DEPARTMENT OF HOMELAND SECURITY
Transportation Security Administration

Docket No. TSA-2004-19160
Privacy Act Notice and
Privacy Impact Assessment
Secure Flight Test Records

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

By notice published on September 24, 2004, the Transportation Security Administration ("TSA") established a system of records ("Secure Flight Test Records") to test TSA's new Secure Flight passenger prescreening program.[1] The agency also published a privacy impact assessment for the proposed program, as well as a request for emergency processing of a new public information collection submitted to the Office of Management and Budget.[2] Together, these documents are referred to by TSA as the "Secure Flight Testing Privacy Package."[3]

According to TSA, Secure Flight "will involve the comparison of information in PNRs for domestic flights to names in the Terrorist Screening Database (TSDB) . . . to include the expanded TSA No-Fly and Selectee Lists, in order to identify individuals known or reasonably suspected to be engaged in terrorist activity."[4] TSA will also "conduct a separate test of the use of commercial data to determine its effectiveness in identifying passenger information that is inaccurate or incorrect."[5] In order to test both

---

[1] Notice to Establish System of Records, 69 Fed. Reg. 57345 (proposed Sept. 24, 2004).

[2] Privacy Impact Assessment, 69 Fed. Reg. 57352 (proposed Sept. 24, 2004); Notice of Emergency Clearance Request, 69 Fed. Reg. 57342 (proposed Sept. 24, 2004).

[3] The "Privacy Package" is available at http://www.tsa.gov/public/display?content=09000519800cf3a7 (last visited Oct. 23, 200o4).

[4] 69 Fed. Reg. at 57346.

[5] *Id.*

Secure Flight and the utility of using commercial information within the program, TSA "is proposing to issue an order to all domestic aircraft operators directing them to submit a limited set of historical passenger name records to TSA."[6] Specifically, TSA intends to collect "PNRs with domestic flight segments completed in the month of June 2004."[7]

Pursuant to the TSA Privacy Act notice and privacy impact assessment, the Electronic Privacy Information Center ("EPIC") submits these comments to address the substantial privacy issues raised by Secure Flight and the new system of records; to request that TSA extend this comment period until the government is willing to make more information about Secure Flight available to the public; to request that TSA substantially revise its Privacy Act notice prior to implementation of Secure Flight; and to urge the agency to delay collecting passenger information from domestic airlines for Secure Flight testing until crucial privacy issues are addressed.

TSA states that it "believes it has taken action to mitigate any privacy risk by designing its next generation passenger prescreening program to accommodate concerns expressed by privacy advocates, foreign counterparts, and others."[8] However, Secure Flight, as described by TSA in its "Privacy Package," is disturbingly similar to the Computer Assisted Passenger Prescreening System ("CAPPS II") TSA proposed more than a year ago,[9] which ultimately failed in large part due to privacy concerns.[10] Like CAPPS II, Secure Flight is a secret, classified system that will include information that is

---

[6] *Id*. at 57342.

[7] *Id*. at 57344.

[8] *Id*. at 57355.

[9] Interim Final Privacy Act Notice, 68 Fed. Reg. 45265 (August 1, 2003).

[10] *See, e.g*., Sara Kehaulani Goo and Robert O'Harrow Jr., *New Airline Screening System Postponed*, Washington Post, July 16, 2004, at A02; Eunice Moscoso, *Agency to Revise Airport Screening; Privacy Concerns Prompt Redesign*, Atlanta Journal-Constitution, July 16, 2004, at 5B; Leslie Miller, *TSA Reworks Air Travel Screening Program*, Associated Press, July 13, 2004; Matthew L. Wald and John Schwartz, *Screening Plans Went Beyond Terrorism*, NY Times, Sept. 18, 2004 at A35.

not "relevant and necessary" to accomplish its stated purpose of improving aviation security. Individuals will have no judicially enforceable right to access information about them contained in the system, nor to request correction of information that is inaccurate, irrelevant, untimely or incomplete. In short, like CAPPS II, Secure Flight is exactly the sort of system Congress intended to prohibit when it enacted the Privacy Act of 1974.[11]

Introduction

The U.S. Supreme Court has long recognized that citizens enjoy a constitutional right to travel. Thus, in *Saenz v. Roe*, the Court noted that the "'constitutional right to travel from one State to another' is firmly embedded in our jurisprudence."[12] Indeed, DHS Deputy Secretary Admiral James Loy has observed that "the founding fathers . . . had mobility as one of the inalienable rights they were talking about."[13] For that reason, any governmental initiative that conditions the ability to travel upon the surrender of privacy rights requires particular scrutiny.

