February 19, 2003

Documentary Services Division Attention: Docket Section, Room PL-101 Docket No. OST-1996-1437 Department of Transportation, SVC-124 Washington, DC 20590

Re: Docket Number OST-1996-1437

Introduction

At a time when Congress, civil liberties groups, and the media are questioning the need for data surveillance systems like Total Information Awareness (TIA), we question the wisdom and legality of the proposed Aviation Security Screening Records (ASSR) system.

We make the following general comments: 1) the system of records does not meet the requirements of the Privacy Act; 2) the overly broad scope of the system, combined with the lack of adequate notice, access, and safeguards, eviscerates civil liberties and would be unconstitutional; 3) the system of records will not be useful for its intended purpose.

For these reasons, we request that the proposed regulations be withdrawn.

In addition, we are concerned that ASSR will be one of the key databases used in the Computer Assisted Passenger Prescreening System II (CAPPS II), which has attracted considerable attention in its own right as a data-mining system that is likely to be implemented before TIA.

Published media reports about CAPPS II indicate that it would subject all air travelers to massive data surveillance over air travel, hotel, vehicle rental, and credit card databases, as well as untold public records databases. CAPPS II therefore also raises major constitutional issues regarding the right to travel. If ASSR is part of CAPPS II, then ASSR enables an intrusive data surveillance regime that intrudes on one's zone of personal privacy merely because a person chooses to exercise his or her right of domestic interstate travel on commercial aircraft. Indeed, it is our understanding that data surveillance regimes are contemplated for other common forms of domestic travel, including trains and buses. If so, then every practical mode of travel will be subject to data surveillance.

We are particularly concerned that your agency may be publishing a notice with regard to the ASSR system of records without making clear to the public that it is in fact part of CAPPS II. If ASSR is part of, or is intended to be part of, CAPPS II, that fact should be plainly stated in the public notice. Otherwise, this public notice would essentially be concealing the truth about ASSR in order to evade the public debate that is currently taking place regarding secret data surveillance systems.

I. ASSR does not comply with the Privacy Act

As the Department of Justice has stated, “the purpose of the Privacy Act is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use, and disclosure of personal information about them.”

Moreover, the Act’s historical context is important to understanding its remedial purposes: “In 1974, Congress was concerned with curbing the illegal surveillance and investigation of individuals by federal agencies that had been exposed during the Watergate scandal; it was also concerned with potential abuses presented by the government's increasing use of computers to store and retrieve personal data by means of a universal identifier--such as an individual's social security number.”

One of the basic policy objectives of the Act, according to the Justice Department, was “[t]o establish a code of ‘fair information practices’ which requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.” Government, industry, and privacy advocates have generally agreed that the core areas of Fair Information Practices include Notice, Choice, Access, Security, and Enforcement.

Notice: The data collector should give you information about their data handling practices. What information are they collecting about you? Are they sharing it with others without your permission?

Choice: The data collector should give you a choice about how they can use the data: opting-in or opting-out. In other words, do they need to get explicit permission first or will they use the information unless you tell them not to?

Access: What rights do you have with regard to the information that has been collected about you? Can you view it? Amend it? Delete it? How much access do you have? Can you see everything that has been collected about you or just a part of it?

Security: Does the entity use adequate security in protecting the information they have stored in their databases? Do they use encryption? Have they undergone any internal audits to review their data practices?

Enforcement: What rights do you have if your information has been compromised either because of misuse or neglect?

The notice does not meet the (e)(4) notice requirements

The Privacy Act requires Federal Register publication of “a notice of the existence and character of the system of records.” 5 U.S.C. § 552a(e)(4). The purpose of this notice requirement is to provide the public with meaningful information about the system of records. Britt v. Naval Investigative Service, 886 F.2d 544, 548 (3d Cir. 1989). Such accountability not only benefits the individual who may be affected by the system but also the public as a whole, which has an overarching interest in knowing how the

government is using individuals' personal information in order to curb potential abuses. Ibid. Unfortunately, the current notice includes so many vaguely-defined, open-ended and inconsistent statements that it should not be considered such a notice.

