

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Docket No. DHS/TSA-2003-1
Interim Final Privacy Act Notice
Aviation Security Screening Records

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

By notice published on August 1, 2003, the Transportation Security Administration ("TSA") established a system of records (DHS/TSA 010 -- Passenger and Aviation Security Screening Records) to support TSA's Computer Assisted Passenger Prescreening System ("CAPPS II").¹ According to TSA, CAPPS II is "intended to conduct risk assessments and authentications for passengers traveling by air to, from or within the United States."² Pursuant to the TSA notice, the Electronic Privacy Information Center ("EPIC") submits these comments to address the substantial privacy issues raised by CAPPS II and the new system of records; to request that TSA substantially revise its Privacy Act notice prior to implementation of CAPPS II; and to urge the agency to desist from its recent efforts to obtain personal information concerning millions of air passengers for use in testing the system.³

In essence, CAPPS II, as described by TSA in its notice, is a secret, classified system that the agency will use to conduct background checks on tens of millions of airline passengers. The resulting "risk assessments" will determine whether individuals will be subject to invasive searches of their persons and belongings, or be permitted to board commercial aircraft. TSA will not inform the public of the categories of information contained in the system. It will include information that is 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,

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

² *Id.* at 45256.

³ EPIC was assisted in the preparation of these comments by Catherine Harper of the Cyberlaw Clinic at the Stanford Law School Center for Internet and Society.

irrelevant, untimely or incomplete. In short, it is precisely the sort of system that Congress sought to prohibit when it enacted the Privacy Act of 1974.⁴

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."⁵ Indeed, TSA Administrator Admiral James Loy has observed that "the founding fathers . . . had mobility as one of the inalienable rights they were talking about."⁶ For that reason, any governmental initiative, such as CAPPs II, 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 seeks to collect information about tens of millions of individuals), CAPPs II understandably has been the focus of concern within Congress⁷ and the general public. It has also engendered strong opposition abroad, where foreign governments and their citizens have resisted the demands of the U.S. government to provide detailed air passenger data as a condition of flight into the United States. Reflecting those concerns, a resolution was passed at the recent International Conference of Data Protection and Privacy Commissioners in Sydney, Australia calling for "an international agreement stipulating adequate data protection requirements, including clear purpose limitation, adequate and non-excessive data collection, limited data retention time, information provision to

⁴ 5 U.S.C. § 552a.

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

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

⁷ In the recently enacted Homeland Security appropriations bill (H.R.2555), Congress has blocked deployment of CAPPs II until the General Accounting Office ("GAO") studies its privacy implications. The GAO report must be completed by February 15, 2004.

data subjects, the assurance of data subject rights and independent supervision" before such data transfers occur.⁸

Much of the controversy surrounding CAPPs II has centered on the system's secrecy and the lack of public information concerning the manner in which it will assess the security risks particular individuals are deemed to pose, and the types of data that TSA will use to make such assessments. 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.⁹ 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[.]"¹⁰ Adherence to these requirements is critical for a system like CAPPs II.

In recent remarks before the international conference of data protection and privacy officials, the Chief Privacy Officer of the Department of Homeland Security 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.¹¹

Unfortunately, TSA's CAPPs II Privacy Act notice, along with the agency's responses to Freedom of Information Act ("FOIA") requests and lack of compliance with fundamental E-Government Act requirements, show that the Department and TSA have fallen far short of such transparency in the realm of aviation security.

⁸ Resolution Concerning the Transfer of Passengers' Data, 25th International Conference of Data Protection & Privacy Commissioners (September 12, 2003) (available at <http://www.epic.org/news/Comm03.html>).

⁹ S. Rep. No. 93-1183, at 1 (1974).

¹⁰ *Id.*

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

I. TSA Has Thwarted Public Scrutiny Under the Freedom of Information Act

Soon after enactment of the Aviation and Transportation Security Act, Pub. L. No. 107-71, and the creation of TSA, EPIC began requesting information from the agency under the FOIA seeking information on the potential privacy impact of 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.¹² TSA ultimately withheld the vast majority of responsive records on the grounds that they were "pre-decisional" 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.¹³ Upon processing the FOIA request, TSA released records demonstrating that a substantial number of passengers had been misidentified as a result 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.¹⁴ As with the previous FOIA requests, a vast amount of responsive material was withheld.¹⁵

Most recently, 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 and the "Capital Asset Plan and Business Case" for the CAPPs II project.¹⁶ 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.

