epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

DEPARTMENT OF HOMELAND SECURITY

Privacy Act of 1974; Implementation of Exemptions; Department of Homeland Security/ALL-030 Use of the Terrorist Screening Database System of Records

Notice of Proposed Rulemaking

[Docket No. DHS-2016-0001]

Privacy Act of 1974; Implementation of Exemptions; Department of Homeland Security/ALL-030 Use of the Terrorist Screening Database System of Records

Notice of Privacy Act System of Records

[Docket No. DHS-2016-0002]

February 22, 2016

By a System of Records Notice ("SORN") published on January 22, 2016, the Department of Homeland Security ("DHS") proposes to "update and reissue a current Department-wide system of records titled, 'Department of Homeland Security(DHS)/ALL-030 Use of the Terrorist Screening Database (TSDB) System of

Records.'"[1] Additionally, by a Notice of Proposed Rulemaking ("NPRM") published on January 22, 2016, DHS "proposes to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements."[2]

DHS maintains a synchronized copy of the Department of Justice's ("DOJ") Federal Bureau of Investigation ("FBI") Terrorist Screening Records System of Records[3] via a mechanism called DHS Watchlist Service ("WLS") that disseminates the feed to DHS components.[4] The FBI's Terrorist Screening Center ("TSC") maintains the TSDB as the U.S. Government's consolidated watchlist system.[5] DHS and its authorized components access TSDB records via the WLS pursuant to memoranda of understanding with FBI/TSC, and DHS maintains a synchronized, mirror copy of the TSDB.[6] According to the agency, DHS currently has six systems that are authorized to receive TSDB data directly from FBI/TSC via the Watchlist Services, and with this updated notice, DHS proposes to add two new systems, Customs and Border Protection ("CBP") Automated Targeting System ("ATS") and U.S. Citizenship and Immigration Services ("USCIS") Fraud Detection and National Security ("FDNS") Directorate, to the Watchlist Service.[7]

---

[1] Notice of Privacy Act System of Records, 81 Fed. Reg. 3811 (proposed Jan. 22, 2016), *available at* https://www.gpo.gov/fdsys/pkg/FR-2016-01-22/pdf/2016-01167.pdf; [hereinafter TSDB SORN].
[2] Notice of Proposed Rulemaking, 81 Fed. Reg. 3,748 (proposed Jan. 22, 2016), *available at* https://www.gpo.gov/fdsys/pkg/FR-2016-01-22/pdf/2016-01169.pdf*;* [hereinafter TSDB NPRM].
[3] 72 FR 47,073, August 22, 2007.
[4] TSDB NPRM at 3,748.
[5] Homeland Security Presidential Directive 6 (HSPD-6), September 2003.
[6] TSDB SORN at 3,812.
[7] *Id.* at 3,811.

DHS clarified that the current category of individuals "include[s] relatives, associates, or others closely connected with a known or suspected terrorist who are excludable from the United States based on these relationships by virtue of sec. 212(a)(3)(B) of the Immigration and Nationality Act, as amended, and do not otherwise satisfy the requirements for inclusion in the TSDB."[8] DHS also proposes adding two new categories of individuals to include:

> (1) Individuals who were officially detained during military operations, but not as enemy prisoners of war, and who have been identified as possibly posing a threat to national security, and who do not otherwise satisfy the requirements for inclusion in the TSDB ("military detainees") . . . ; and (2) individuals who may pose a threat to national security because they are (a) known or suspected to be or have been engaged in conduct constituting, in aid of, or related to transnational organized crime, thereby posing a possible threat to national security, and (b) do not otherwise satisfy the requirements for inclusion in the TSDB ("transnational organized crime actors") . . . .[9]

In 2011, the Electronic Privacy Information Center ("EPIC") and a coalition of 17 privacy, consumer rights, and civil liberties organizations urged DHS to suspend the very system of records that DHS plans to expand with this notice.[10] The coalition argued that a full review of the privacy, security, and legal implications of the database—including compliance with the federal Privacy Act—should be conducted prior to moving forward with the database.[11] In response to the Coalition comments, DHS removed two proposed

---

[8] *Id.*
[9] *Id.*
[10] EPIC *et al.*, *Comments on Docket Nos. DHS-2011-0060 and DHS-2011-0061: Concerning Use of the Terrorist Screening Database System of Records* (Aug. 5, 2011), *available at* https://epic.org/apa/comments/EPIC-DHS-TSD-Comments.pdf.
[11] EPIC *et al.*, *Comments on Docket Nos. DHS-2011-0060 and DHS-2011-0061: Concerning Use of the Terrorist Screening Database System of Records* (Aug. 5, 2011), *available at* https://epic.org/apa/comments/EPIC-DHS-TSD-Comments.pdf.