Given its constitutional implications, and the massive scope of the system (which sought to collect information about tens of millions of individuals), CAPPS II understandably was the focus of concern within Congress[14] and among the general

---

[11] 5 U.S.C. § 552a.

[12] 526 U.S. 489 (1999), quoting *United States v. Guest*, 383 U.S. 745 (1966).

[13] Testimony of Admiral James Loy before House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census (May 6, 2003).

[14] In Homeland Security appropriations bill (H.R.2555), Congress blocked deployment of CAPPS II until the General Accounting Office ("GAO") studied the program's implications. The GAO's ensuing report found that seven of eight concerns voiced by Congress had not been addressed. General Accounting Office, *Aviation Security: Computer Assisted Passenger Prescreening Program Faces Significant Implementation Challenges*, GAO-04-385 (Feb. 2004) (hereinafter "GAO Report"). Congress's concern about CAPPS II is also evident in Press Release, Office of Senator Ron Wyden, Wyden Wins Commerce Committee Approval to Require Oversight of CAPPS II Airline Passenger Screening System (Mar. 13, 2003); Press Release, Office of Senator Patrick Leahy, Reaction of Senator Leahy to GAO's Report on Flaws in the CAPPS II Program (Feb. 13, 2004); Press Release, Senate Governmental Affairs Committee, Senators Collins, Lieberman Ask TSA: What Other Airlines Have Been Contacted and Asked for Passenger Information? (Apr. 14, 2004).

public.[15] It also engendered strong opposition abroad, where foreign governments and their citizens resisted the demands of the U.S. government to provide detailed air passenger data as a condition of flight into the United States.[16] Much of the controversy surrounding CAPPS II centered on the system's secrecy and the lack of public information concerning the manner in which the system would assess the security risks particular individuals are deemed to pose, as well as the types of data that TSA would use to make such assessments. When the General Accounting Office ("GAO") issued a report on CAPPS II at Congress's request in February 2004, the agency concluded that TSA had failed to address concerns about, among other things, privacy implications and provision of adequate redress.[17]

Unfortunately, Secure Flight presents the same problems. When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal information that federal agencies could collect and, significantly, required agencies to be transparent in their information practices.[18] 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[.]"[19] Adherence to these requirements is critical for a system like Secure Flight.

In remarks before the international conference of data protection and privacy officials last year, the Chief Privacy Officer of the Department of Homeland Security

---

[15] Editorials on CAPPS II published in major newspapers included Editorial, *Safe Skies*, Washington Post, Mar. 21, 2003, at A12; and Editorial, *Airport Screening System More Minus Than Plus*, Atlanta Journal Constitution, Mar. 25, 2004, at 14A.

[16] *See, e.g.*, Sara Kehaulani Goo, *U.S., EU Will Share Passenger Records*, Washington Post, May 2004, at A02.

[17] GAO Report, *supra* at n14.

[18] S. Rep. No. 93-1183, at 1 (1974).

[19] *Id.*

assured the delegates that "[u]nder the Privacy Act, in concert with the Freedom of Information Act and the E-Government Act, citizens, legal residents, and visitors to the United States have been afforded almost unequalled transparency into the federal government's activities and the federal government's use of personal information about them."[20] Unfortunately, TSA's exemption-heavy Privacy Act notice, along with a complete lack of responsiveness to requests for information under Freedom of Information Act ("FOIA"), show that the Department, TSA, and other agencies involved in administering Secure Flight continue to fall short of such transparency in the realm of aviation security.

I. The FBI, TSA, and CBP Have Thwarted Public Scrutiny of Secure Flight Under the Freedom of Information Act

As discussed in the comments EPIC submitted on CAPPS II last year, EPIC met staunch resistance when it attempted to use the FOIA to obtain information about CAPPS II.[21] EPIC has continued to encounter tremendous difficulty using the FOIA to learn more about TSA's most recent passenger prescreening initiative.

