COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

DEPARTMENT OF HOMELAND SECURITY

on

DOCKET NOS. DHS-2007-0042 AND DHS-2007-0043

Notice of Privacy Act System of Records: U.S. Customs and Border Protection, Automated Targeting System, System of Records
and
Notice of Proposed Rulemaking: Implementation of Exemptions; Automated Targeting System

---

SEPTEMBER 5, 2007

TABLE OF CONTENTS

I. INTRODUCTION

By notices published on August 6, 2007, the Department of Homeland Security ("DHS") announced a new system of records notice for the Automated Targeting System ("ATS") and a rulemaking in which the agency "proposes to exempt certain records of the Automated Targeting System from one or more provisions of the Privacy Act."[1] On August 3, DHS released responses to questions about ATS raised by groups in the November 2006 system of records notice concerning the system.[2] The DHS Privacy Office also published a Privacy Impact Assessment for ATS on August 3.[3]

In December 2006, EPIC joined 29 organizations and 16 experts in privacy and technology submitted comments about the November 2006 system of records notice concerning ATS.[4] In those comments, we urged DHS to "(A) suspend the 'Automated Targeting System' as applied to individuals, or in the alternative, (B) fully apply all Privacy Act safeguards to any person subject to the Automated Targeting System." The Department of Homeland Security has done neither.

---

[1] Dep't of Homeland Sec., *Notice of proposed rulemaking: Implementation of Exemptions; Automated Targeting System*, 72 Fed. Reg. 43,567 (Aug. 6, 2007) [hereinafter "ATS Proposed Rulemaking"], *available at* http://edocket.access.gpo.gov/2007/E7-15198.htm; Dep't of Homeland Sec., *Notice of Privacy Act System of Records: U.S. Customs and Border Protection, Automated Targeting System*, 72 Fed. Reg. 43,650 (Aug. 6, 2007) [hereinafter "ATS System of Records Notice"], *available at* http://edocket.access.gpo.gov/2007/E7-15197.htm.

[2] Dep't of Homeland Sec., *Discussion of Public Comments Received on the Automated Targeting System System of Records Notice Published November 2, 2006*, Aug. 3, 2007 [hereinafter "DHS Response to November 2006 SORN"], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_publiccmts_cbp_atsupdate.pdf.

[3] Privacy Office, Dep't of Homeland Sec., *Privacy Impact Assessment for the Automated Targeting System*, Aug. 3, 2007 [hereinafter "ATS Privacy Impact Assessment"], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_atsupdate.pdf.

[4] Thirty Organizations and 16 Experts in Privacy and Technology, *Comments Urging the Department of Homeland Security To (A) Suspend the "Automated Targeting System" As Applied To Individuals, Or In the Alternative, (B) Fully Apply All Privacy Act Safeguards To Any Person Subject To the Automated Targeting System* (Dec. 4, 2006) [hereinafter "Coalition Comments on ATS"], *available at* http://epic.org/privacy/pdf/ats_comments.pdf; *see generally* EPIC, Automated Targeting System, http://www.epic.org/privacy/travel/ats/.

Though DHS has made changes to the system, they are not enough. All of the key characteristics of the Automated Targeting System – including the assessment, the basis for the assessment, the rules that apply, and the "targeting activities" – remain shrouded in mystery.

The Automated Targeting System was created to screen shipping cargo. Yet in 1999, without adequate notice and in violation of the Privacy Act, Customs and Border Protection began using ATS to conduct background checks on tens of millions of travelers and to assign secret terrorist ratings on U.S. citizens.[5] The categories of individuals covered by the system are expansive:

> A. Persons seeking to enter, exit, or transit through the United States by land, air, or sea. This includes passengers who arrive and depart the United States by air or sea, including those in transit through the United States on route to a foreign destination and crew members who arrive and depart the United States by air or sea, including those in transit through the United States on route to a foreign destination, and crew members on aircraft that over fly the United States.
>
> B. Persons who engage in any form of trade or other commercial transaction related to the importation or exportation of merchandise.
>
> C. Persons who are employed in any capacity related to the transit of merchandise intended to cross the United States border.
>
> D. Persons who serve as operators, crew, or passengers on any vessel, vehicle, aircraft, train, or other conveyance that arrives in or departs the United States.
>
> E. Persons who serve as booking agents, brokers, or other persons who provide information on behalf of persons seeking to enter, exit, or transit through the United States.[6]

