epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

DEPARTMENT OF HOMELAND SECURITY

Privacy Act of 1974; Department of Homeland Security/Transportation Security Administration—DHS/TSA-021 TSA PreCheck Application Program System of Records

Notice of Privacy Act System of Records and Notice of Proposed Rulemaking

[Docket Nos. DHS-2013-0040 and 0041]

Privacy Act of 1974; Department of Homeland Security/Transportation Security Administration—DHS/TSA-019 Secure Flight Records System of Records

[Docket No. DHS-2013-0020]

October 10, 2013

By notice published on September 10, 2013,[1] the Department of Homeland Security ("DHS") proposes to establish a new Privacy Act system of records titled, "Department of Homeland Security/Transportation Security Administration—DHS/TSA—021 TSA PreCheck Application Program System of Records" ("TSA PreCheck Application Database" or "TSA Database"). By notice published on September 11, 2013,[2] DHS proposes to exempt the TSA PreCheck Application Database from several significant provisions of the Privacy Act of 1974. And by a separate notice published on September 10, 2013, DHS proposes to update and reissue a current DHS system of records titled, "Department of Homeland Security/Transportation Security Administration—DHS/TSA—019 Secure Flight Records

[1] Notice of Privacy Act System of Records, 78 Fed. Reg. 55,274 (proposed Sept. 10, 2013) (hereinafter "PreCheck SORN").
[2] Notice of Proposed Rulemaking, 78 Fed. Reg.55,657 (proposed Sept. 11, 2013) (hereinafter "PreCheck NPRM").

System of Records."[3] Pursuant to DHS's notices, the Electronic Privacy Information Center ("EPIC") submits these comments to: (1) address the substantial privacy and security issues raised by the database; (2) urge DHS to significantly narrow the Privacy Act exemptions for the TSA PreCheck Application Database; and (3) recommend that DHS withdraw unlawful and unnecessary proposed routine use disclosures.

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 to protect privacy, the First Amendment, and constitutional values. EPIC has previously opposed other DHS passenger profiling programs,[4] and has called for an independent audit to determine whether the Transportation Security Administration ("TSA") airport screeners engage in racial profiling.[5] EPIC highlighted the problems inherent in passenger profiling systems like Secure Flight in previous testimony and comments. In testimony before the National Commission on Terrorist Attacks Upon the United States (more commonly known as "the 9/11 Commission"), EPIC President Marc Rotenberg explained, "there are specific problems with information technologies for monitoring, tracking, and profiling. The techniques are imprecise, they are subject to abuse, and they are invariably applied to purposes other than those originally intended."[6]

---

[3] Notice of Modified Privacy Act System of Records, 78 Fed. Reg. 55,270 (proposed Sept. 10, 2013) (hereinafter "Secure Flight SORN"). Although these comments focus primarily on TSA PreCheck, certain portions of the Secure Flight SORN implicate TSA PreCheck and EPIC has addressed those portions in these comments.

[4] *See, e.g.*, EPIC et al., *Comments on the Terrorist Screening Database System of Records, Notice of Privacy Act System of Records and Notice of Proposed rulemaking, Docket Nos. DHS 2011-0060 and DHS 2011-0061* (Aug. 5, 2011), *available at* http://epic.org/privacy/airtravel/Comments_on_DHS-2011-0060_and_0061FINAL.pdf; EPIC, *Comments on Secure Flight*, *Docket Nos. TSA-2007-28972, 2007-28572* (Sept. 24, 2007), *available at* http://epic.org/privacy/airtravel/sf_092407.pdf; EPIC, *Secure Flights Should Remain Grounded Until Security and Privacy Problems are Resolved, Spotlight on Surveillance Series* (August 2007), *available at* http://epic.org/privacy/surveillance/spotlight/0807/default.html; EPIC: Passenger Profiling, http://epic.org/privacy/airtravel/profiling.html; EPIC: Secure Flight, http://epic.org/privacy/airtravel/secureflight.html; EPIC: Air Travel Privacy, http://epic.org/privacy/airtravel/.

[5] Letter from EPIC et al., to Secretary Janet Napolitano and Honorable Charles K. Edwards, Department of Homeland Security (Dec. 1, 2011), *available at* http://epic.org/privacy/airtravel/12-01-11-Coalition-Racial-Profiling-Audit-DHS-Letter.pdf.