On September 28, 2004, EPIC submitted a FOIA request to TSA asking for information about Secure Flight.[22] EPIC asked that the request be processed expeditiously, noting the intense media interest surrounding Secure Flight. Specifically, EPIC demonstrated that 485 articles had been published about the program since TSA announced its plans for Secure Flight. EPIC also mentioned the October 25, 2004 deadline for public comments on the test phase of the system, explaining the urgency for the public to be as well informed as possible about Secure Flight in order to meaningfully

---

[20] Remarks of Nuala O'Connor Kelly Before the 25th International Conference of Data Protection and Privacy Commissioners, Sydney Australia, September 11, 2003 ("Kelly Remarks").

[21] Comments of the Electronic Information Center on CAPPS II Interim Final Privacy Act Notice, Sept. 30, 2003, *available at* http://www.epic.org/privacy/airtravel/capps-comments.pdf.

[22] Letter from Marcia Hofmann, Staff Counsel, EPIC, to Patricia Reip-Dice, Associate Director, FOIA Headquarters Office, TSA, Sept. 28, 2004 (on file with EPIC).

respond to the agency's proposal for the program. TSA determined these circumstances did not justify the information's immediate release, and refused EPIC's request that the information be made public prior to the October 25 deadline for these comments.[23] TSA also denied EPIC a fee waiver, which the agency has never done before in its three-year existence. This maneuver has imposed a significant procedural barrier to EPIC's ability to obtain the information. EPIC has appealed TSA's decision.

On September 30, 2004, EPIC submitted a FOIA request to the FBI asking for information about the maintenance and administration of the Terrorist Screening Database.[24] EPIC showed that 213 articles had been published containing both "Secure Flight" and "FBI," and again noted the urgency for the public to learn as much as possible about Secure Flight prior to the expiration of the comment period. The FBI also denied EPIC's request, claiming that EPIC failed to adequately justify the need for the information's quick release.[25] Incredibly, the agency also refused to recognize that EPIC is "primarily engaged in disseminating information," despite a federal court decision in May that found otherwise.[26] In response to the FBI's decision, EPIC filed suit and a motion for a temporary restraining order and preliminary injunction asking a federal judge to order the FBI to process and release the documents immediately.[27] The very next day, the FBI voluntarily granted expedited processing of EPIC's request.[28] EPIC has

---

[23] Letter from Catrina M. Pavlik, Associate Director, Freedom of Information Act and Privacy Act Division, TSA, to Marcia Hofmann, Staff Counsel, EPIC, Oct. 7, 2004 (on file with EPIC).

[24] Letter from Marcia Hofmann, Staff Counsel, EPIC, to David M. Hardy, Chief, Record/Information Dissemination Section, Records Management Division, FBI, Sept. 30, 2004 (on file with EPIC).

[25] Letter from David M. Hardy, Chief, Record/Information Dissemination Section, Records Management Division, FBI, to Marcia Hofmann, Staff Counsel, EPIC, Oct. 1, 2004 (on file with EPIC).

[26] *American Civil Liberties Union v. Dep't of Justice*, 321 F. Supp. 2d 24, 29 n5 (D.D.C. 2004).

[27] Motion for a Temporary Restraining Order and Preliminary Injunction, *Electronic Privacy Information Center v. Dep't of Justice*, C.A. 04-1736 (D.D.C. 2004 HHK).

[28] Letter from David M. Hardy, Chief, Record/Information Dissemination Section, Records Management Division, FBI, to Marcia Hofmann, Staff Counsel, EPIC, Oct. 13, 2004 (on file with EPIC).

yet to receive the documents.

Finally, on September 30, 2004, EPIC submitted a FOIA request to the Bureau of Customs and Border Protection ("CBP"), asking for documents concerning the impact Secure Flight might have on the agreement between the European Union and CBP for the transfer of PNR data to the CBP, and whether such records might be transferred to the FBI or Terrorist Screening Center for inclusion in the Terrorist Screening Database.[29] EPIC once again asked for expedited processing, noting the extraordinary media interest in Secure Flight and the pendency of the public comment period for the test phase of Secure Flight.[30] To date, CBP has not responded.