¹² *EPIC v. Department of Transportation*, Civ. No. 02-475 (D.D.C.).

¹³ *EPIC v. Transportation Security Administration*, Civ. No. 02-2437 (D.D.C.).

¹⁴ *EPIC v. Department of Homeland Security*, Civ. No. 03-1255 (D.D.C.).

¹⁵ TSA has not yet fully articulated the basis for its decision to withhold this material; pursuant to court order, it must do so by October 2, 2003.

¹⁶ *EPIC v. Transportation Security Administration*, Civ. No. 03-1846 (D.D.C.).

Although the agency relented after EPIC filed suit, its refusal to voluntarily expedite the processing of the two documents for possible release belies the suggestion that TSA is committed to an open and informed public dialogue on the significant issues raised by the CAPPs II initiative.¹⁷ As we discuss in detail in Sec. III.A., *infra*, TSA's Privacy Act notice indicates the agency's continuing unwillingness to design and implement CAPPs II in an open and transparent manner.

II. TSA Has Not Complied With the Intent of the E-Government Act

As noted, EPIC's most recent FOIA request sought the release of TSA's Privacy Impact Assessment ("PIA") and the "Capital Asset Plan and Business Case" for the CAPPs II project. On September 25, TSA responded to the request and advised EPIC that both documents exist only in draft form and that "final versions . . . are not expected until early 2004."¹⁸ The fact that the PIA and Business Case have not been finalized is significant because their preparation for a system such as CAPPs II is mandated by the E-Government Act and Office of Management and Budget ("OMB") regulations, respectively. The E-Government Act requires that agencies "*shall* conduct a privacy impact assessment . . . *before* . . . initiating a new collection of information that . . . will be collected, maintained, or disseminated using information technology."¹⁹ Likewise, OMB regulations require agencies, when proposing "major" or "significant" information technology projects, to address privacy and security issues in their Business Case submissions and to prepare PIAs.²⁰

¹⁷ In addition to Ms. Kelly's remarks concerning "transparency," quoted above, other DHS and TSA officials have similarly acknowledged the public's right to know about the CAPPs II project. Most recently, TSA spokesman Brian Turmail was quoted as saying, "The American people have the right to know whether this system will work. We should have a dialogue based on fact and not innuendo." Ryan Singel, *JetBlue Data to Fuel CAPPs Test*, Wired News, September 16, 2003.

¹⁸ Letter from Patricia M. Riep-Dice to David L. Sobel, September 25, 2003 (available at <http://www.epic.org/privacy/airtravel/pia-foia-response.pdf>).

¹⁹ Pub. L. No. 107-347 (December 17, 2002), § 208 (emphasis added).

²⁰ OMB Circular A-11, part 3, Planning, Budgeting and Acquisition of Capital Assets (July 2000); Memorandum from Joshua B. Bolton, "Implementation Guidance for the E-Government

In his testimony before Congress on May 6, 2003, Admiral Loy stated that "TSA is mindful that privacy protections must be built into the CAPPS II system from its very foundation" and said that the agency was "working to finalize its CAPPS II business case, which will detail how privacy and security are built into the system" and "also will conduct a Privacy Impact Assessment."²¹ It is thus surprising to find TSA moving ahead with CAPPS II before the privacy implications of the system have been fully addressed and disclosed to the public. The General Accounting Office, in a recent report on another DHS information system, noted that "OMB requires that IT projects . . . perform a system privacy impact assessment, so that relevant privacy issues and needs are understood and appropriately addressed *early and continuously* in the system life cycle."²² CAPPS II has been under development for almost two years; it is clear that TSA has failed to meet its obligation to address the privacy implications "early and continuously," as federal law requires.

III. CAPPS II 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."²³ 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.²⁴

Act of 2002" (August 1, 2003) (available at <http://www.whitehouse.gov/omb/memoranda/m03-18.pdf>).