[6] Marc Rotenberg, President, EPIC, *Prepared Testimony and Statement for the Record of a Hearing on Security & Liberty: Protecting Privacy, Preventing Terrorism Before the National Commission on Terrorist Attacks Upon the United States* (Dec. 8, 2003), *available at* http://www.epic.org/privacy/terrorism/911commtest.pdf.

Despite EPIC's recommendations and empirical evidence of the ineffectiveness of passenger profiling, DHS continues to expand its passenger profiling capabilities and now proposes broad Privacy Act exemptions to the operation of the TSA PreCheck Application Database.

Purpose and Scope of the TSA PreCheck Application Database

According to DHS, the TSA PreCheck Application Database "will use the information provided by applicants to the [TSA PreCheck] Program to perform a security threat assessment to identify individuals who present a low risk to transportation security. This passenger prescreening enables TSA to determine the appropriate level of security screening the passenger will receive before the passenger receives a boarding pass."[7] DHS states that passengers that qualify for expedited screening "typically will receive more limited physical screening, *e.g.*, will be able to leave on their shoes, light outerwear, and belt, to keep their laptop in its case, and to keep their 3-1-1 compliant liquids/gels bag in a carry-on."[8]

To qualify for PreCheck, applicants provide their biographic and biometric information to DHS and, as described by DHS, TSA will use applicant information to perform a "security threat assessment" of "law enforcement, immigration, and intelligence databases, including a fingerprint-based criminal history check conducted through the Federal Bureau of Investigation."[9] The agency states it will use the security threat assessment to "identify individuals who present a low risk to transportation security."[10] TSA will then provide a "Known Traveler Number" ("KTN") to "low risk" individuals.[11]

After having received a KTN, passengers will supply their KTNs to commercial airlines when making flight reservations.[12] The airline will then send passenger Secure Flight Passenger Data ("SFPD"), which includes KTNs, name, gender, date of birth, available passport information, available redress number, "reservation control number, record sequence number, record type, passenger update indicator,

[7] PreCheck NPRM, 78 Fed. Reg. at 55,657.
[8] PreCheck SORN, 78 Fed. Reg. at 55,275.
[9] PreCheck NPRM, 78 Fed. Reg. at 55,657.
[10] PreCheck SORN, 78 Fed. Reg. at 55275.
[11] PreCheck NPRM, 78 Fed. Reg. at 55,658.
[12] *Id*.

traveler reference number, and itinerary information" to the TSA.[13] The TSA will then compare SFPD to the TSA PreCheck Application Program and various undisclosed watch lists.[14] DHS further states that in comparing SFPD against PreCheck Application Program and various watch lists, it will review that information "using intelligence-driven, risk-based analysis to determine whether individual passengers will receive expedited, standard, or enhanced screening; the results will be indicated on the passenger's boarding pass."[15] Although DHS states that the "primary result of the risk-based analysis will be the identification of passengers who are eligible for expedited screening,"[16] DHS also acknowledges that "watch list matches will receive screening appropriate for their watch list status."[17]

TSA PreCheck Application Database would contain "any or all" of the following information:

> (a) Name (including aliases or variations of spelling); (b) Gender; (c) Current and historical contact information (including, but not limited to, address, telephone number, and email address); (d) Date and place of birth; (e) Physical description, fingerprint and/or other biometric identifier, including photograph; (f) Control number, Social Security Number (SSN), or other unique identification number assigned to an individual; (g) Information necessary to assist in tracking submissions, payments, and transmission of records; (h) Other data as required by Form FD-258 (fingerprint card) or other standard fingerprint cards used by the federal government; (i) Information provided by individuals covered by this system in support of their application, such as driver's license, passport or other documents used to verify identity, confirm immigration status, or other eligibility requirements; (j) Criminal history records; (k) Records obtained from the Terrorist Screening Center of known or suspected terrorists in the Terrorist Screening Database; and records regarding individuals identified on classified and unclassified governmental watch lists used or maintained by TSA; (l) Records containing the matching analyses and results of comparisons of individuals to the TSDB and other classified and unclassified governmental databases, such as law enforcement, immigration, or intelligence databases, and individuals who have been distinguished from individuals on a watch list through a redress process or other means; (m) Other information provided by federal, state, local, tribal, territorial, and foreign government agencies or other entities relevant to the security threat assessment and adjudication of the application; (n) Results of any analysis performed for security threat assessments and adjudications; and (o) Communications between TSA and applicants regarding the results of the security threat assessments and adjudications.[18]

---

[13] *Id*.
[14] *Id*.
[15] Secure Flight SORN, 78 Fed. Reg. at 55,271.
[16] *Id*.
[17] PreCheck NPRM, 78 Fed. Reg. at 55,658.
[18] PreCheck SORN, 78 Fed. Reg. at 55,276.