Privacy Act exemptions.[12] As described below, however, the database continues to raise substantial privacy risks.

Pursuant to DHS's notices, EPIC submits these comments to urge the agency to: (1) adhere to Congress's intent to maintain transparent and secure government recordkeeping systems; (2) provide individuals judicially enforceable rights of notice, access, and correction; (3) conform to a revised SORN and NPRM that includes requirements for the agency to respect individuals' rights to control their information in possession of federal agencies, as the Privacy Act requires; and (4) premise its technological and security approach on decentralization.

I. Introduction

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 previously commented on DHS's use of the Terrorist Screening Database and traveler screening databases that collect large amounts of personal information. EPIC opposes the agency's practice of largely exempting itself from the obligations of the Privacy Act.

In 2007, EPIC urged the DHS to curtail the revised Automated Targeting System, a federal screening system that creates secret, terrorist ratings on tens of millions of

[12] Privacy Act of 1974; Implementation of Exemptions; Department of Homeland Security/ALL-030 Use of the Terrorist Screening Database System of Records, 76 Fed. Reg. 81,787, 81,788 (final rule Dec. 29, 2011).

American citizens.[13] In 2007, EPIC also led a coalition of 29 organizations and 16 privacy and technology experts that detailed significant privacy and security risks in ATS.[14] In February 2007, EPIC explained that TSA's "internal quality assurance procedures" were not working, and urged the agency to fully apply Privacy Act requirements of notice, access, and correction to DHS's new traveler redress program, Traveler Redress Inquiry Program ("TRIP"), and its underlying watchlist system.[15]

In May 2006, EPIC recommended that CBP substantially narrow the Privacy Act exemptions prior to the revision and expansion of the Global Enrollment System, a database full of individuals' biometric and biographic data, which would be used to determine individual eligibility for the "Trusted Traveler" program.[16] In December 2005, EPIC detailed privacy and security flaws in the Registered Traveler program and recommended DHS suspend the passenger-prescreening program.[17]

---

[13] EPIC, *Comments on Docket Nos. DHS-2007-0042 and DHS-2007-0043 Concerning the Automated Targeting System* (Sept. 5, 2007), *available at* http://www.epic.org/privacy/travel/ats/epic_090507.pdf.
[14] Thirty Orgs. & 16 Privacy & Tech. Experts, *Comments on Dockets No. DH6-2006-0060: Notice of Privacy Act System of Records* (Dec. 4, 2006), *available at* http://epic.org/privacy/pdf/ats_comments.pdf.
[15] EPIC, *Comments on Docket Nos. DHS-2007-0003: Implementation of Exemptions; Redress and Response Records System* (Feb. 20, 2007), *available at* http://www.epic.org/privacy/airtravel/profiling/trip_022007.pdf.
[16] EPIC, *Comments on Docket No. DHS-2005-0053: Notice of Revision and Expansion of Privacy Act System of Records* (May 22, 2006), *available at* http://www.epic.org/privacy/airtravel/ges052206.pdf.
[17] EPIC, *Comments on Docket Nos. TSA-2004-19166 and TSA-2004-17982: Notice to Alter Two Existing Systems of Records; Request for Comments* (Dec. 8, 2005), *available at* http://www.epic.org/privacy/airtravel/profiling/rt120805.pdf.

II. The Terrorist Screening Database Contains Sensitive, Personal Information on Individuals

Currently, DHS states that the following categories of individuals are covered by the "Department of Homeland Security (DHS)/ALL-030 Use of the Terrorist Screening Database (TSDB) System of Records":

- Individuals known or suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism ("known or suspected terrorists").