²¹ May 6 Loy Testimony.

²² INFORMATION TECHNOLOGY: Homeland Security Needs to Improve Entry Exit System Expenditure Planning, GAO-03-563 (June 2003) (emphasis added).

²³ Pub. L. No. 93-579 (1974).

²⁴ *Id.*

DHS's Chief Privacy Officer recently touted the protections afforded by the Privacy Act (and the purpose of a notice like the one at issue here), explaining that the law

provides substantial notice, access, and redress rights for citizens and legal residents of the United States whose information is held by a branch of the federal government. The law provides robust advance notice, though detailed 'system of records' notices, about the creation of new technological or other systems containing personal information. The law also provides the right of access to one's own records, the right to know and to limit other parties with whom the information has been shared, and the right to appeal determinations regarding the accuracy of those records or the disclosure of those records.²⁵

The notice published by TSA, however, exempts CAPPS II from nearly all of the Privacy Act provisions Ms. O'Connor Kelly described.²⁶ As we detail below, the exemptions claimed by the TSA 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) as authority for its exemption of specific Privacy Act requirements. The only subsections of that provision that appear to be possibly relevant to the CAPPS II system are (k)(1) and (k)(2). 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,"²⁷ 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 airlines"²⁸ clearly are not subject to government classification.

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

²⁵ Kelly Remarks.

²⁶ Indeed, TSA has invoked exemptions for *all* of the requirements that the Privacy Act permits an agency to invoke.

²⁷ Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45268.

²⁸ *Id.*

Given that TSA seeks to exempt the CAPPS II 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 specify which subsection(s) of 5 U.S.C. § 552a(k) it is claiming as 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 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.²⁹

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 the access, challenge and disclosure provisions."³⁰ TSA must cure these defects before collecting personal data for inclusion in the CAPPS II system of records.

²⁹ S. Rep. No. 93-3418, at 75 (1974).

³⁰ 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").

A. 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. TSA has frustrated that intent by exempting the CAPPs II system of records from the requirement that it publish "the categories of sources of records in the system."³¹

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" ³² The Senate Report 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."³³ 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."³⁴ 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."³⁵

In its authoritative guidance on implementation of the Privacy Act, OMB 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."³⁶ While "[s]pecific

³¹ 5 U.S.C. § 552a(e)(4)(I); Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45269.

³² S. Rep. No. 93-1183, at 2 (1974).

³³ *Id.* at 74.

³⁴ *Id.*

³⁵ *Id.* at 75.

³⁶ OMB Guidelines at 28964.

individuals or institutions need not be identified," the Act contemplates that general categories, such as "financial institutions" or "educational institutions" should be listed.³⁷

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 that it inform the public of the sources of information that will feed into the CAPPS II system. TSA does not even attempt to meet its burden of demonstrating that the publication of such basic information about the system would somehow impede its presumed effectiveness.

In the supplementary material accompanying its Privacy Act notice, TSA asserts that it "will not use measures of creditworthiness, such as FICO scores, and individual health records in the CAPPS II traveler risk determination."³⁸ That assurance rings hollow, however, in light of the agency's stated intention to keep secret the sources of information that will eventually be fed into the system.³⁹

TSA's determination that CAPPS II will be exempt from the requirement of publishing categories of sources of records is at odds with specific assurances the agency provided to Congress. When asked about this issue just four months ago, Admiral Loy indicated that such information would, in fact, be disclosed:

SEN. BYRD: Will the new notice name the precise databases of information that CAPPS II will collect about air passengers?

ADM. LOY: I don't know that we have any reason not to name those in the privacy notice⁴⁰

³⁷ *Id.*

³⁸ Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45267.

³⁹ This is one of several instances in which assurances contained in the supplementary material accompanying the Privacy Act notice are contradicted by the language of the notice itself. EPIC urges TSA to clarify these apparent discrepancies and to clearly state, for instance, whether the public would be notified if the "categories of sources of records" included in the CAPPS II system were to include, at some time in the future, creditworthiness and health data.