TSA has presented has five purposes for collecting, maintaining, using, and disclosing this personally identifiable information:

> (a) perform[ing] security threat assessments and to identify individuals who are a low risk to transportation or national security and are therefore eligible to receive expedited security screening; (b) assist[ing] in the management and tracking of the status of security threat assessments of individuals who apply to the TSA PreCheck Application Program; (c) permit[ting] the retrieval of the results of security threat assessments, including criminal history records checks and searches in other governmental data systems, performed on the individuals covered by this system;
> (d) permit[ting] the retrieval of information from other terrorist-related, law enforcement, immigration, and intelligence databases on the individuals covered by this system; and
> (e) track the fees incurred, and payment of those fees, when appropriate, for services related to security threat assessments.[19]

Information contained in the TSA PreCheck Application Database may be obtained from "TSA PreCheck Application Program applicants, the [Terrorist Screening Center] TSC, law enforcement, immigration, and intelligence agency record systems, other government databases, and other DHS systems," as well as the Federal Bureau of Investigation ("FBI").[20]

Incredibly, DHS proposes to exempt this database containing detailed, sensitive personal information from well-established Privacy Act safeguards. It is inconceivable that the drafters of the Privacy Act would have permitted a federal agency to propose a profiling system on U.S. citizens and be granted broad exemptions from Privacy Act obligations. Consistent and broad application of Privacy Act obligations are the best means of ensuring accuracy and reliability of the data used in a system that profoundly affects millions of individuals as they travel throughout the United States on a daily basis.

I. The DHS's Notice of Proposed Rulemaking Fails to Fairly Apprise the Public of DHS's Proposal

As a preliminary matter, DHS's proposal is procedurally deficient because the agency has failed to provide sufficient notice of its proposal. Specifically, DHS proposes to exempt the TSA PreCheck

[19] *Id*.
[20] PreCheck SORN, 78 Fed. Reg. at 55,278.

Application Program System of Records from certain Privacy Act provisions pursuant to 5 U.S.C. §§ 552a(k)(1) and (k)(2). The Privacy Act permits agencies to promulgate rules exempting system of records from certain Privacy Act provisions, but those rules must be "in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e)" of the Administrative Procedure Act ("APA").[21]

The APA general notice requirements mandate that Notices of Proposed Rulemaking ("NPRMs") contain "either the terms or substance of the proposed rule or description of the subjects and issues involved."[22] "The adequacy of the notice must be tested by determining whether it would fairly apprise interested persons of the 'subjects and issues' before the agency."[23] Proposals that are "too general and open-ended to have fairly apprised the public" do not meet the APA standard of requisite notice.[24] As discussed below, DHS's proposed rule contains ambiguous key terms that do not fairly apprise the public of the proposed TSA PreCheck Application Database proposals. Accordingly, DHS's proposal violates the APA. DHS must therefore issue an unambiguous proposal and again solicit public comments, or abandon its current proposal because it has not fairly apprised the public of the system of records Privacy Act exemptions.

Throughout the NPRM, DHS states that TSA PreCheck prescreens and identifies "low risk passengers" that are "eligible to receive expedited screening."[25] After conducting a "security threat assessment" on these individuals, TSA will provide "individual[s] [who] pose [] a low risk to transportation or national security" a KTN.[26] Known Traveler Numbers are "unique number assigned to an individual for whom the Federal government has conducted a security threat assessment and

