 2016) http://www.gao.gov/assets/680/674829.pdf (hereafter "GAO Cybersecurity Report").
[15] U.S. Gov't Accountability Office, Federal Agencies Need to Better Protect Sensitive Data (Nov. 17, 2015), http://www.gao.gov/assets/680/673678.pdf (hereafter "GAO Sensitive Data Report").
[16] *Id.*
[17] *Id.* at 12.

experienced a data breach that compromised the records of at least 25,000 employees, including undercover investigators.[18] In 2015, another DHS contractor suffered a data breach that affected as many as 390,000 people associated with DHS, including current and former employees as well as contractors and job applicants.[19] More recently, a 16-year-old teenage boy was arrested in connection with hacks that exposed the information of more than 20,000 FBI employees and 9,000 DHS employees, as well as the personal email accounts of DHS Secretary Jeh Johnson and Central Intelligence Agency ("CIA") director John Brennan.[20] Overall, the number of government data breaches, including for DHS, has exploded in the last decade, rising from 5,503 in 2006 to 67,168 in 2014.[21]

Of particular concern to TSA should be that these recent breaches occurred, in some cases, due to contractors.[22] In a recent Privacy Impact Assessment for the Pre-Check program, TSA stated that biometric information would be sent to a private, independent third party. Sharing information with outside parties only increases the risk that a data breach will occur either due to poor security practices, more individuals with increased access to the information, or an individual bad actor within the private third party.

There is also reason to be concerned about foreign governments compromising the IDENT database. Foreign governments continue to show a willingness to interfere with and

[18] Jim Finkle & Mark Hosenball, U.S. Undercover Investigators Among Those Exposed in Data Breach, REUTERS (Aug. 22, 2014), http://www.reuters.com/article/us-usa-security-contractor-cyberattackidUSKBN0GM1TZ20140822.
[19] Alicia A. Caldwell, 390,000 Homeland Employees May Have Had Data Breached, ASSOCIATED PRESS (June 15, 2015), http://www.pbs.org/newshour/rundown/390000-homeland-employees-may-have-haddata-breached/.
[20] Alexandra Burlacu, Teen Arrested Over DHS and FBI Data Hack, TECH TIMES (Feb. 13, 2016), http://www.techtimes.com/articles/133501/20160213/teen-arrested-over-dhs-and-fbi-data-hack.htm.
[21] GAO Sensitive Data Report at 4.
[22] Kali Hays, *US Marine Sues OPM, Contractor Over Data Breach,* Law360, Sep. 24, 2015, https://www.law360.com/articles/706601/us-marine-sues-opm-contractor-over-data-breach.

infiltrate government agencies.[23] The ability for foreign agencies to access information from IDENT is particularly concerning given recent revelations that foreign governments have been willing to provide false information that has the potential to derail investigations.[24]

The extensive storage of biometrics increases the risk of harm posed by these security breaches. Several Internet of Things and mobile computing devices use biometrics for secure access and operation. As these devices become ever more integrated into people's daily lives the security of biometric information will become increasingly important. If a database storing the biometric information of millions of individuals is compromised, individuals will be placed at substantial risk.[25] Biometrics are unique to each individual person, if they are compromised then individuals' privacy and security will be forever at risk.

B. The Increased Use and Continued Dissemination of Biometrics Raises the Privacy and Civil Liberties Risks while Increasing the Chances of Mission Creep

TSA's continued dissemination of biometric data to other agencies for use beyond the purpose of collection raises substantial privacy and civil liberties risks. Large biometric databases like NGI and IDENT have the potential to undermine the ability of an individual to be anonymous. Publicly participating in society as a relatively anonymous individual becomes increasingly impossible if every fingerprint left behind, image from a camera or CCTV, or

---

[23] Brian Ross & Pete Madden, United States Remains Vulnerable to North Korean Cyber-Attack, Analysts Say, ABC News, Apr. 22, 2017, http://abcnews.go.com/International/united-states-remains-vulnerablenorth-korean-cyber-attack/story; David E. Sanger, Putin Ordered 'Influence Campaign' Aimed at U.S. Election, Report Says, New York Times, Jan. 6, 2017, https://www.nytimes.com/2017/01/06/us/politics/russia-hack-report.html.