⁴⁰ *The Fiscal Year 2004 Appropriations for the Bureau of Customs and Border Security; Transportation Security Administration and Federal Law Enforcement Training Center, Hearing Before the Homeland Security Subcommittee of the Senate Appropriations Committee*, 108th Cong. (May 13, 2003) (testimony of Admiral James Loy).

If TSA cannot articulate any reason to exempt CAPPS II 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.

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

In its notice, TSA has exempted CAPPS II 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;⁴¹ 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.⁴²

In lieu of the statutory, judicially enforceable right of access provided by the Act, TSA has established the "CAPPS II Passenger Advocate," apparently to act as a sort of ombudsman, to receive and process requests for access. According to the supplementary information accompanying TSA's notice, "passengers can request a copy of *most* information contained about them in the system from the CAPPS II passenger advocate."⁴³ The formal notice section, however, states that "[a]ll persons may request access to records containing information *they* provided," which presumably would include only the name, address, and telephone number given to an airline when making a travel reservation.⁴⁴ In addition, the notice provides that the system of records "may not be accessed for purposes of determining if the system contains a record pertaining to a particular individual."⁴⁵ Such limited, discretionary access to information

⁴¹ 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).

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

⁴³ Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45267 (emphasis added).

⁴⁴ *Id.* at 45269 (emphasis added).

⁴⁵ *Id.*

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 CAPPS II.

TSA's "passenger advocate" acting as middleman is no substitute for the judicially-enforceable access rights provided by the Privacy Act. TSA's notice states that access to one's personal information may be obtained "by sending a written request to the CAPPS II Passenger Advocate" and that "to the greatest extent possible and consistent with national security requirements, such access will be granted."⁴⁶ No time guidelines are specified for the procedure. However, TSA explains that "in most cases, the response to a record access request will very likely be that no record of the passenger exists in the system" because records are maintained for too short a time, although "[t]he duration of data retention" for non-U.S. persons "is still under consideration," and "[e]xisting records obtained from other government agencies, including intelligence information, watch lists, and other data will be retained for three years, or until superseded."⁴⁷

As a practical matter, therefore, the only information a passenger can access is the information he provided to the airlines himself. Moreover, even this information may not be accessible, as that information will likely be destroyed in the time it takes a passenger to contact the passenger advocate. In most cases, a passenger will be unable to gain access to records about him kept by the agency, and, in many cases, he will not even be able to learn that a record pertaining to him exists. In fact, the only indication a passenger may have that the government is keeping records about him is if he is given extra scrutiny at the security gate (or, of course, detained and arrested there). 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.

⁴⁶ *Id.*

⁴⁷ *Id.*

C. 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 the CAPPS II system 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;⁴⁸
- an agency must make notes of requested amendments within the records;⁴⁹ and
- an agency must establish procedures to handle disputes between the agency and individual as to the accuracy of the records.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 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 "[a] passenger who, having accessed his or her records in this system, wishes to contest or seek amendment of those records should direct a written request

⁴⁸ 5 U.S.C. § 552a(d)(2)(B), (d)(3).

⁴⁹ 5 U.S.C. § 552a(d)(4).

⁵⁰ 5 U.S.C. § 552a(f)(4).

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

⁵² 5 U.S.C. § 552a(g)(1).

to the CAPPS II Passenger Advocate."⁵³ Further, "[i]f the matter cannot be resolved by the CAPPS II Passenger Advocate, further appeal for resolution may be made to the DHS Privacy Office."⁵⁴ Notably, TSA reserves the right to alter even these minimal, discretionary procedures: "These remedies for all persons will [be] more fully detailed in the CAPPS II privacy policy, which will be published before the system becomes fully operational."⁵⁵ In addition, "DHS is currently developing a robust review and appeals process, to include the DHS privacy office."⁵⁶

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

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

Incredibly, TSA has exempted CAPPS II 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.⁵⁷ TSA does not even attempt to explain why it would be desirable or beneficial to maintain information in the CAPPS II system that is irrelevant and unnecessary, although it apparently intends to do so.

⁵³ Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45269.

⁵⁴ *Id.*

⁵⁵ *Id.*

⁵⁶ *Id.*

⁵⁷ 5 U.S.C. § 552a(e)(1); Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45269.