Though DHS states that it does not create a terrorist "score," the agency does assign "risk assessments" to determine whether individuals will be subject to invasive searches of their persons or belongings, and whether U.S. citizens will be permitted to

[5] ATS System of Records Notice at 43,651, *supra* note 1.
[6] *Id*. at 43,653.

enter or exit the country.[7] In fact, DHS Chief Privacy Officer Hugo Teufel explained in August that the Automated Targeting System will be used to "intercept high-risk travelers, identify persons of concern, and identify patterns of suspicious activity."[8] As the agency notice makes clear, the ATS profiles may be integrated with other government databases and may be used for a wide variety of purposes.

According to DHS, ATS is made up of six modules. The two of interest are ATS-Passenger ("ATS-P") and ATS-Land ("ATS-L"). According to the DHS Privacy Office, ATS-P "is the module used at all U.S. airports and seaports receiving international flights and voyages to evaluate passengers and crewmembers prior to arrival or departure."[9] ATS-P's traveler screening relies upon "Advanced Passenger Information System (APIS), Non Immigrant Information System (NIIS), Suspect and Violator Indices (SAVI), the Department of State visa databases, the PNR information from the airlines, TECS crossing data, TECS seizure data, information from the consolidated and integrated terrorist watch list maintained by the TSC."[10]

As defined by DHS, "ATS-P processes available information from these databases to develop a risk assessment for each traveler."[11] The agency states:

> ATS-P does not use a score to determine an individual's risk level; instead, ATS-P compares PNR and information in the above-mentioned databases against lookouts and patterns of suspicious activity identified through past investigations and intelligence. This risk assessment is an analysis of the threat-based scenario(s) that a traveler matched when traveling on a given flight. These scenarios are drawn from previous and current law enforcement and intelligence information.[12]

---

[7] *Id*. at 43,651.
[8] Privacy Office, Dep't of Homeland Sec., *Statement by Homeland Security Chief Privacy Officer Hugo Teufel III on the Privacy Act System of Records Notice for the Automated Targeting System*, Aug. 3, 2007, *available at* http://www.dhs.gov/xnews/releases/pr_1186178812301.shtm.
[9] ATS Privacy Impact Assessment at 5, *supra* note 3.
[10] *Id*.
[11] *Id*.
[12] *Id*.

ATS-L is used to analyze and create risk assessments of private passenger vehicles crossing U.S. borders. ATS-L "process[es] and check[s] the license plate numbers of vehicles seeking to cross the border,"[13] allowing Customs and Border Protection "to cross-reference the TECS crossing data, TECS seizure data, and State Department of Motor Vehicle (DMV) data to employ the weighted rules-based assessment system of ATS."[14] DHS states that, "ATS-L provides, within seconds, a risk assessment for each vehicle that assists CBP officers at primary booths in determining whether to allow a vehicle to cross without further inspection or to send the vehicle for secondary evaluation."[15]

The Supreme Court has long recognized that citizens enjoy a constitutional right to travel. In *Saenz v. Roe*, the Court noted that the "'constitutional right to travel from one State to another' is firmly embedded in our jurisprudence."[16] For that reason, any government initiative that conditions the ability to travel upon the surrender of privacy rights requires particular scrutiny. Adherence to Privacy Act requirements is critical for a system such as the Automated Targeting System, which seeks to profile a massive amount of people, including every person "seeking to enter or exit the United States."

Incredibly, CBP proposes to exempt ATS from key fair information practices, such as the requirements that an individual be permitted access to personal information, that an individual be permitted to correct and amend personal information, and that an agency assure the reliability of personal information for its intended use.[17] It is inconceivable that the drafters of the Privacy Act would have permitted a federal agency

[13] *Id*.
[14] ATS Privacy Impact Assessment at 5, *supra* note 3.
[15] *Id*. at 5-6.
[16] 526 U.S. 489 (1999), quoting *United States v. Guest*, 383 U.S. 745 (1966).
[17] ATS System of Records Notice at 43,653, *supra* note 1; *see generally* 5 U.S.C. § 552a (1974).

to propose a secret profiling system on U.S. citizens and be granted broad exemptions from Privacy Act obligations.

DHS itself states that the Automated Targeting System's "risk assessments" are substantial reviews of individuals. DHS states that it uses ATS "[i]n lieu of manual reviews of traveler information and intensive interviews with every traveler arriving in or departing from the United States."[18] Automated Targeting System significantly affects millions of individuals per year.

