DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Docket No. TSA-2004-17982
Privacy Act Notice
Registered Traveler Operations Files

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

By notice published on June 1, 2004, the Transportation Security Administration ("TSA") established a system of records (DHS/TSA 015 — Registered Traveler Operations Files) to conduct the Registered Traveler Pilot Program ("Registered Traveler").[1] According to the notice, the Registered Traveler program

> is designed to pre-screen and positively identify volunteer travelers using advanced identification technologies and conduct a terrorist-focused background check to ensure that the volunteer is not connected to terrorists or terrorist activity. This system may expedite the pre-boarding process for the traveler and improve the allocation of TSA's security resources on individuals who may pose a security threat.[2]

Pursuant to this TSA notice, the Electronic Privacy Information Center ("EPIC") submits these comments to address the substantial privacy issues raised by the Registered Traveler program and the new system of records established to facilitate the program. EPIC requests that TSA substantially revise its Privacy Act notice prior to implementation of the final phase of Registered Traveler.

The Supreme Court recently underscored the importance of the Privacy Act's restrictions upon agency use of personal information to protect privacy interests, noting that:

---

[1] Privacy Act Notice, 69 Fed. Reg. 30948 (June 1, 2004).
[2] *Id*. at 30949.

> "[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.[3]

TSA's notice for the Registered Traveler system of records, however, exempts the system from many protections the Privacy Act is intended to provide. As proposed in the notice, Registered Traveler is a program for which TSA is asking individuals to volunteer information that will be used to conduct potentially invasive background checks in exchange for the determination that they have a relatively low likelihood of being terrorists or connected to terrorists, and may be subject to less security screening than others prior to boarding airplanes. However, TSA has unnecessarily exempted the system from crucial safeguards intended to promote record accuracy and secure the privacy of individuals whose information is maintained within the system. TSA will be under no legal obligation to inform the public of the categories of information contained in the system or provide the ability to access and correct records that are irrelevant, untimely or incomplete. The program will contain information that is unnecessary and wholly irrelevant to the determination of whether an individual poses a threat to aviation security.

Given TSA's checkered record of privacy protection in developing other systems of records, EPIC urges the agency to suspend Registered Traveler until it fully evaluates the privacy implications of this program and revises its information collection and maintenance practices to comply fully with the intent of the Privacy Act.

[3] *Doe v. Chao*, No. 02-1377, slip op. at 3 (Feb. 24, 2004).

I. TSA Has a History of Secrecy and Privacy Insensitivity

Although TSA was created less than three years ago, the agency's brief history has been marked by a lack of transparency and little regard for individual privacy interests. Given this unimpressive record, TSA should not unnecessarily exempt a system of records from crucial requirements intended to ensure the rights of individuals to control their personal information.

EPIC has repeatedly found through its Freedom of Information Act ("FOIA") work that TSA is not forthcoming with records of its activities, even though the public is by law entitled to such information. Soon after enactment of the Aviation and Transportation Security Act, Pub. L. No. 10771, and the creation of TSA, EPIC began seeking information from the agency under the FOIA about the potential privacy impact of the second generation Computer Assisted Passenger Prescreening System ("CAPPS II") and other aviation security initiatives. The first such requests were submitted in February 2002, seeking, *inter alia*, "records concerning the development of airline passenger screening/profiling systems." When the agency failed to respond in a timely manner, EPIC filed suit in U.S. District Court.[4] TSA ultimately withheld the vast majority of responsive records on the grounds that they were "predecisional" and constituted "sensitive security information" ("SSI") under 49 CFR Part 1520. In October 2002, EPIC requested information from TSA concerning the agency's creation and maintenance of "no-fly lists." Again, TSA failed to comply with the FOIA's time limits and EPIC filed suit.[5] Upon processing the FOIA request, TSA released records demonstrating that a substantial number of passengers had been misidentified as a result

[4] *EPIC v. Department of Transportation*, Civ. No. 02-475 (D.D.C.).
[5] *EPIC v. Transportation Security Administration*, Civ. No. 02-2437 (D.D.C.).