DHS proposes to add the following categories of individuals:

- Individuals who are foreign nationals or lawful permanent resident aliens and who are excludable from the United States based on their familial relationship, association, or connection with a known or suspected terrorist as described in Section 212(a)(3)(B) of the Immigration and Nationality Act of 1952 ("INA exceptions");
- Individuals who were officially detained during military operations, but not as Enemy Prisoners of War, and who have been identified to pose an actual or possible threat to national security ("military detainees"); and
- Individuals known or suspected to be or have been engaged in conduct constituting, in aid of, or related to transnational organized crime, thereby posing a possible threat to national security ("transnational organized crime actors.")[18]

Currently, the database contains the following categories of records:

- Identifying information, such as name, date of birth, place of birth, biometrics, photographs, passport and/or drivers license information, and other available identifying particulars used to compare the identity of an individual being screened with a known or suspected terrorist, including audit records containing this information;
- For known or suspected terrorists, in addition to the categories of records listed above, references to and/or information from other government law enforcement and intelligence databases, or other relevant databases that may contain terrorism information.

DHS proposes to revise the database to include:

[18] TSDB SORN at 3,813.

- Identifying biographic information, such as name, date of birth, place of birth, passport and/or driver's license information, and other available identifying particulars used to compare the identity of an individual being screened with a subject in the TSDB;
- Biometric information, such as photographs, fingerprints, or iris images, and associated biographic and contextual information;
- References to or information from other government law enforcement and intelligence databases, or other relevant databases that may contain terrorism or national security information, such as unique identification numbers used in other systems;
- Information collected and compiled to maintain an audit trail of the activity of authorized users of WLS information systems; and
- System-generated information, including metadata, archived records and record histories from WLS.[19]

DHS states that the agency is currently planning "future enhancements" to the Watchlist Services that will streamline the process by which DHS relays potential watchlist matches to the FBI.[20] Any "future enhancements" relaying potential watchlist matches may compromise personal privacy, as the TSDB has routinely threatened individual privacy. Since EPIC's previous TSDB comments, government watchlist problems continue to persist. The government's Watchlisting Guidance document, dated March 2013, was made public in 2014.[21] The guidance document provides the rules for inclusion in the TSDB and the many watchlists maintained by that database—setting a low bar of "reasonable suspicion" for inclusion on watchlists.[22] The document indicates that concrete facts are not required for the government to label an individual a terrorist, stating, "Although irrefutable evidence or concrete facts are not necessary, to be

[19] *Id.*
[20] TSDB SORN at 3,813.
[21] National Counterterrorism Center, *March 2013 Watchlisting Guidance*, *available at* https://theintercept.com/document/2014/07/23/march-2013-watchlisting-guidance/.
[22] *Id.* at 33.

reasonable, suspicion should be as clear and as fully developed as circumstances permit."[23]

There are exceptions to the low reasonable suspicion standard. Immediate family members of suspected terrorists can be watchlisted without suspicion.[24] Similarly, certain associates with a defined relationship to the suspected terrorist can be placed on a watchlist without suspicions.[25] The consequence is that innocent individuals and his/her immediate family members could be subject to secret government dragnets.

Once on a watchlist, it is nearly impossible to be removed.[26] The DHS does not inform people that they are in the agency's TSDB. The only recourse for an individual who thinks s/he might incorrectly be placed in the TSDB is through the DHS Traveler Redress Inquiry Program ("TRIP"), in which a TRIP applicant submits a request to the TSA for an administrative appeals process. The TSA then conducts an internal review and based on that review, the Terrorist Screening Center will make a final agency decision.

In September 2014, the GAO reported that despite the DHS's stated guidelines that it will provide a final agency decision on the appeal within 60 days of the receipt of the appeal, the average total processing time for the appeals process for fiscal years 2011 through 2013 was 276 days.[27] Until their appeals are cleared, passengers may be denied boarding, delayed, or subject to intrusive enhanced security procedures. A 2012 GAO

[23] *Id.* at 34.
[24] *Id.* at 43.
[25] *Id.* at 44-45.
[26] *See Ibrahim v. Dep't of Homeland Sec.*, 669 F.3d 983 (9th Cir. 2012).
[27] Government Accountability Office, Secure Flight: TSA Could Take Additional Steps to Strengthen Privacy Oversight Mechanisms 24 (Sept. 2014).

report found that there was no agency "responsible and accountable for routinely conducting government-wide assessments of how agencies are using the watchlist to make screening or vetting decisions and related outcomes or the overall impact screening or vetting programs are having on agency resources and the traveling public."[28]

Despite the high risk of error in the database, the documented cases of innocent people ending up in the database, DHS proposes to continue to exempt this database containing detailed, sensitive personal information from well-established Privacy Act safeguards. Consistent and broad application of Privacy Act obligations are the best means of ensuring accuracy and reliability of the data used in government databases.[29]