Today, we write to again to urge the Department of Homeland Security to (A) suspend the "Automated Targeting System" as applied to individuals, or in the alternative, (B) fully apply all Privacy Act safeguards to any person subject to the Automated Targeting System. Such action is the only way to ensure the privacy and civil liberty rights of citizens are protected.

II. DHS HAS EXPANDED AUTOMATED TARGETING SYSTEM'S BROAD EXEMPTIONS, WHICH CONTRAVENE INTENT OF PRIVACY ACT OF 1974

Though we detailed in our December 2006 comments the many ways in which the Automated Targeting System's broad exemptions contravened the intent of the Privacy Act of 1974, the Department of Homeland Security did not narrow the exemptions proposed for Automated Targeting System, but instead included more exemptions in this new system of records notice.[19] These broad exemptions for law enforcement agencies and "investigatory materials collected for law enforcement purposes" would allow CBP to use this massive database with little accountability.

[18] ATS System of Records Notice at 43,651, *supra* note 1
[19] *See generally* Coalition Comments on ATS, *supra* note 4.

CBP proposes exempting ATS from all Privacy Act provisions guaranteeing citizens the right to access records containing information about them and provisions defining the government's obligation to allow citizens to challenge the accuracy of information contained in their records. The exemptions proposed are: "5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (5), and (8); (f), and (g)) pursuant to 5 U.S.C. 552a(j)(2) and (k)(2))."[20] These include all of the exemptions CBP proposed in November 2006, and adds 5 U.S.C. 552a(c)(4); (e)(2), (3), (5) and (8), and (g).[21] These provisions of the Privacy Act ensure:

- an agency must give individuals access to the accounting of disclosure of their records[22];
- any agency or individual to whom the records are disclosed must also receive "any correction or notation of dispute"[23];
- individual may request access to records an agency maintains about him or her[24];
- an agency must correct identified inaccuracies promptly;[25]
- an agency must make notes of requested amendments within the records;[26]
- an agency must ensure it only collects data "relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive order of the President"[27];
- an agency must "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs"[28];

[20] ATS System of Records Notice at 43,653, *supra* note 1.
[21] ATS Proposed Rulemaking at 43,568 – 43,569, *supra* note 1.
[22] 5 U.S.C. § 552a(c)(3).
[23] 5 U.S.C. § 552a(c)(4).
[24] 5 U.S.C. § 552a(d)(1).
[25] 5 U.S.C. § 552a(d)(2)(B), (d)(3)
[26] 5 U.S.C. § 552a(d)(4).
[27] 5 U.S.C. § 552a(e)(1).
[28] 5 U.S.C. § 552a(e)(2).

- each individual must be informed whom the agency asks to supply information[29];
- an agency must publish a notice of the existence of records in the Federal Register, along with the procedures to be followed to obtain access[30];
- an agency must establish procedures to handle disputes between the agency and individual as to the accuracy of the records[31]; and,
- an individual may seek judicial review to enforce the statutory right of access provided by the Act.[32]

As we explained in our December 2006 comments, when it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal data that Federal agencies could collect and required agencies to be transparent in their information practices.[33] 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:

> "[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.[34]

The Privacy Act is intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government[.]"[35] It is also intended to guard the privacy interests of citizens and lawful permanent residents against government intrusion. Congress found that "the privacy of an individual is directly

---

[29] 5 U.S.C. § 552a(e)(3).
[30] 5 U.S.C. §§ 552a(e)(4)(G), (e)(4)(H), (f).
[31] 5 U.S.C. § 552a(f)(4).
[32] 5 U.S.C. § 552a(g)(1).
[33] S. Rep. No. 93-1183 at 1 (1974).
[34] *Doe v. Chao*, 540 U.S. 614, 618 (2004).
[35] S. Rep. No. 93-1183 at 1.