of the agency's "selectee" and "no-fly" lists, but withheld significant amount of material as SSI. In March 2003, EPIC sought TSA records reflecting the agency's assessment of the "potential privacy and/or civil liberties implications of the activities planned or proposed for the CAPPS II project." Upon TSA's failure to respond within the statutory timeframe, EPIC again sought judicial relief.[6] As with the previous FOIA requests, a vast amount of responsive material was withheld. EPIC again found it necessary to seek the court's intervention when TSA refused to expedite the processing of a request for two specific documents — the Privacy Impact Assessment[7] and the "Capital Asset Plan and Business Case" for the CAPPS II project.[8] EPIC's request for expedition was premised upon the obvious relevance of the requested information to the Privacy Act notice at issue here and the approaching deadline for public comments. Most recently, EPIC filed suit against TSA in June 2004 to seek the immediate processing of three FOIA requests related to the agency's role in commercial airline disclosures of passenger data to the government. TSA granted expedited processing for all the requests, but failed to disclose the requested information within the time prescribed by law.[9]

In addition to lack of transparency, TSA also has a long history of disregard for personal privacy in its information handling practices. A February 2004 report from the General Accounting Office ("GAO"), Congress' investigative arm, found that TSA has failed to provide adequate justification for the Privacy Act exemptions it claimed for CAPPS II.[10] The GAO found:

---

[6] *EPIC v. Department of Homeland Security*, Civ. No. 03-1255 (D.D.C.).
[7] At the writing of these comments, TSA has yet to release a Privacy Impact Assessment for CAPPS II.
[8] *EPIC v. Transportation Security Administration*, Civ. No. 03-1846 (D.D.C.).
[9] *EPIC v. Department of Homeland Security*, Civ. No. 04-0944 (D.D.C.).
[10] General Accounting Office, *Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, GAO-04-385 (Feb. 2004) 23 ("GAO Report").

> TSA published a proposed rule to exempt the system from seven Privacy Act provisions but has not yet provided the reasons for these exemptions, stating that this information will be provided in a final rule to be published before the system becomes operational. As a result, TSA's justification for these exemptions remains unclear. Until TSA finalizes its privacy plans for CAPPS II and addresses such concerns, we lack assurance that the system will fully comply with the Privacy Act.[11]

Also in February 2004, the Department of Homeland Security Privacy Office released a report on TSA's role in the JetBlue Airways transfer of passenger data to a Defense Department contractor, which found that "TSA employees involved acted without appropriate regard for individual privacy interests or the spirit of the Privacy Act of 1974."[12] The report ordered the employees involved in the transfer to undergo Privacy Act and privacy policy training.[13]

Most recently, TSA Acting Administrator Admiral David Stone admitted to the Senate Governmental Affairs Committee that in 2002 TSA facilitated the transfer of passenger data from American Airlines, Continental Airlines, Delta Airlines, America West Airlines, Frontier Airlines, and JetBlue Airways to TSA "cooperative agreement recipients" for purposes of CAPPS II testing, as well as to the Secret Service and IBM for other purposes.[14] Stone also stated that Galileo International and "possibly" Apollo, two central airline reservation companies, had provided passenger data to recipients working on behalf of TSA.[15] Further, TSA directly obtained passenger data from JetBlue and Sabre, another central airline reservation company, for CAPPS II development.[16] TSA

---

[11] *Id*.
[12] Department of Homeland Security Privacy Office, *Report to the Public on Events Surrounding jetBlue Data Transfer* (Feb. 2004) 9 ("Privacy Office Report").
[13] *Id*.
[14] *See U.S. Senate Committee on Governmental Affairs Pre-hearing Questionnaire for the Nomination of Admiral David Stone to be Assistance Secretary of Homeland Security, Transportation Security Administration* 17, 19, *available at* http://www.epic.org/privacy/airtravel/stone_answers.pdf.
[15] *Id*.
[16] *Id*. at 19.

did not observe Privacy Act requirements with regard to any of these collections of information.[17] Stone's admission followed repeated denials to the public, Congress, General Accounting Office, and Department of Homeland Security Privacy Office that TSA had acquired or used real passenger data to test CAPPS II.[18]

In light of the fact that TSA's actions have repeatedly raised questions about the agency's lack of transparency and commitment to individual privacy, it is vital that the agency comply with the dictates of the Privacy Act in its creation of the Registered Traveler system of records, and not claim exemptions from the law unless necessary and justifiable.