III. The Privacy Act Requires DHS to Afford Fundamental Privacy Rights to the Subjects of TSDB Records

When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal information federal agencies could collect, and it required agencies to be transparent in their information practices.[30] Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[31] In 2004, the Supreme Court underscored the importance of the Privacy Act's restrictions upon agency use of personal data to protect privacy interests, noting that:

---

[28] GAO, *Terrorist Watchlist: Routinely Assessing Impacts of Agency Actions since the December 25, 2009, Attempted Attack Could Help Inform Future Efforts*, 26 (May 2012), *available at* http://www.gao.gov/assets/600/591312.pdf.
[29] The Privacy Act of 1974, Pub. L. 93-579, § 2, 88 Stat. 1896 (Dec. 31, 1974).
[30] S. Rep. No. 93-1183 at 1 (1974).
[31] Pub L. No. 93-579 (1974).

> [I]n order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary . . . to regulate the collection, maintenance, use, and dissemination of information by such agencies." Privacy Act of 1974, §2(a)(5), 88 Stat. 1896. The Act gives agencies detailed instructions for managing their records and provides for various sorts of civil relief to individuals aggrieved by failures on the Government's part to comply with the requirements.[32]

Despite these clear statements of legislative mandate and the ongoing privacy and civil liberties risks posed by watchlists, DHS proposes to reissue Privacy Act exemptions for the agency's copy of the TSDB, while expanding the number of people in the database and adding additional consumers of the information.[33] This would exclude the records from a number of meaningful privacy protections Congress established in the Privacy Act.

IV. DHS's Broad Claims of Privacy Act Exemptions Remove any Meaningful Privacy Safeguards for this Vast Database

DHS claims numerous Privacy Act exemptions for the TSDB. DHS claims exemption for the records maintained in TSDB from §§ 552a(c)(3)-(4); (d); (e)(1);(e)(2); (e)(3); (e)(4)(G), (H), and (I); (e)(5); (e)(8); (f); and (g). Several of DHS's claimed exemptions would further exacerbate the impact of its proposed expansions to the categories of records in this system of records.

For example, DHS exempts itself from § 552a(e)(1), which requires agencies to maintain only those records relevant to the agency's statutory mission. The agency exempts itself from § 552a(e)(4)(I), which requires agencies to disclose the categories of sources of records in the system. And the agency exempts itself from its Privacy Act

[32] *Doe v. Chao*, 540 U.S. 614, 618 (2004).
[33] *See* TSDB SORN at 3,811; TSDB NPRM at 3,748.

duties under to § 552a(e)(4)(G) and (H) to allow individuals to access and correct information in its records system. In other words, the DHS claims the authority to collect any information it wants without disclosing where it came from or accounting for its accuracy or acknowledging its existence. DHS attempts to circumvent the intent of the Privacy Act by expanding a massive government database of detailed personal information that lacks accountability. DHS's proposed exemptions from 5 U.S.C. § 552a(c)(3), (e)(8), and (g) only serve to increase the secrecy of the database and erode agency accountability. DHS claims that accounting for disclosures, granting individuals access to their records, and implementing notification regulations may put entities on notice that they are being investigated, thereby hindering their investigative efforts.[34]

While EPIC recognizes the need to withhold notice during the period of the investigation, individuals should be able to know, after an investigation is completed or made public, the information stored about them in the system. Access to records of a completed investigation, with appropriate redactions to protect the identities of witnesses and informants, would provide individuals and entities with the right to address potential inaccuracies. And because the investigations have already been completed, DHS's law enforcement purposes would not be undermined and DHS could still protect individual privacy rights.

The Privacy Act is intended to guard the privacy interests of citizens and lawful permanent residents against government intrusion and to establish accountability for the government's collection and use of personal information. By asserting an exemption that

[34] TSDB NPRM at 3,749-50.

allows the agency to encroach on an individual's right to know about disclosures of her/his personal information held by the agency, DHS violates the central purpose of the Privacy Act.

V. Conclusion and Recommendations

For the foregoing reasons, DHS's proposed expansion of the TSDB is contrary to the core purpose of the federal Privacy Act. Accordingly, DHS must narrow the scope of its proposed Privacy Act exemptions.

Sincerely,

Khaliah Barnes
EPIC Associate Director and Administrative Law Counsel

Jeramie D. Scott
EPIC National Security Counsel

Jin Nie
EPIC Law Clerk

Ajay Sunder
EPIC Law Clerk