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."[36] It thus sought to "provide certain protections for an individual against an invasion of personal privacy" by establishing a set of procedural and substantive rights.[37]

The rights of access and correction were central to what Congress sought to achieve through the Privacy Act:

> The committee believes that this provision is essential to achieve an important objective of the legislation: Ensuring that individuals know what Federal records are maintained about them and have the opportunity to correct those records. The provision should also encourage fulfillment of another important objective: maintaining government records about individuals with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to individuals in making determinations about them.[38]

Customs and Border Protection's notice establishes a system that provides neither adequate access nor the ability to amend or correct inaccurate, irrelevant, untimely and incomplete records. CBP allows individuals to petition through the Traveler Redress Inquiry Program to access any passenger name record ("PNR") data that the individual himself gave to an air carrier or travel agent, but no other information in Automated Targeting System files. And, DHS claims this poor attempt at access and correction of data is its policy, not that the agency is required under law to allow access and correction of individual data. Specifically, DHS states:

> *DHS policy allows* persons (including foreign nationals) to access and redress under the Privacy Act to raw PNR data maintained in ATS-P. The PNR data, upon request, may be provided to the requester in the form in which it was collected from the respective carrier, but may not include certain business confidential information of the air carrier that is also contained in the record, such

[36] 5 U.S.C. § 552a.
[37] *Id*.
[38] H.R. Rep. No. 93-1416, at 15 (1974).

> as . [sic] This access does not extend to other information in ATS obtained from official sources (which are covered under separate SORNs) or that is created by CBP, such as the targeting rules and screening results, which are law enforcement sensitive information and are exempt from certain provisions of the Privacy Act. For other information in this system of records, individuals generally may not seek access for purposes of determining if the system contains records pertaining to a particular individual or person. (emphasis added)[39]

Not only is DHS restricting individuals from accessing or correcting "other information in ATS obtained from official sources (which are covered under separate SORNs) or that is created by CBP, such as the targeting rules and screening results," which DHS believes to be "law enforcement sensitive information and are exempt from certain provisions of the Privacy Act," but also any "other information in this system of records."[40] Even if we grant that the "targeting rules and screening results" are exempt, it is in fact, improper to conceal unclassified data by mixing it with classified data. By refusing to allow access to all Automated Targeting System data except that which the individual has personally provided, the Department of Homeland Security seeks to keep the Automated Targeting System opaque and arbitrary.

This secrecy is a violation of privacy laws, according to the Government Accountability Office in a recent review of Customs and Border Protection and its traveler prescreening programs, including ATS.[41] In a May report to Congress, GAO explained that "CBP's current disclosures do not fully inform the public about all of its systems for prescreening aviation passenger information nor do they explain how CBP combines data in the prescreening process, as required by law. As a result, passengers are not assured that their privacy is protected during the international passenger prescreening

[39] ATS System of Records Notice at 43,653, *supra* note 1.
[40] *Id.*
[41] Gov't Accountability Office, *Aviation Security: Efforts to Strengthen International Passenger Prescreening are Under Way, but Planning and Implementation Issues Remain,* GAO-07-346 (May 2007), *available at* http://www.gao.gov/new.items/d07346.pdf.

process."[42] DHS needs to be more forthcoming about the Automated Targeting System in order to ensure adequate protection of travelers' privacy and security rights.

III. DATA CONCERNING RACE, ETHNICITY OR POLITICAL AFFILIATION MAY BE USED IN ATS 'RISK ASSESSMENTS'

The only data that individuals are allowed to see or correct under DHS's proposal is data related to "passenger name records" ("PNR"). Such records can include up to 19 categories of data. Besides the usual name, credit card information, and travel dates, PNR also can contain "general remarks including Other Service Indicated (OSI), Special Service Indicated (SSI) and Supplemental Service Request (SSR) information."[43] It is possible for PNR to "include information that could directly indicate the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, or sex life of the individual."[44]

Though CBP claims "it does not unconstitutionally discriminate based on religion, nationality, ethnicity, race, or gender," and that it "employs an automated system that filters certain of these terms," CBP also admits that it is possible for the agency to gather, retain, and use such data in the Automated Targeting System's "risk assessments."[45] This raises the distinct possibility that travelers will be discriminated against based upon race, political ideology, religious or sexual beliefs, among other personal matters.

---

[42] *Id*. at 25.
[43] ATS System of Records Notice at 43,653, *supra* note 1.
[44] *Id*.
[45] *Id*.; DHS Response to November 2006 SORN at 23, *supra* note 2.