II. TSA's Notice Evades the Government Transparency that the Privacy Act is Intended to Provide

Under the Privacy Act, government transparency is the rule rather than the exception. Although TSA has listed in this notice the categories of records it currently intends to collect for Registered Traveler, the agency has frustrated the Privacy Act's goal of transparency by exempting the Registered Traveler system of records from the requirement that TSA publish "the categories of sources of records in the system."[19] In the future, therefore, TSA leaves open the option to cull Registered Traveler information from categories of records not included in this notice without informing the public.

---

[17] *Id*. at 18.

[18] *See, e.g*., Ryan Singel, *More False Information From TSA*, Wired News, June 23, 2004 ("After the JetBlue transfer was brought to public attention in September 2003, TSA spokesman Brian Turmail told Wired News that the TSA had never used passenger records for testing CAPPS II, nor had it provided records to its contractors. In September 2003, Wired News asked TSA spokesman Nico Melendez whether the TSA's four contractors had used real passenger records to test and develop their systems. Melendez denied it, saying, 'We have only used dummy data to this point.'"); *U.S. Representative John Mica (R-FL) Holds Hearing on Airline Passenger Profiling Proposal: Hearing Before the Aviation Subcomm. of the House Transportation and Infrastructure Comm*., 105th Cong. (March 2004) (Admiral Stone testifying that CAPPS II testing was likely to begin in June 2004); GAO Report at 17 ("TSA has only used 32 simulated passenger records – created by TSA from the itineraries of its employees and contractor staff who volunteered to provide the data – to conduct [CAPPS II] testing"); Privacy Office Report at 8 ("At this time, there is no evidence that CAPPS II testing has taken place using passenger data").

[19] Privacy Act Notice, 69 Fed. Reg. 30948, 30951.

The legislative history of the Privacy Act unequivocally demonstrates that government agencies must be open about their information collection practices unless they can show that exceptional circumstances require secrecy. One key objective of the Privacy Act is to ensure that agencies "give detailed notice of the nature . . . of their personal data banks and information systems[.]"[20] The Senate Report on the Privacy Act notes that "it is fundamental to the implementation of any privacy legislation that no system of personal information be operated or maintained in secret by a Federal agency."[21] In those few instances in which a limited exemption for national security and law enforcement was recognized, the exemption was "not intended to provide a blanket exemption to all information systems or files maintained by an agency which deal with national defense and foreign policy information."[22] Rather, the agency must show that the implementation of specific Privacy Act provisions would "damage or impede the purpose for which the information is maintained."[23]

In its authoritative guidance on implementation of the Privacy Act, the Office of Management and Budget explained that "[f]or systems of records which contain information from sources other than the individual to whom the records pertain, the notice should list the types of sources used."[24] While "[s]pecific individuals or institutions need not be identified," the Act contemplates that general categories, such as "financial institutions" or "educational institutions" should be listed.[25]

---

[20] S. Rep. No. 93-1183, at 2 (1974).
[21] *Id*. at 74.
[22] *Id.*
[23] *Id*. at 75.
[24] Office of Management and Budget, Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28948, 28964 (July 9, 1975) ("OMB Guidelines").
[25] *Id.*

Despite the Privacy Act's clear emphasis on transparency and TSA's claimed dedication to preserving individuals' privacy, the agency seeks to avoid the requirement in the future that it inform the public of the sources of information that will feed into the Registered Traveler system of records. TSA does not even attempt to meet its burden of demonstrating that the publication of such basic information would somehow impede the system's presumed effectiveness.

In its Privacy Act notice, TSA indicates that "[i]nformation contained in this system may be obtained from the Registered Traveler applicant, law enforcement and intelligence agency record systems, government and commercial databases, military and National Guard records, and other Department of Homeland Security systems."[26] However, such a listing of possible record source categories of the Registered Traveler information clearly frustrates the Privacy Act notice requirement in light of the agency's intention to keep secret the sources of information that will eventually be fed into the system. Registered Traveler participants have no assurance that the sources of information listed in the notice are indeed the sources that will be used in the program.

If TSA cannot articulate any reason to exempt Registered Traveler from publishing categories of sources of records, it should not exempt the system from that requirement. The Privacy Act does not permit such secrecy unless an agency can demonstrate that it is absolutely necessary for reasons of national security and law enforcement.

[26] Privacy Act Notice, 69 Fed. Reg. 30948, 30951.