---

[21] 5 U.S.C.§ 552a(k).
[22] 5 U.S.C. § 553(b).
[23] *Prometheus Radio Project v. F.C.C.*, 652 F.3d 431, 449 (3d Cir. 2011) (*quoting Prometheus Radio Project v. F.C.C.*, 373 F.3d 372, 411 (3d Cir. 2004)).
[24] *Prometheus Radio Project*, 652 F.3d at 453.
[25] *See, e.g.*, PreCheck NPRM, 78 Fed. Reg. at 55,657-55,658. *See also* Secure Flight SORN, 78 Fed. Reg. at 55,274.
[26] PreCheck NPRM, 78 Fed. Reg. at 55,658.

determined *does not* pose a security threat."[27] Pursuant to federal Secure Flight regulations, Known Traveler Numbers are reserved for passengers who do "not pose a security threat."[28] With TSA PreCheck, DHS has expanded Known Traveler Numbers to individuals who pose some risk—albeit "low"— to transportation security. Practically speaking, DHS has amended a prior legislative rule—without conducting a public rulemaking as required by law—by granting Known Traveler Numbers to individuals who pose a "low risk" security threat.[29]

Notwithstanding this procedural deficiency, DHS fails to define "low risk passengers"—a key term used throughout the NPRM. Moreover, TSA states "[e]ligibility for the TSA PreCheck Application Program is within the sole discretion of the TSA" and that the TSA will only advise applicants if FBI criminal records disclose information "that would disqualify [applicants] from the TSA PreCheck Application Program."[30] By maintaining discretion over who is a "low risk passenger," failing to define "low risk passenger," and maintaining an opaque algorithm to determine individual risk, DHS's proposal is "too general and open-ended to have fairly apprised the public" on the scope and subject matter of the agency's proposal.[31]

Additionally, the TSA's proposal is "too general and open-ended to have fairly apprised the public" because it fails to disclose the watch lists that TSA uses to determine the level of passenger screening.[32] The TSA acknowledges that it will perform watch list matching analyses against "classified and unclassified governmental watch lists used or maintained by the TSA" including the Terrorist Screening Database, but fails to provide additional information.[33] DHS must reissue its NPRM and disclose the watch lists to fairly apprise individuals of the proposed rule and its impact. Specifically, by

[27] 49 C.F.R. § 1560.3 (emphasis added).
[28] *Id*.
[29] *Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec.*, 653 F.3d 1, 6-7 (D.C. Cir. 2011).
[30] PreCheck NPRM, 78 Fed. Reg. at 55,658.
[31] *Prometheus Radio Project,* 652 F.3d at 453.
[32] *Id.*
[33] PreCheck SORN, 78 Fed. Reg. at 55,275.

disclosing the TSA PreCheck Application watch lists, individuals can raise arguments concerning the appropriateness of certain watch list database comparison. For example, pursuant to a FOIA lawsuit, EPIC uncovered that one of the main watch lists TSA PreCheck uses for comparison—the Terrorist Screening Database ("TSDB")—uses "particularized derogatory information" to place individuals on the watch list.[34] Alarmingly, this is a standard that has never been recognized by a court of law. EPIC's FOIA documents also revealed that individuals might remain on the TSDB watch list even if charges are dropped or a case is dismissed.[35] For the aforementioned reasons, DHS must reissue its NPRM clarifying the definition of "low risk passengers" and providing additional information on its watch lists.

II. DHS Must Provide Transparency in the TSA PreCheck Algorithm and Must Make Public the Factors Used for TSA PreCheck "Risk Assessments"

There is no publicly available information on how DHS uses its algorithms to determine which individuals will be scrutinized upon traveling throughout the United States. The key characteristics of TSA PreCheck system – including the risk and security threat assessment and the basis for the assessments– are secret. DHS evaluates personally identifiable information to determine whether individual passengers will receive "expedited, standard, or enhance screening."[36] The result of the "risk-based" analysis that determines the individual level of screening is opaque. DHS fails to clearly articulate how personally identifiable information factors into DHS risk assessments.

TSA PreCheck operates via automated data processing. This troubling practice will ultimately violate important personal rights as enumerated in such well-established privacy provisions as Article 15.1 of the 1995 EC Directive on Data Protection. The Directive, which provoked many European countries to enact provisions along the lines of article 15.1,[37] states that "Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or

[34] *EPIC FOIA - FBI Watchlist*, EPIC, http://epic.org/foia/fbi_watchlist.html (last visited Oct. 10, 2013).
[35] *Id*.
[36] Secure Flight SORN, 78 Fed. Reg. at 55,271.
[37] Lee A. *Bygrave, Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, 17 COMPUTER LAW & SOC. REP. 17, 18 (2001).

significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc."[38] In particular, Article 12.1 of the EU Data Protection Directive also grants individuals the right to obtain "the logic," *i.e.* the algorithm, of the processing of personal data.