[24] Karoun Demirjian & Devlin Barrett, How a Dubious Russian Document Influenced the FBI's Handling of the Clinton Probe, Washington Post, May 24, 2017, https://www.washingtonpost.com/world/nationalsecurity/how-a-dubious-russian-document-influenced-the-fbis-handling-of-the-clintonprobe/2017/05/24/f375c07c-3a95-11e7-9e48-c4f199710b69_story.html.

[25] April Glaser, *Biometrics Are Coming, Along With Serious Security Concerns,* Wired, Mar. 9, 2016, https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/; Russell Brandom, *Your Phone's Biggest Vulnerability Is Your Fingerprint,* The Verge, May 2, 2016, https://www.theverge.com/2016/5/2/11540962/iphone-samsung-fingerprint-duplicate-hack-security.

recording of one's voice becomes an identifier; an identifier that can reveal the protests one participate in, the groups one associate with, or the things one spoke out about. The TSA, DHS, and FBI biometric databases increase the government's ability to do surveillance on individuals, including individuals who are not suspected of any wrongdoing.

Additionally, the wide dissemination of biometric data by the TSA increases the chance of mission creep. Even in the relatively short period of time that these databases have been used to collect and store biometric information, their use has expanded beyond what was initially intended.[26] Concerns over these databases are not mitigated by the fact that Pre-Check is a voluntary program. Given the increasing scope and use of these databases, no one can be sure of how their information will be used in the future. If information is going to be collected from individuals who have done nothing wrong, there must be transparency in how the government is using that information, both now and in the future.

II. TSA Should Consider Privacy-Enhancing Alternatives

The TSA must consider alternative means to the biometric information collected to conduct security threat assessments for the Pre-Check program. Pre-Check is a voluntary program put in place to make traveling more convenient and the application process should not be used as a means to collect and store massive amounts of information on people. Individuals who are approved for the Pre-Check program should have some say over how their biometric information is used, stored, and should have the option to have that information removed from databases.

[26] *Privacy Impact Assessment for the Automated Biometric Identification System (IDENT)*, Department of Homeland Security, Dec. 7, 2012; 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 (showing an increase in facial recognition searches and that NGI is now primarily being used for non-criminal purposes).

There are several ways that the TSA could mitigate the risks posed by the increased collection of biometric information. For example, because individuals who are approved for TSA Pre-Check have presumably been found not to be dangerous or suspect individuals there is no need to keep their information for 75 or 110 years to be used for law enforcement or immigration purposes. TSA could ensure that for Pre-Check applicants, biometric information is only kept for as long as it is needed to determine whether an individual can be admitted to the Pre-Check program. TSA could also provide Pre-Check applicants with simple, easy to follow instructions on how to have their biometric information deleted from the NGI and IDENT databases if they do not wish to have that information stored for the rest of their lives.

Providing Pre-Check applicants with such information would not frustrate the TSA's purposes for increasing the use of biometric collection. Individuals who would like to have their information kept and stored because they anticipate going through similar security threat assessments or would like to participate in the BAT could easily provide informed consent to have information stored for a longer period of time. Such an option would not frustrate the TSA's ability to keep information for additional security threat assessments or to test the BAT program. Furthermore, providing choices in how long biometric information is stored would allow the TSA to test using biometrics at security checkpoints in place of boarding passes and establish trust in such a system. Instead of putting people into a program by default, the TSA will be providing a choice and should the program prove to be effective and secure individuals can later choose to provide additional information. The purpose of Pre-Check is to allow for easier and faster access through airport security checkpoints, individuals who wish to be part of the Pre-Check program should not be forced to be test subjects for a new system that poses substantial security risks.

III. Conclusion

For the foregoing reasons, EPIC urges the TSA to revise its plan to collect and store additional biometric information as part of the TSA Pre-Check application. The TSA must provide Pre-Check applicants with the opportunity to protect their biometric data and fully explain to them the risks of long-term storage of such sensitive information.

Respectfully Submitted,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Jeramie Scott*
Jeramie Scott
EPIC National Security Counsel

/s/ *Kim Miller*
Kim Miller
EPIC Policy Fellow