III. TSA's Notice Fails to Provide Meaningful Citizen Access to Personal Information

In its notice, TSA has exempted Registered Traveler from all Privacy Act provisions guaranteeing citizens the right to access records containing information about them. The Privacy Act provides, among other things, that

- an individual may request access to records an agency maintains about him or her;[27] and
- the agency must publish a notice of the existence of records in the Federal Register, along with the procedures to be followed to obtain access.[28]

In lieu of the statutory, judicially enforceable right of access provided by the Privacy Act,[29] TSA has substituted a highly discretionary procedure by which a system manager is responsible for handling notification requests, access requests, and the contesting of records. According to TSA's notice, an individual wishing to access his information contained in the system would have to follow the steps set forth in the "notification procedure," which entails writing to the system manager and providing "your full name, current address, date of birth, and a description of information that you seek, including the time frame during which the record(s) may have been generated. You may also provide your Social Security Number or other unique identifier(s) but you are not required to do so."[30] The notice, however, fails to include any time line for the system manager's response to requests, any guarantee that requests will even be considered or granted, or a right to appeal adverse determinations.

---

[27] 5 U.S.C. § 552a(d)(1). Individuals may seek judicial review to enforce the statutory right of access provided by the Act under 5 U.S.C. § 552a(g)(1).
[28] 5 U.S.C. §§ 552a(e)(4)(G), (e)(4)(H), (f).
[29] 5 U.S.C. § 552a(d)(1).
[30] Privacy Act Notice, 69 Fed. Reg. 30948, 30951.

When making an access request, the applicant is to include "the time frame during which the record(s) may have been generated."[31] This requirement is especially onerous since information may be collected from not only the Registered Traveler applicant, but also from "law enforcement and intelligence agency record systems, government and commercial databases, military and National Guard records, and other Department of Homeland Security systems."[32] As a result, this provision appears deliberately vague, since an applicant may not be aware of the time frame during which particular records were generated. If a record is the basis of an applicant's rejection from Registered Traveler, his failure to specify the correct time frame may preemptively deny him an opportunity to make a proper access request. Also, if information in the Registered Traveler System of records is to be kept current, regular updates are necessary, in which case an applicant may not know the exact time frame when more recent records were generated.

Another reading of the time frame requirement suggests that an applicant would simply refer to the general time period in which his application was submitted to indicate when the records would have been compiled. This interpretation would be less problematic for the applicant making the access request; however, if this were TSA's intention, less ambiguous language should have been used in the notice to avoid confusion.

In the event that appropriate steps are followed to make an access request, there remains no guarantee that TSA will produce the records. Such limited, discretionary access to information is an inadequate substitute for the access provisions set forth in the

[31] *Id*.
[32] *Id.*

Privacy Act, and TSA offers no explanation as to why such restricted access is necessary in the context of Registered Traveler.

Individuals who submit their information for Registered Traveler will, by default, agree to have their records "retained in accordance with a schedule to be determined by the National Archives and Records Administration."[33] As a practical matter, it can safely be assumed that many people who will want to access their records will be people who have been denied entry into the Registered Traveler program based on an analysis of information provided by them and collected from other sources. Without adequate access, they will have limited opportunity to review their records and contest any errors. Furthermore, it remains unclear what recourse an applicant has if he is denied Registered Traveler status based on false or inaccurate information, especially if there are difficulties in accessing the records. Even worse, with a retention period that is unspecified in the notice, erroneous information about Registered Traveler applicants may be maintained indefinitely in various databases. TSA's weak access provisions are in direct conflict with the goals of the Privacy Act, which is intended to provide citizens with an enforceable right of access to personal information maintained by government agencies.

IV. TSA's Notice Fails to Provide Meaningful Opportunities to Correct Inaccurate, Irrelevant, Untimely and Incomplete Information

Companion and complementary to the right to access information is the right to correct it. TSA's notice establishes a system that provides neither adequate access nor the ability to amend or correct inaccurate, irrelevant, untimely and incomplete records. The agency has exempted Registered Traveler from the Privacy Act requirements that

[33] *Id*.

define the government's obligation to allow citizens to challenge the accuracy of information contained in their records, such as:

- an agency must correct identified inaccuracies promptly;[34]
- an agency must make notes of requested amendments within the records;[35] and
- an agency must establish procedures to handle disputes between the agency and individual as to the accuracy of the records.[36]

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.[37]

Instead of the judicially enforceable right to correction set forth in the Privacy Act, TSA has established its own discretionary set of procedures for passengers to contest the accuracy of their records. TSA's notice states that the method for contesting records is once again to follow the "notification procedure," which remains unacceptably vague for a process in which individuals should have the right to correct information being used to make important determinations about them.