TSA PreCheck screening would directly violate this right because the decision of which persons should undergo additional screening is entirely automated. DHS must ensure transparency and make public the algorithm that it has established to assign "risk-based" profiles to individuals so as to not further violate personal rights.

III. DHS Should Impose Strict Information Security Safeguards on its Biometric Information Collection and Limit its Dissemination of Biometric Information

Information security is a critical consideration for any organization that collects digital records and data, and it is even more important when government agencies collect sensitive and personally identify information. Government agencies must make every effort to safeguard sensitive information. Without proper safeguards, individuals and groups with malicious intent to intrude, access, and obtain sensitive information may disrupt operations or launch attacks against computer systems and networks. This concern is validated by an ever-increasing number of security incidents, the ease of obtaining hacking tools, and their growing sophistication.[39]

TSA PreCheck collects biometric identifiers, including fingerprints and photographs. Over the last several years, TSA and DHS have repeatedly encountered security failures. For example, in 2007, the TSA reported that an external hard drive containing Social Security numbers, payroll information, and

[38] Council Directive 95/46, On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 15, 1995 O.J. (L 281) 11.23.1995 (EC).
[39] *See, e.g.*, Ben Weitzenkorn, *How to Hack an iPhone With a USB Charger,* TECHNEWSDAILY (June 3, 2013, 05:43 PM), http://www.technewsdaily.com/18241-iphone-malicious-charger.html; Harry Kazianis, *Spear phishing: How the non-nerds hack into you,* THE NATION (June 14, 2013, 1:00 AM), http://www.nationmultimedia.com/opinion/Spear-phishing-How-the-non-nerds-hack-into-you-30208233.html.

bank data for about 100,000 TSA employees was stolen from a "secure area."[40] Moreover, in 2008 the TSA suffered significant security problems with its passenger redress website when the TSA failed to secure the website; large amounts of personal information were leaked, exposing hundreds of travelers to identity theft.[41] And earlier this year DHS again encountered issues securing personal and sensitive information of its employees as recently as last month. Tens of thousands of DHS employees and contractors who submitted background investigation information were at risk of having their personal data stolen, exposing them to identify theft. An internal DHS notice sent to employees noted that "[a]s a result of this vulnerability, information including name, Social Security numbers (SSN) and date of birth (DOB), stored in the vendor's database of background investigations was potentially accessible by an unauthorized user since July 2009."[42]

These weaknesses in DHS databases increase the risk that unauthorized individuals could read, copy, delete, add, and modify sensitive information, including biometric information. Accordingly, to the extent that DHS continues to collect biometric information, DHS should limit biometric information to only those agencies and government actors that require the information as a necessity. Further, DHS should strictly limit biometric information to uses for which it was originally collected.

IV. DHS Proposes Broad Exemptions for the TSA PreCheck Application Database, Contravening the Intent of the Privacy Act of 1974

DHS proposes broad Privacy Act exemptions for the TSA PreCheck Application Database, thus contravening the intent of the Privacy Act of 1974. DHS asserts these claims for "law enforcement or national security purposes."[43] DHS claims that "[n]o exemption shall be asserted with respect to information maintained in the system that is submitted by a person if that person, or his or her agent,

[40] Spencer S.Hsu, *TSA Hard Drive With Employee Data Is Reported Stolen*, WASHINGTON POST (May 5, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/05/04/AR2007050402152.html.
[41] U.S HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM. INFORMATION SECURITY BREACH AT TSA, THE TRAVELER REDRESS WEBSITE (January 2008), *available at* http://www.hsdl.org/?view&did=482286.
[42] Jason Miller, *Data Breach puts DHS employees at Risk of Identity Theft*, FEDERAL NEWS RADIO (May 22, 2013, 4:05 PM), http://www.federalnewsradio.com/473/3332836/Data-breach-puts-DHS-workers-at-risk-of-identity-theft.
[43] PreCheck NPRM, 78 Fed. Reg. at 55,658.