IV. ATS'S REDRESS PROCEDURES ARE INADEQUATE AND FLAWED

DHS proposes in its Federal Register notices to exempt the Automated Targeting System from the judicially enforceable rights of access and correction under the Privacy Act. In its place, DHS proposes poor substitutes. The individual may petition for access to his PNR data in ATS through a "Privacy Act Access Request" sent to Customs and Border Protection or through the Traveler Redress Inquiry Program ("TRIP").[46]

In February comments to the Department of Homeland Security, EPIC detailed the many privacy and security problems in TRIP, and urged DHS to fully apply Privacy Act requirements of notice, access, correction, and judicially enforceable redress to TRIP and the underlying system of watch lists.[47] Full application of the Privacy Act requirements to government record systems is the only way to ensure that data is accurate and complete, which is especially important in the context of watch lists and the Automated Targeting System, where mistakes and misidentifications are costly.

TRIP is described as "a central gateway to address watch list misidentification issues, situations where individuals believe they have faced screening problems at immigration points of entry, or have been unfairly or incorrectly delayed, denied boarding or identified for additional screening at our nation's transportation hubs."[48] EPIC explained in February, that, because TRIP provides a central system for submitting,

---

[46] ATS Privacy Impact Assessment at 22, *supra* note 3.

[47] EPIC, *Comments on Docket No. DHS 2006-0077: Privacy Act; Redress and Response System of Records and Docket Number DHS-2007-0003: Privacy Act of 1974: Implementation of Exemptions; Redress and Response Records System* (Feb. 20, 2007) [hereinafter "EPIC Comments on TRIP"], *available at* http://www.epic.org/privacy/airtravel/profiling/trip_022007.pdf

[48] Press Release, Dep't of Homeland Sec., *DHS to Launch Traveler Redress Inquiry Program*, Jan. 17, 2007, *available at* http://www.dhs.gov/xnews/releases/pr_1169062569230.shtm.

directing and tracking, but not resolving complaints, it fails to resolve the significant problems in current traveler redress procedures.[49]

It is unknown how a person would know that there is incorrect information in ATS when the system cannot be accessed under the Privacy Act for inspection. In fact, the only indication a traveler may have that the government is keeping records about him is if he is subjected to extra scrutiny, detained or arrested at the border. This secrecy conflicts with the purposes of the Privacy Act, which was intended to provide an enforceable right of access to personal information maintained by government agencies. TRIP is not an adequate replacement for the judicially enforceable rights of access and correction enshrined in the Privacy Act.

V. UNDERLYING DATABASES USED BY AUTOMATED TARGETING SYSTEM ARE ERROR-FILLED

According to the Privacy Impact Assessment for ATS, the DHS Privacy Office states that the prescreening program "uses data obtained from other governmental information systems including: […] airline reservation data; nonimmigrant entry records; and records from secondary referrals, CBP incident logs, suspect and violator indices, state Department of Motor Vehicle Records (for vehicle license plate numbers), [terrorist screening database records], seizure records, and law enforcement lookout information."[50] A major part of terrorist screening database records is the watch lists, which we have repeatedly explained are filled with holes.

Under the Aviation and Transportation Security Act of 2002, the Transportation Security Administration ("TSA") was authorized to maintain watch lists of names of

[49] EPIC Comments on TRIP at 4-5, *supra* note 47.
[50] ATS Privacy Impact Assessment at 5, *supra* note 3.

individuals suspected of posing "a risk of air piracy or terrorism or a threat to airline or passenger safety."[51] Documents obtained in 2002 by EPIC from TSA under the Freedom of Information Act established that the agency administers two lists: a "no fly" list and a "selectee" list.[52] The lists are sent to the airlines, which run passenger names against the watch lists.

When a passenger checks in for a flight, he may be labeled a threat if his name matches an entry on one of the watch lists, even if he is not the person actually on the list. A match to the "no fly" list requires the airline to notify TSA and to call a law enforcement officer to detain and question the passenger. In the case of a Selectee, an "S" or special mark is printed on the individual's boarding pass and the person receives additional security screening. Customs and Border Protection also uses the lists to screen travelers. Many travelers have reported problems with being mistakenly matched to names on watch lists.