The notice provides TSA the discretion to correct erroneous information upon a passenger's request, but does not obligate the agency to do so. Significantly, there would be a limited, though for all practical purposes ineffective, right to judicial review of

[34] 5 U.S.C. § 552a(d)(2)(B), (d)(3).
[35] 5 U.S.C. § 552a(d)(4).
[36] 5 U.S.C. § 552a(f)(4).
[37] H.R. Rep. No. 93-1416, at 15 (1974).

TSA's determinations. Although TSA has not specifically exempted the Registered Traveler system of records from 5 U.S.C. § 552a(g), which grants the right to judicial review, the effectiveness of this provision is severely restricted because TSA has exempted the system from access, correction, and relevance requirements. Ordinarily, the agency's failure to comply with these measures would be subject to judicial oversight.[38]

In place of judicial review, TSA will provide a correction process that offers a token nod to the principles embodied in the Privacy Act, but does not provide a meaningful avenue to pursue correction and is subject to change at TSA's whim. Furthermore, the agency presents no explanation why judicially enforceable Privacy Act correction procedures would be inappropriate in the context of Registered Traveler. Denying individuals the right to ensure that the system contains only accurate, relevant, timely and complete records will increase the probability that Registered Traveler will be an error-prone system that contains inaccurate, outdated, or erroneous information.

V. TSA's Notice Fails to Assure Collection of Information Only for "Relevant and Necessary" Use

Incredibly, TSA has exempted Registered Traveler from the fundamental Privacy Act requirement that an agency "maintain in its records only such information about an individual as is relevant and necessary" to achieve a stated purpose required by Congress or the President.[39]

---

[38] 5 U.S.C. §§ 552a(g)(1)(A) and (g)(1)(B) do not apply in the context of Registered Traveler because these sections specifically refer to judicial review of the agency's failure to comply with §§ 552a(d)(3) and (d)(1), from which TSA has exempted this system of records. TSA has also exempted the system from 5 U.S.C. § 552a(e)(1), the requirement to maintain only "relevant and necessary" information, which restricts the reach of 5 U.S.C. § 552a(g)(1)(C), as well. Therefore, the judicial review available to Registered Traveler applicants is limited to the extent that 5 U.S.C. §§ 552a(g)(1)(C) and 552a(g)(1)(D) apply.

[39] Privacy Act Notice, 69 Fed. Reg. 30948, 30951.

TSA does not even attempt to explain why it would be desirable or beneficial to maintain information in the Registered Traveler system that is irrelevant and unnecessary, although it apparently intends to do so. Such open-ended, haphazard data collection plainly contradicts the objectives of the Privacy Act and raises serious questions concerning the likely impact of the Registered Traveler program on its participants.

In adopting the Privacy Act, Congress was clear in its belief that the government should not collect and store data without a specific, limited purpose. The "relevant and necessary" provision

> reaffirms the basic principles of good management and public administration by assuring that the kinds of information about people which an agency seeks to gather or solicit and the criteria in programs for investigating people are judged by an official at the highest level to be relevant to the needs of the agency as dictated by statutes . . . . This section is designed to assure observance of basic principles of privacy and due process by requiring that where an agency delves into an area of personal privacy in the course of meeting government's needs, its actions may not be arbitrary[.][40]

As the Office of Management and Budget noted in its Privacy Act guidelines, "[t]he authority to maintain a system of records does not give the agency the authority to maintain any information which it deems useful."[41]

The Privacy Act's "relevant and necessary" provision thus seeks to protect individuals from overzealous, arbitrary and unnecessary data collection. It embodies the common sense principle that government data collection is likely to spiral out of control unless it is limited to only that information which is likely to advance the government's stated (and legally authorized) objective. Like TSA's prior deviations from customary Privacy Act requirements, the "relevant and necessary" exemption will serve only to

[40] S. Rep. No. 93-3418, at 47 (1974).
[41] OMB Guidelines at 28960.

increase the likelihood that Registered Traveler will become an error-filled, invasive repository of all sorts of information bearing no relationship to its stated goals of expediting the pre-boarding process for travelers and improving transportation security.[42]