seeks access to or amendment of such information."[44] DHS, however, further states "[t]his system . . . may contain records or information created or recompiled from information contained in other systems of records that are exempt from certain provisions of the Privacy Act" and that DHS will also claim the original Privacy Act exemptions for those records.[45]

Notwithstanding access or amendment rights to information that TSA PreCheck Applicants submit, DHS will not provide individuals access to the following records:

> (j) Criminal history records; (k) Records obtained from the Terrorist Screening Center of known or suspected terrorists in the Terrorist Screening Database; and records regarding individuals identified on classified and unclassified governmental watch lists used or maintained by TSA; (l) Records containing the matching analyses and results of comparisons of individuals to the TSDB and other classified and unclassified governmental databases, such as law enforcement, immigration, or intelligence databases, and individuals who have been distinguished from individuals on a watch list through a redress process or other means; (m) Other information provided by federal, state, local, tribal, territorial, and foreign government agencies or other entities relevant to the security threat assessment and adjudication of the application; (n) Results of any analysis performed for security threat assessments and adjudications; (o) Communications between TSA and applicants regarding the results of the security threat assessments and adjudications.[46]

DHS will, however, provide an opportunity for individuals to correct inaccurate immigration records or FBI criminal records.[47]

Furthermore, DHS proposes to claim Privacy Act exemptions to:

> preclude subjects of investigations from learning of and exploiting sensitive investigatory material that would interfere with the investigative process; avoid disclosure of investigative techniques; protect sensitive and classified information compiled during the investigation; protect Transportation Security Administration Office of Intelligence and Analysis and other federal agency information; ensure DHS's and other federal agencies' ability to obtain information from third parties and other sources; protect the privacy of third parties; and safeguard Sensitive Security Information pursuant to 49 U.S.C. 114(r).[48]

---

[44] *Id*.
[45] *Id*.
[46] PreCheck SORN, 78 Fed. Reg. at 55,276.
[47] PreCheck NPRM, 78 Fed. Reg. at 55,658.
[48] *Id*.

Specifically, pursuant to 5 U.S.C. §§ 552a(k)(1) and (k)(2), DHS proposes to exempt the TSA PreCheck Application Database from: "5 U.S.C. 552a(c)(3); (d); e (1); e (4)(G), (H), (I), and (f)." These provisions of the Privacy Act ensure that:

- an agency must give individuals access to the accounting of disclosure of their records;[49]
- an individual may request access to records an agency maintains about him or her, as well as have a copy made;[50]
- the agency must permit the individual to amend a record about him or her and acknowledge the request in writing within 10 days, as well as timely correct the record if necessary or provide a reason for refusal of the proposed amendment, as well as allow a review of the refusal;[51]
- an agency must make notes of requested amendments within the records;[52]
- an agency must collect records "about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President";[53]
- an agency must publish the establishment or revision of the notice of the existence of records in the Federal Register, along with the procedures to be followed to obtain access, contest content, and learn the categories of sources or records in the system;[54]
- the agency shall promulgate rules establishing procedures that notify an individual in response to record requests pertaining to him or her, including "reasonable times, places, and requirements for identifying an individual", instituting disclosure procedures for medical and psychological records, create procedures, review amendment requests, as well as determining the request, the status of appeals to denial of requests, and establish fees for record duplication, excluding the cost for search and review of the record;[55]

DHS attempts to circumvent the intent of the Privacy Act in order to create a massive database that lacks accountability. DHS's proposed exemptions from 5 U.S.C. § 552a(c)(3), (d), (e)(4)(G), (H), (I), and (f) only serve to increase the secrecy of the database. DHS claims that accounting for disclosures,

[49] 5 U.S.C. § 552a(c)(3).
[50] 5 U.S.C. § 552a(d)(1).
[51] 5 U.S.C. §§ 552a(d)(2), (d)(3).
[52] 5 U.S.C. § 552a(d)(4).
[53] 5 U.S.C. §552a(e)(1).
[54] 5 U.S.C. §§ 552a(e)(4)(G), (H), (I).
[55] 5 U.S.C. §§ 552a(f)(1), (2), (3), (4), (5).

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.[56]

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.