The unwillingness of TSA and other agencies to release information about Secure Flight prior to the close of this comment period frustrates the ability of the public to submit meaningful, well informed comments in response to TSA's "Privacy Package." In order for this notice and comment period to be anything other than a perfunctory exercise, TSA must extend the time for comment until TSA and other agencies are willing to release more substantial information about Secure Flight.

II. Like TSA's CAPPS II Notice, TSA's Secure Flight Proposal Contravenes the Intent of the Privacy Act

The Privacy Act was intended to guard citizens' privacy interests against government intrusion. Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[31] It thus sought to "provide certain

---

[29] Letter from Marcia Hofmann, Staff Counsel, EPIC, to Freedom of Information Act Officer, CBP, Sept. 30, 2004 (on file with EPIC).

[30] *Id*. at 2.

[31] Pub. L. No. 93-579 (1974).

protections for an individual against an invasion of personal privacy" by establishing a set of procedural and substantive rights.[32]

In its February 2004 report on CAPPS II, the GAO flagged TSA's failure to justify the Privacy Act exemptions claimed for the program:

> In January 2003, TSA published a proposed rule to exempt [CAPPS II] 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.[33]

TSA apparently has not taken the GAO finding to heart, since the agency claims nearly every Privacy Act exemption for Secure Flight that it did for CAPPS II, and again fails to explain why. As we detail below, the exemptions claimed by the TSA for Secure Flight are thoroughly inconsistent with the purpose and intent of the Privacy Act.

As an initial matter, we note that TSA has invoked 5 U.S.C. § 552a(k)(1) and (k)(2) as authority for its exemption of specific Privacy Act requirements. Subsection (k)(1) is applicable only where the system of records is "subject to the provisions of section 552(b)(1) of this section," *i.e.*, if the system contains classified information. While TSA has designated the "Security Classification" of the system of records as "[c]lassified, sensitive,"[34] it is not apparent that *all* information in the system of records warrants (or is entitled to) such classification. For instance, "Passenger Name Records (PNRs) obtained from aircraft operators"[35] clearly are not subject to government classification.

Subsection (k)(2) is applicable only where the system of records is "investigatory

---

[32] *Id.*

[33] GAO Report at 23.

[34] 69 Fed. Reg. 57347.

[35] *Id.*

material compiled for law enforcement purposes." The subsection provides, however, that "if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual . . . " Given that TSA seeks to exempt the Secure Flight system of records from the Privacy Act's access provisions, as we discuss below, it is unclear whether subsection (k)(2) authorizes TSA's action. As such, we urge TSA to explain how (k)(1) and (k)(2) give TSA authority to exempt the system of records from the various Privacy Act provisions it cites.

We also question whether TSA's invocation of exemptions is procedurally and substantively sound. The legislative history of the Privacy Act suggests it is not:

> Once the agency head determines that he has information legitimately in one of his information systems which falls within these definitions [of exemptable categories] then he must, via the rulemaking process, determine that application of the challenge, access and disclosure provisions would "seriously damage or impede the purpose for which the information is maintained." The Committee intends that this public rulemaking process would involve candid discussion of the general type of information that the agency maintains which it feels falls within these definitions and the reasons why access, challenge or disclosure would "seriously damage" the purpose of the maintenance of the information. The Committee hastens to point out that even if the agency head can legitimately make such a finding he can only exempt the information itself or classes of such information . . . and not a whole filing system simply because intelligence or investigative information is commingled with information and files which should be legitimately subject to the access, challenge and disclosure provisions.[36]

TSA's notice does not appear to be the kind of "rulemaking" that Congress envisioned. Nor has the agency stated whether, let alone why, it has determined that the application of standard Privacy Act procedures would "seriously damage" the purpose of the system of records. In addition, the application of the claimed exemptions to the *entire* system of records is clearly inappropriate, as it will obviously contain information "which should be legitimately subject to

[36] S. Rep. No. 93-3418, at 75 (1974).

the access, challenge and disclosure provisions."[37] TSA must cure these defects before collecting personal data for inclusion in the Secure Flight system of records.