TSA has given notice of its plans to exempt CAPPS II from the "relevant and necessary" requirement.[43] The General Accounting Office, in a February 2004 report on CAPPS II to Congress, articulated serious concerns about this exemption:

> These plans reflect the subordination of the *use limitation* and *data quality* practice (personal information should be relevant to the purpose for which it is collected) to other goals and raises concerns that TSA may collect and maintain more information than is needed for the purpose of CAPPS II, and perhaps use this information for new purposes in the future.[44]

(Emphasis in original.) Although participation in the Registered Traveler program, unlike CAPPS II, will be voluntary, participants may logically assume that the information they provide to the government, and that the government collects about them from other sources, will be limited to that which is needed to run the program. They may reasonably assume that the information will not be used for purposes unrelated to that for which it was collected. In exempting Registered Traveler from the fundamental Privacy Act requirement that information collected about people be relevant and necessary for a given program, TSA could mislead program participants about the scope and use of information collected, which is ostensibly intended to enhance aviation security and facilitate the pre-boarding process.

---

[42] *See*, *e.g.*, Interim Final Privacy Act Notice, 68 Fed. Reg. 45265 (August 1, 2003).
[43] *Id*.
[44] GAO Report at 24.

VI. The Broad "Routine Uses" of Registered Traveler Data Will Exacerbate the System's Privacy Problems

TSA's notice identifies thirteen categories of "routine uses" of personal information that will be collected and maintained in the Registered Traveler system of records. Some of these categories are extremely broad. For instance, TSA anticipates disclosure to "the appropriate Federal, State, local, tribal, territorial, foreign or international agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where TSA becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation."[45] This category is so broad as to be almost meaningless, allowing for potential disclosure to virtually any government agency worldwide for a vast array of actual or "potential" undefined violations.

These broadly drawn routine disclosures are particularly alarming because, as we have shown, the information to be disclosed is likely to include material about individuals that is not "relevant and necessary" to any legitimate transportation security or expedited air passenger boarding purpose, nor would such information be subject to a meaningful and enforceable process to ensure that it is accurate, relevant, timely or complete. The broad dissemination of Registered Traveler information that TSA anticipates underscores the need for full transparency (and resulting public oversight), as well as judicially enforceable rights of access and correction.

In addition, some identified "routine uses" of Registered Traveler information fail to provide an explanation of the purpose for the anticipated disclosure. For instance, a registered traveler's collected data may be given to the Attorney General "when

[45] Privacy Act Notice, 69 Fed. Reg. 30948, 30950.

information indicates that an individual meets any of the disqualifications for receipt, possession, shipment or transport of a firearm under the Brady Handgun Violence Prevention Act."[46] If the validity of the information provided by TSA to the Attorney General is then disputed, "it shall be a routine use of the information in this system of records to furnish records or information to the national Background Information Check system[.]"[47] It is entirely unclear what relevance the national handgun registry has to the stated goals of the Registered Traveler program, and for what purpose passengers' information will be provided to the gun registry.

Not only is the purpose of such a "routine use" of passengers' information unclear, but it evokes the issue of "mission creep" — the tendency of government agencies to expand the use of personal information beyond the purpose for which it was initially collected. Whatever the government's interest may be in identifying those people who fail to meet the national qualifications for gun ownership, such uses of Registered Traveler data are plainly beyond the authorized scope of TSA's mission of ensuring aviation security. It is crucial that TSA strictly define the purpose of Registered Traveler at the outset and limit the use of collected information to its core mission.

Conclusion

For the foregoing reasons, EPIC believes that TSA must revise its Privacy Act notice for the Registered Traveler system to 1) ensure greater transparency by claiming only Privacy Act exemptions that are truly necessary; 2) provide individuals enforceable rights of access and correction; 3) limit the collection of information to only that which is necessary and relevant; and 4) substantially limit the routine uses of collected

[46] *Id.* at 30950.
[47] *Id.*

information. Further, EPIC urges TSA not to implement the final version of the Registered Traveler program until TSA reconsiders and substantially modifies its privacy practices.

Respectfully submitted,

David L. Sobel
General Counsel

Marcia Hofmann
Staff Counsel

Samantha Liskow
IPIOP Law Clerk

Dina Mashayekhi
IPIOP Law Clerk

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