The accuracy and effectiveness of the watch lists are in question. In August, it was revealed that "the government's terrorist screening database flagged Americans and foreigners as suspected terrorists almost 20,000 times last year. But only a small fraction of those questioned were arrested or denied entry into the United States."[53] CBP logged about 10,000 of those encounters, but only "turned back or handed over to authorities 550, most of them foreigners."[54]

---

[51] Pub. L. No. 107-71, 115 Stat. 597 (2002).
[52] EPIC, *Documents Show Errors in TSA's "No-Fly" Watchlist*, http://www.epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html.
[53] Fed. Bureau of Investigations, Dep't of Justice, *FY 2008 Authorization Budget Request to Congress* (2007), *available at* http://www.fas.org/irp/agency/doj/fbi/2008just.pdf; Ellen Nakashima, *Terror Suspect List Yields Few Arrests*, Wash. Post, Aug. 25, 2007.
[54] *Id.*

There have been myriad stories about mistakes associated with the watch lists, with sometimes chilling results. An April 2006 report by the Department of Homeland Security's Privacy Office on the impact of the watch lists explained that "individuals who are mistakenly put on watch lists or who are misidentified as being on these lists can potentially face consequences ranging from inconvenience and delay to loss of liberty."[55] The report described complaints "alleg[ing] misconduct or disrespect by airline, law enforcement, TSA or CBP officials" toward people mistakenly matched.[56] According to the Privacy Office:

> reported experiences of individuals whose names appear to match names on the No-fly and Selectee lists can be trying and unpleasant. Complaints filed with CRCL have alleged that individuals have experienced long delays, have been separated from members of their family and given no explanation or conflicting explanations about what is going on. Some complaints alleged that officers have asked […] whether one traveler knew anyone at his mosque who hates Americans or disagrees with current policies, targeted a traveler for additional screening because she wore traditional Muslim attire and told another traveler that he and his wife and children were subjected to body searches because he was born in Iraq, is Arab, and Muslim.[57]

Also, documents recently obtained by EPIC under the Freedom of Information Act show nearly a hundred complaints from airline passengers between November 2003 and May 2004 about the government's traveler screening security measures.[58] The complaints describe the bureaucratic maze passengers encounter if they happen to be mistaken for individuals on the list, as well as the difficulty they encounter trying to exonerate themselves through the redress process. One person named in the documents,

---

[55] Privacy Office, Dep't of Homeland Sec., *Report Assessing the Impact of the Automatic Selectee and No Fly Lists on Privacy and Civil Liberties as Required Under Section 4012(b) of the Intelligence Reform and Terrorism Prevention Act of 2004* i (Apr. 27, 2006), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_nofly.pdf.
[56] *Id*. at 18.
[57] *Id*.
[58] Transp. Sec. Admin., Dep't of Homeland Sec., *Complaint Log: Nov. 2003 to May 2004,* obtained by EPIC through FOIA litigation, *available at* http://www.epic.org/privacy/airtravel/foia/complaint_log.pdf.

Sister Glenn Anne McPhee, U.S. Conference of Catholic Bishops' secretary for education, spent nine months attempting to clear her name from a TSA watch list. The process was so difficult, Sister McPhee told a reporter, "Those nine months were the closest thing to hell I hope I will ever experience."[59]

In January, at a hearing of the Senate Commerce Committee, Sen. Ted Stevens complained that his wife, Catherine, is frequently mismatched to the watch list name "Cat Stevens."[60] Senators Ted Kennedy and Don Young are among those who have been improperly flagged by watch lists.[61] Sen. Kennedy was able to resolve the situation only by enlisting the help of then-Homeland Security Secretary Tom Ridge.

In 2005, Congress ordered the Government Accountability Office to investigate TSA's airline passenger screening programs. GAO found significant problems with handling of personal information and violations of privacy laws.[62] In September, GAO reviewed the watch list system and found "about half of the tens of thousands of potential matches sent to the center between December 2003 and January 2006 for further research turned out to be misidentifications."[63] According to the GAO, these misidentifications are a significant problem, and they:

> highlight the importance of having a process -- often referred to as redress -- for affected persons to express their concerns, seek correction of any inaccurate data, and request other actions to reduce or eliminate future inconveniences. Similarly,

---

[59] Ryan Singel, *Nun Terrorized by Terror Watch*, Wired News, Sept. 26, 2005.
[60] Beverley Lumpkin, *Aviation Security Chief Says No-Fly List is Being Reduced by Half*, Associated Press, Jan. 18, 2007.
[61] *See, e.g.,* Sara Kehaulani Goo, *Committee Chairman Runs Into Watch-List Problem*, Wash. Post, Sept. 30, 3004; Leslie Miller, *House Transportation Panel Chairman Latest to be Stuck on No-Fly List*, Associated Press, Sept. 29, 2004; Shaun Waterman, *Senator Gets a Taste of No-Fly List Problems*, United Press Int'l, Aug. 20, 2004.
[62] Gov't Accountability Office, *Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public*, GAO-05-864R (July 22, 2005), *available at* http://www.gao.gov/new.items/d05864r.pdf.
[63] Gov't Accountability Office, *Terrorist Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public,* GAO-06-1031 (Sept. 2006), *available at* http://www.gao.gov/new.items/d061031.pdf.