A. Like CAPPS II, the Secure Flight Test Phase Fails to Provide Meaningful Citizen Access to Personal Information

In its notice, TSA has exempted the Secure Flight test phase from all Privacy Act provisions guaranteeing citizens the right to access records containing information about them. We note that TSA claimed these same exemptions for CAPPS II.[38] The Privacy Act provides, among other things, that

- an individual may request access to records an agency maintains about him or her;[39] 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.[40]

In lieu of the statutory, judicially enforceable right of access provided by the Act, "DHS has determined that all persons may request access to information about them contained in a PNR by sending a written request to the TSA Privacy Officer,"[41] TSA will provide access "[t]o the greatest extent possible and consistence with national security requirements."[42] No time guidelines are specified for the procedure. Furthermore, the notice specifically states that "this system of records may not be accessed for purposes of

---

[37] *See also* Office of Management and Budget, Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28948, 28972 (July 9, 1975) ("OMB Guidelines") ("agencies should, wherever practicable, segregate those portions of systems for which an exemption is considered necessary so as to hold to the minimum the amount of material which is exempted").

[38] 68 Fed. Reg. 45265, 45267.

[39] 5 U.S.C. § 552a(d)(1). Individuals may seek judicial review to enforce the statutory right of access provided by the Act. 5 U.S.C. § 552a(g)(1).

[40] 5 U.S.C. §§ 552a(e)(4)(G), (e)(4)(H), (f).

[41] 69 Fed. Reg. 57348.

[42] *Id*. at 57347.

determining if the system contains a record pertaining to a particular individual."[43] Such limited, discretionary access to information is an inadequate substitute for the access provisions set forth in the Privacy Act, and TSA offers no explanation why such restricted access is necessary in the context of Secure Flight.

TSA's weak access provisions are in direct conflict with the purposes of the Privacy Act, which sought to provide citizens with an enforceable right of access to personal information maintained by government agencies. It is hardly reassuring when TSA guarantees that "[u]pon completion of the testing phase, and before Secure Flight is operational, TSA will establish comprehensive passenger redress procedures and personal data and civil liberties protections for the Secure Flight program."[44] As DHS Privacy Officer Nuala O'Connor Kelly testified before Congress in February, "[i]ssues of privacy and civil liberties are most successfully navigated when the necessary legal, policy, and technological protections are built in to the systems or programs from the very beginning."[45] Secure Flight clearly lacks such a protective framework at this stage.

B. Like TSA's CAPPS II Notice, TSA's Secure Flight Test Phase Proposal 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. As it

---

[43] *Id*. at 57348.

[44] *Id*. at 57347.

[45] Statement of Chief Privacy Officer Nuala O'Connor Kelly Before the House of Representatives Judiciary Subcommittee on Commercial and Administrative Law (Feb. 10, 2004) *at* http://www.dhs.gov/dhspublic/interapp/testimony/testimony_0024.xml (last accessed Oct. 23, 2004).

did for CAPPS II, the agency has exempted[46] Secure Flight from the Privacy Act requirements that 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;[47]
- an agency must make notes of requested amendments within the records;[48] and
- an agency must establish procedures to handle disputes between the agency and individual as to the accuracy of the records.[49]

The GAO noted these exemptions as one of CAPPS II's key problems :

> TSA plans to limit the application of the *individual participation* practice—which states that individuals should have the right to know about the collection of personal information, to access that information, and request correction — by prohibiting passenger access to all personal information about them accessed by CAPPS II. This raises concerns that inaccurate personal information will remain uncorrected in and continue to be accessed by CAPPS II.[50]

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.[51]

Instead of the judicially enforceable right to correction set forth in the Privacy

---

[46] 69 Fed. Reg. 57348.

[47] 5 U.S.C. § 552a(d)(2)(B), (d)(3).

[48] 5 U.S.C. § 552a(d)(4).

[49] 5 U.S.C. § 552a(f)(4).

[50] *Id*. at 24.

[51] H.R. Rep. No. 93-1416, at 15 (1974).