When Congress enacted the Privacy Act in 1974, it sought to restrict the amount of personal data that Federal agencies were able to collect, and furthermore, required agencies to be transparent in their information practices.[57] 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: "in 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." [58]

The Privacy Act is intended to guard the privacy interests of citizens and lawful permanent residents against government intrusion. By allowing DHS to encroach on an individual's right to access and amend their information, DHS violates the intent of the Privacy Act. If DHS claims these exemptions, then the government fails to ensure the reliability of the data and fails to provide citizens with access to their personal data and opportunities to correct inaccurate or incomplete data.

[56] PreCheck NPRM, 78 Fed. Reg. at 55,658-59.
[57] S. Rep. No. 93-1183 at 1 (1974).
[58] *Doe v. Chao*, 540 U.S. 614, 618 (2004).

V. DHS's Proposed Routine Uses Contravene the Intent of the Privacy Act and Exceed the Authority of the Agency

The Privacy Act's definition of "routine use" is precisely tailored, and has been narrowly prescribed in the Privacy Act's statutory language, legislative history, and relevant case law. The TSA PreCheck Application Database contains a broad category of personally identifiable information. By disclosing information in a manner inconsistent with the purpose for which the information was originally gathered, DHS exceeds its statutory authority to disclose personally identifiable information without obtaining individual consent.

When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal information that federal agencies could collect and required agencies to be transparent in their information practices.[59] 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."[60]

The Privacy Act prohibits federal agencies from disclosing records they maintain "to any person, or to another agency" without the written request or consent of the "individual to whom the record pertains."[61] The Privacy Act also provides specific exemptions that permit agencies to disclose records without obtaining consent.[62] One of these exemptions is "routine use."[63] The TSA PreCheck Application system of records notice states that "all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3)."[64] "Routine use" means

[59] S. Rep. No. 93-1183 at 1 (1974).
[60] Pub. L. No. 93-579 (1974).
[61] 5 U.S.C. § 552a(b).
[62] *Id*. §§ 552a(b)(1) – (12).
[63] *Id*. § 552a(b)(3).
[64] PreCheck SORN, 78 Fed. Reg. at 55,276.

"with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected."[65]

The Privacy Act's legislative history and a subsequent report on the Act indicate that the routine use for disclosing records must be specifically tailored for a defined purpose for which the records are collected. The legislative history states that:

> [t]he [routine use] definition should serve as a caution to agencies to think out in advance what uses it will make of information. This Act is not intended to impose undue burdens on the transfer of information . . . or other such housekeeping measures and necessarily frequent interagency or intra-agency transfers of information. It is, however, intended to discourage the unnecessary exchange of information to another person or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material.[66]

The Privacy Act Guidelines of 1975—a commentary report on implementing the Privacy Act—interpreted the above Congressional explanation of routine use to mean that a "'routine use' must be not only compatible with, but related to, the purpose for which the record is maintained."[67]

Subsequent Privacy Act case law interprets the Act's legislative history to limit routine use disclosure based upon a precisely defined system of records purpose. In *United States Postal Service v. National Association of Letter Carriers, AFL-CIO*, the Court of Appeals for the D.C. Circuit relied on the Privacy Act's legislative history to determine that "the term 'compatible' in the routine use definitions contained in [the Privacy Act] was added in order to limit interagency transfers of information."[68] The Court of Appeals went on to quote the Third Circuit as it agreed, "[t]here must be a more concrete relationship or similarity, some meaningful degree of convergence, between the disclosing agency's purpose in gathering the information and in its disclosure."[69]

---

[65] 5 U.S.C. § 552a(a)(7).
[66] *Legislative History of the Privacy Act of 1974 S, 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).
[67] *Id*.
[68] *U.S. Postal Serv. v. Nat'l Ass'n of Letter Carriers, AFL-CIO*, 9 F.3d 138, 144 (D.C. Cir. 1993).
[69] *Id*. at 145 (quoting *Britt v. Natal Investigative Serv*., 886 F.2d 544, 549-50 (3d. Cir. 1989). *See also Doe v. U.S. Dept. of Justice*, 660 F.Supp.2d 31, 48 (D.D.C. 2009) (DOJ's disclosure of former AUSA's termination letter to Unemployment Commission was compatible with routine use because the routine use for collecting the personnel

DHS proposes to disclose TSA PreCheck Application information for purposes that do not relate to aviation security and screening. DHS states that it may disclose information within the TSA PreCheck Application Database with "other DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligences, or other homeland security functions."[70] These proposed disclosures transform the TSA PreCheck Application Database from a narrowly defined aviation security system of records to a general law enforcement repository. With its proposal, DHS fashions the TSA PreCheck Application Database as a virtual line up that law enforcement agencies may access for purposes other than aviation security. So, while TSA PreCheck applicants volunteer their sensitive information in the hopes of obtaining expedited airport screening, DHS intends to grant law enforcement blanket access to this information for non-TSA PreCheck purposes. The agency therefore exceeds its authority with this purpose and should not adopt it.