> such a process would apply to other persons affected by the maintenance of watch list data, including persons whose names are actually on the watch list but should not be ("mistakenly listed persons") as well as persons who are properly listed.[64]

Also, according to the director of TSA's redress office, "some customers (air passengers) call and complain about having problems even though they have taken the necessary steps to be placed on the cleared list."[65] The watch lists remain filled with errors, and these problems need to be resolved before they are used in yet another passenger profiling system to restrict the movement of U.S. citizens.

VI. MORE ACCESS AND TRANSPARENCY IS NEEDED, AS THE SYSTEM'S ACCURACY AND EFFECTIVENESS ARE IN QUESTION

In December 2006, we explained that there are significant questions about the accuracy and effectiveness of Automated Targeting System, and urged against the use of this flawed program on travelers.[66] The Government Accountability Office reported in March 2006 that there are significant questions about the system. The office's review of ATS showed that CBP "currently does not have reasonable assurance that ATS is effective," testified Richard M. Stana, Director of Homeland Security and Justice Issues at the Government Accountability Office, at a Senate committee hearing in March.[67] Stana also questioned the accuracy and reliability of ATS risk assessments. "CBP does not yet have key internal controls in place to be reasonably certain that ATS is providing the best available information to allocate resources for targeting and inspecting that are

---

[64] *Id*. at 2.
[65] *Id*. at 34.
[66] Coalition Comments on ATS at 12-14, *supra* note 4.
[67] Richard M. Stana, Dir., Homeland Sec. & Justice Issues, Gov't Accountability Office, *Testimony at a Hearing on Neutralizing the Nuclear and Radiological Threat: Securing the Global Supply Chain (Part Two) Before the Subcom. on Investigations of the S. Comm. on Homeland Security and Governmental Affairs*, 109th Cong. (Mar. 30, 2006), *available at* http://www.gao.gov/new.items/d06591t.pdf.

the highest risk and not overlook inspecting containers that pose a threat to the nation."[68] These criticisms remain even after GAO suggested improvements to the system in 2004.

These accuracy and effectiveness questions are especially important as the Automated Targeting System will retain the risk assessments for 15 years, even assessments of people who are not considered a threat.[69] Though we support the reduction from 40 years to 15 years of the time data will be retained in Automated Targeting System, this is not enough.[70]

According to the system of records notice, "CBP has determined that it can continue to uncover and use information relating to terrorism and other serious crimes within this shorter retention period."[71] However, even 15 years is too long to retain such data, yet there is no real explanation of why the period of 15 years was chosen, or why CBP initially insisted that it needed to keep Automated Targeting System records for 40 years.

VII. AUTOMATED TARGETING SYSTEM STILL ALLOWS MANY FEDERAL AGENCIES TO IMPROPERLY ACCESS THE PROFILES

Though we applaud the Department of Homeland Security for rejecting the most egregious of the "routine uses" set out in the November 2006 notice for the Automated Targeting System, we are disappointed that DHS continues to propose broad routine use

---

[68] *Id*. at 5-6.
[69] ATS System of Records Notice at 43,653, *supra* note 1.
[70] "Additionally, the following further access restrictions pertain to the retention and use of PNR, which is contained only in ATS-P: ATS-P users will have general access to PNR for seven years, after which time the PNR data will be moved to dormant, non- operational status. PNR data in dormant status will be retained for eight years and may be accessed only with approval of a senior DHS official designated by the Secretary of Homeland Security and only in response to an identifiable case, threat, or risk." Also, "[n]otwithstanding the above, information that is maintained only in ATS that is linked to law enforcement lookout records, CBP matches to enforcement activities, investigations or cases (*i.e.,* specific and credible threats, and flights, individuals and routes of concern, or other defined sets of circumstances)—will remain accessible for the life of the law enforcement matter." DHS Response to November 2006 SORN at 9, *supra* note 2.
[71] ATS System of Records Notice at 43,652, *supra* note 1.