Act,[52] TSA has established its own, discretionary set of procedures for passengers to contest the accuracy of their records. TSA's notice states that "[I]f an individual wishes to contest or amend records received in this manner, he or she may do so by sending the request to TSA. . . . Before implementing a final program, however, TSA will create a robust redress mechanism to resolve disputes concerning the Secure Flight program."[53] The notice provides TSA the discretion to correct erroneous information upon a passenger's request, but does not obligate the agency to do so. This correction process 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. Not surprisingly, the GAO identified the same failure in CAPPS II:

> TSA has not yet finalized a redress process for passengers who are erroneously delayed or prohibited from boarding their scheduled flights, termed "false positives." According to TSA officials, a redress process for such passengers is a critical element of CAPPS II, and TSA intends to establish a process by which passengers who are subject to additional screening or denied boarding will be provided the opportunity to seek redress by filing a complaint. However, officials stated that such a program cannot be fully developed until key program policies are finalized[.][54]

Most importantly, there would be no right to judicial review of TSA's determinations. The agency presents no explanation why judicially-enforceable Privacy Act correction procedures would be inappropriate in the context of Secure Flight. Denying citizens the right to ensure that the system contains only accurate, relevant, timely and complete records will increase the probability that Secure Flight will be an error-prone, ineffective means of singling out passengers as they seek to exercise their constitutional right to travel. This problem will only be exacerbated by TSA's failure to

---

[52] 5 U.S.C. § 552a(g)(1).

[53] 69 Fed. Reg. At 57354.

[54] GAO Report at 25.

provide a schedule for retention and disposal of records.[55]

TSA's repeated failure to provide the public a Privacy Act-compliant correction and redress procedure is unjustified and unacceptable. TSA should not collect any information about individuals, even if only for testing purposes, until it can articulate an appeals process to the public that complies with the requirements of the Privacy Act.

C. Like TSA's CAPPS II Notice, TSA's Secure Flight Test Phase Proposal Fails to Assure Collection of Information Only for "Relevant and Necessary" Use

Incredibly, TSA has also exempted Secure Flight 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.[56] TSA does not even attempt to explain why it would be desirable or beneficial to maintain information in the Secure Flight 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 Secure Flight rating process on millions of law-abiding travelers.

This Privacy Act exemption was also claimed for CAPPS II. In its report, the GAO stated:

> TSA plans to exempt CAPPS II from the Privacy Act's requirements to maintain only that information about an individual that is relevant and necessary to accomplish a proper agency purpose. These plans reflect the subordination of the *use limitation* practice 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.[57]

---

[55] 69 Fed. Reg. 57347.

[56] 5 U.S.C. § 552a(e)(1); 69 Fed. Reg. 57348.

[57] GAO Report at 24 (emphasis in original).

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[.][58]

As OMB 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."[59] 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 other deviations from customary Privacy Act requirements, the "relevant and necessary" exemption will serve only to increase the likelihood that Secure Flight will become an error-filled, invasive repository of all sorts of information bearing no relationship to its stated goal of increasing aviation security. TSA should be particularly sensitive to this issue because the maintenance of information that is neither relevant nor necessary to achieve Secure Flight's stated goals encourages "mission creep" — the tendency of government agencies to expand the use of personal information beyond the purpose for which it was initially collected. It is crucial that TSA strictly limit the use of collected information to Secure Flight's core mission.

---

[58] S. Rep. No. 93-3418, at 47 (1974).

[59] OMB Guidelines at 28960.

D. Testing of Secure Flight Should Not Proceed Until TSA's Notice on the Secure Flight Test Phase is Revised

As part of its "Privacy Package," TSA intends to order all domestic airlines to turn over a month's worth of PNR data on October 29, 2004.[60] Such data acquisition will place in the agency's hands personal information concerning millions of individuals without, as we have discussed, meaningful rights of access or correction. TSA has articulated no reason why such rights should not be provided and, as such, even limited use of personal information for testing purposes raises significant privacy issues that TSA seems unprepared to address. For this reason, acquisition of personal data should not proceed until TSA revises its policies and practices to bring them into conformance with the intent of the Privacy Act.

Conclusion

For the foregoing reasons, EPIC believes that TSA must revise its Privacy Act notice for the Secure Flight system to 1) ensure greater transparency through the establishment of a nonclassified system; 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 information. Further, development of the system should be suspended until TSA and other agencies involved in Secure Flight's development are willing to disclose information about the program to the public, and TSA subsequently solicits public comments. Finally, the agency should not acquire personal information, even for testing purposes, until it has revised its Privacy Act notice as suggested above.

Respectfully submitted,

Marcia Hofmann
Staff Counsel

[60] 69 Fed. Reg. 57344.

David L. Sobel
General Counsel

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