VI. Proposed Routine Uses G, I, and J Remove Privacy Act Safeguards by Disclosing Records to Foreign and International Agencies That are Not Subject to the Privacy Act

Proposed Routine Use G would permit DHS to disclose information:

> [t]o an appropriate federal, state, tribal, local, territorial, or foreign government law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, including criminal, civil, or regulatory violations, and such disclosure is proper and consistent with the official duties of the person making the disclosure.[71]

Proposed Routine Use I would permit DHS to disclose information:

> [t]o the appropriate federal, state, local, tribal, territorial, foreign governments, or other appropriate authority, regarding or to identify individuals who pose, or are under reasonable suspicion of posing, a risk to transportation or national security.[72]

---

file was to disclose to income administrative agencies); *Alexander v. F.B.I*, 691 F. Supp.2d 182, 191 (D.D.C. 2010) (FBI's routine use disclosure of background reports was compatible with the law enforcement purpose for which the reports were collected).

[70] PreCheck SORN, 78 Fed. Reg. at 55,275-6.

[71] *Id*. at 55,277.

[72] *Id*.

Proposed Routine Use J would permit DHS to disclose information:

> [t]o foreign governmental and international authorities, in accordance with law and formal or informal agreements.[73]

The provisions in these Routine Uses that would permit DHS to disclose information to foreign agencies and international agencies must be removed. The Privacy Act only applies to records maintained by United States government agencies.[74] Releasing information to foreign entities does not protect individuals covered by TSA PreCheck Application Database from Privacy Act violations. DHS does not have jurisdiction over foreign agents. Therefore, the provisions in these Routine Uses that would permit DHS to disclose information to foreign or multilateral entities must be removed.

VII. DHS's Proposed Routine Use K Contravenes the Legislative Intent of the Privacy Act

Proposed Routine Use K would permit the agency to disclose information:

> [t]o the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy. [75]

The limitations on disclosure in proposed Routine Use K is too broad to have any substantive effect, creates opportunities for violations of statutory rights, and goes against the legislative intent of the Privacy Act. As it stands, Routine Use K directly contradicts Congressman William Moorhead's testimony that the Privacy Act was "intended to prohibit gratuitous, ad hoc, disseminations for private or otherwise irregular purposes."[76]

---

[73] *Id*.
[74] 5 U.S.C. § 552a(b).
[75] PreCheck SORN, 78 Fed. Reg. at 55,277.
[76] Legislative History of the Privacy Act of 1974 S, 3418 (Public Law 93-579): Source Book on Privacy, 1031 (1976).

The phrase "when disclosure is necessary to preserve confidence in the integrity of DHS"[77] in Routine Use K is discordant with the Privacy Act because it gratuitously puts the face of the agency above an individual's right to privacy. The term "necessary" is overly ambiguous; DHS could take advantage of this criterion to unduly influence its image. DHS should remove this phrase from the proposed Routine Use because creating a category that is too broad can easily lead to the abuse of privacy rights of individuals whose data has been gathered and stored by DHS.

Conclusion

For the foregoing reasons, the proposed TSA PreCheck Application Database is contrary to the core purpose of the federal Privacy Act. Accordingly, DHS must narrow the scope of its proposed Privacy Act exemptions and not adopt its proposed unlawful routine use disclosures.

Respectfully submitted,

Marc Rotenberg
EPIC President and Executive Director

Khaliah Barnes
EPIC Administrative Law Counsel

Electronic Privacy Information Center (EPIC)
1718 Connecticut Avenue NW, Suite 200
Washington, D.C. 20009
(tel) 202 – 483 – 1140
(fax) 202 – 483 –1248

[77] PreCheck SORN, 78 Fed. Reg. at 55,277.