categories, allowing for potential disclosure to virtually any government agency worldwide for an array of actual or potential undefined violations.[72] In December 2006, we explained that "these categories are so broad as to be almost meaningless," and they remain so under the new system of records notice.[73]

DHS was correct to delete the routine uses described in the November 2006 notice that would have allowed access to Automated Targeting System files for background checks and hiring decisions. Yet it sets out a breathtakingly wide list of categories of individual who may access ATS files. These include:

> A. To appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where CBP believes the information would assist enforcement of applicable civil or criminal laws; [. . . and]
>
> C. To an organization or individual in either the public or private sector, either foreign or domestic, where there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, or where the information is relevant to the protection of life, property, or other vital interests of a data subject and such disclosure is proper and consistent with the official duties of the person making the disclosure.[74]

In our December 2006 comments, we explained that routine use C (then labeled routine use H) is questionable. We said:

> The Privacy Act [(b)(8)] already has a procedure for disclosing information pursuant to a showing of compelling circumstances. Routine use H duplicates and weakens the statutory condition of disclosure. Moreover, it does not include the disclosure notification to the individual required by the statute. The agency is seeking to evade an important notification procedure required by the statute. It may not do so by its creative invocation of the routine use exception. (internal citations omitted.)[75]

---

[72] *Id*. at 43,652 – 43,653.
[73] Coalition Comments on ATS at 14, *supra* note 4.
[74] ATS System of Records Notice at 43,654, *supra* note 1.
[75] Coalition Comments on ATS at 15, *supra* note 4.

In its published response to comments submitted in response to the November 2006 notice about the Automated Targeting System, the Department of Homeland Security did not respond to our statement. We remain in the dark about the agency's reasons for proposing this duplicative routine use.

The agency also proposes to disclose all or portion of the records or information contained in the system outside of DHS when "it is suspected or confirmed that the security or confidentiality of information in the system of record has been compromised" and for other purposes.[76] This is a routine use also proposed in the November 2006 notice. At that time, we said:

> [t]his routine use would stand the presumption of the Privacy Act on its head. Instead of the agency making known to the individual information in the possession of the agency that could have an adverse impact, it would make the information widely known across to the federal government while keeping it secret from the person whose interests are supposed to be protected by the Privacy Act.[77]

In its published response to comments submitted in response to the November 2006 notice about the Automated Targeting System, the Department of Homeland Security confirmed our statement about this routine use [then O, now M]. DHS said, "Routine use O was added in response to recent information breaches at other agencies. This routine use was crafted by the Department of Justice in its work on the Identity Theft Task Force."[78] DHS continued, stating "[t]he commenter is correct that disclosures within the Department are covered by (b)(1); however, this routine use is not meant to cover this

[76] ATS System of Records Notice at 43,654, *supra* note 1.
[77] Coalition Comments on ATS at 15, *supra* note 4.
[78] DHS Response to November 2006 SORN at 15, *supra* note 2.

situation. Rather, following a breach DHS may need to share information with entities to facilitate notifying the affected individuals or conducting an investigation."[79]

It is clear that the data would be widely known not only across to the federal government but also to unnamed third parties, while DHS continues to keep the data secret from the person whose interests are supposed to be protected by the Privacy Act. This is a strange use of the Privacy Act exemptions.

If the Automated Targeting System is exempted from these Privacy Act provisions, then the government fails to ensure the reliability of the data, provide citizens with access to their personal data, or opportunities to correct inaccurate or incomplete data. These are significant failures, the Automated Targeting System's "risk assessments" will affect every citizen who travels into or exits from the United States. They will determine whether individuals will be subject to invasive searches of their persons and belongings, or be permitted to cross the border.

VIII. CONCLUSION

For the foregoing reasons, the Automated Targeting System should not be used to establish secret profiles on individuals subject to Privacy Act safeguards. We urge the agency to suspend this activity.

If the program goes forward, CBP must revise its Privacy Act notice for the Automated Targeting System to 1) provide individuals judicially enforceable rights of access and correction; 2) limit the collection and distribution of information to only those necessary for the screening process, and 3) substantially limit the routine uses of

[79] *Id.*

information. The recent changes to the Automated Targeting System are not enough to ensure the protection of the privacy and civil liberty rights of citizens.

Respectfully submitted,

_____

Marc Rotenberg
Executive Director

_____

Melissa Ngo
Senior Counsel

ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, DC 20009
(202) 483-1140

Filed: September 5, 2007