Such open-ended, haphazard data collection plainly contradicts the objectives of the Privacy Act and raises serious questions concerning the likely impact of the CAPPS II rating process on millions of law-abiding travelers.

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 CAPPS II will become an error-filled, invasive repository of all sorts of information bearing no relationship to its stated goal of increasing aviation security.

E. The Broad "Routine Uses" of CAPPS II Data will Exacerbate the System's Privacy Problems

TSA's notice identifies six categories of "routine uses" of the information that will be collected and maintained in the CAPPS II system of records.⁶⁰ These include anticipated

⁵⁸ S. Rep. No. 93-3418, at 47 (1974).

⁵⁹ OMB Guidelines at 28960.

⁶⁰ Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45268.

disclosure to a broad range of individuals and entities, such as "Federal, State, local, international, or foreign agencies or authorities . . . contractors, grantees, experts, or consultants . . . airports and aircraft operators."⁶¹ As we have shown, the information that would be disclosed is likely to include material about individuals that is not "relevant and necessary" to any legitimate aviation security requirements. 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 CAPPS II information that TSA anticipates underscores the need for full transparency (and resulting public oversight) and judicially-enforceable rights of access and correction.

Related to the breadth of the routine uses is 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. Admiral Loy discussed the issue in Congressional testimony, stating that "mission creep, if you will, is one of those absolute parameters that . . . I am enormously concerned about and we will build such concerns into the privacy strategy that we will have for CAPPSS II."⁶² Three months before the notice was published, Admiral Loy assured Congress that CAPPSS II was designed as an aviation security tool, and not as a law enforcement tool.⁶³

Despite those assurances, the CAPPSS II system already contains a carve-out for a purpose beyond its original mission. The notice states that "[a]fter the CAPPSS II system becomes operational, it is contemplated that information regarding persons with outstanding state or federal arrest warrants for crimes of violence may also be analyzed in the context of this

⁶¹ *Id.*

⁶² May 6 Loy Testimony.

⁶³ *Id.* Admiral Loy stated:

[w]e are not searching [the National Crime Information Center database] as part of the . . . data that we're looking at [A]t the moment we are charged with finding in the aviation sector foreign terrorists or those associated with foreign terrorists and keep[ing] them off airplanes. That is our very limited goal at the moment. . . . [E]ven as heinous as it sounds, the axe murderer that gets on the airplane with a clean record in New Orleans and goes to Los Angeles and commits his or her crime, that is not the person we are trying to keep off that airplane at the moment.

system."⁶⁴ While the government clearly has a legitimate interest in apprehending accused felons, there are innumerable reasons why it may want to locate particular individuals. Such uses of CAPPS II data, however, are plainly beyond the authorized scope of TSA's mission of ensuring aviation security. It is crucial that TSA define the purpose of CAPPS II, at the outset, more strictly and limit the use of collected information to its core mission.

F. Testing of CAPPS II Should Not Proceed Until TSA's Notice is Revised

While we welcome TSA's assurance that "[a] further Privacy Act notice will be published in advance of any active implementation of the CAPPS II system,"⁶⁵ we note the agency's statement that "[w]ith the publication of this notice, internal systems testing will begin, using this System of Records."⁶⁶ According to the agency, "[d]uring these tests, TSA will use and retain [Passenger Name Record] data for the duration of the test period."⁶⁷ It was recently reported that TSA is contemplating the issuance of a security directive requiring U.S. airlines to provide the agency with passenger information for use in the testing process.⁶⁸ Such data acquisition would 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 would raise significant privacy issues. 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.

⁶⁴ Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45266.

⁶⁵ *Id.*

⁶⁶ *Id.* at 45265-45266.

⁶⁷ *Id.* at 45267.

⁶⁸ Sara Kehaulani Goo, *TSA May Try to Force Airlines to Share Data*, Washington Post, September 27, 2003, Page A11.

Conclusion

For the foregoing reasons, EPIC believes that TSA must revise its Privacy Act notice for the CAPPS II system to 1) ensure greater transparency through the establishment of a non-classified 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 prepares a final Privacy Impact Assessment, discloses it to the public and receives 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,

David L. Sobel
General Counsel

Marcia Hofmann
Staff Counsel*

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

* *Bar admission pending*