Categories of individuals (B) Under § 552a(e)(4)(B), an agency must publish "the categories of individuals on whom records are maintained in the system." This requirement enables members of the public to understand whether and why their records are being maintained. The instant notice identifies two categories: "all individuals" who are air passengers, and "individuals who are deemed to pose a possible risk" with respect to transportation, national security, air piracy, terrorism or "a potential threat to airline or passenger safety, aviation safety, civil aviation, or national security." Substantially more detailed information is stored (and retained for a far longer period) on "individuals who are deemed to pose a possible risk . . . [or] potential threat."

This description of "categories" is too vague to be valid. The proffered description is so broad that it could be interpreted to include *all* passengers (since after all, any passenger is a possible risk and potential threat). To be valid, the description must provide reasonable notice as to who falls into which category.

Put another way, suppose that an individual somehow learns that information about him or her is being maintained because he or she is "deemed" a risk or threat. Nothing in this notice provides any sort of guidance as to whether the maintenance of such information is warranted or unwarranted. Furthermore, the Act's protections are designed to enable accountability to the public as well as to directly affected individuals. Thus, to be considered adequate, notice must describe the criteria and process for "deeming" individuals under this category such that it is possible to determine objectively the accuracy of categorization. Otherwise, criteria for categorization can shift with time or even be manipulated to fit individual cases, making it impossible for anyone to evaluate the fairness of the system.

Categories of records (C) Under § 552a(e)(4)(C), an agency must publish "the categories of records" maintained in the system. The notice here states that Passenger Name Records (PNRs) "and associated data" are stored for all individuals. The PNR consists of the information contained in airline reservation systems; the details are not described in this document (and indeed, one source argues that such fundamental concepts as name, date of birth, and passport number are not even part of the PNR but are instead included in the Advance Passenger Information (API) record).

It is our understanding that the PNR currently includes, among other things, the date the booking was made; the name of the travel agent or agency that made the booking; an itinerary listing all destinations to which the traveler flew; the manner of payment for the ticket; seat selection; and the number of pieces of baggage checked.

Our understanding what the PNR currently includes may be incorrect. If so, that is another reason to label this notice inadequate.

If the definition of the PNR expands over time, will the system of records automatically track the additional information? If the definition of the PNR is reduced over time, will any information eliminated from the PNR be eliminated from the system of records? Equally important, the phrase “associated data” is not described, and could easily be construed to provide no limits on the data that can be stored.

The information stored for “deemed” individuals contains several categories that are effectively unbounded; the information “may include” such extremely broad categories of risk assessment reports, financial and transactional data, public source information, proprietary data, and information from law enforcement and intelligence sources. In particular, “financial and transactional data,” “proprietary data” and “risk assessment reports” are such broad categories to be open-ended in practice.

To be considered adequate notice, this section must define the specific categories of information to be tracked by the system, which includes eliminating any open-ended categories such as “associated data,” provide an authoritative reference to the definition of any “terms of art” (e.g., "PNRs," “proprietary data” and “associated data”), and provide for periodic updated notices of changes in any such definitions over time.

Routine uses (D)

The notice states that “Information may be disclosed from this system as follows: (1) To appropriate Federal, State, territorial, tribal, local, international, or foreign agencies responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where TSA becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.” As we explain below, this routine use is incredibly sweeping and cannot be countenanced by the Privacy Act.

“It was Congress' intent that the routine use exception should serve as a caution to agencies to think out in advance what uses it (sic) will make of information." Britt, 866 F.2d at 548 (citation and internal quotation marks omitted). In Britt, the Third Circuit rejected as overbroad a notice of routine use to "federal regulatory agencies with investigative units." Id. at 548. The court said: “Because it is difficult to envision an agency that does not have some investigative unit, one could only conclude . . . that the [agency] might disclose any information it possessed to virtually any agency in the executive branch. Such breadth fails to constrain in a meaningful manner the [agency’s] discretion to disclose information.” Ibid.

The same is true here. By its plain terms, this routine use permits disclosure to any government agency with any kind of implementing, enforcement or licensing authority. It is hard to imagine any government agency that is outside this definition. Moreover, such disclosure would be permitted whenever TSA “becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.” Just about anything can constitute “awareness” of an “indication” of a “potential” violation. Indeed, the plain

terms of the routine use do not even clearly limit TSA's disclosure to agencies responsible for investigating or enforcing the "potential" violation. The word "appropriate" is too vague to provide a judicially cognizable standard limiting. As written, if TSA believed that a person had received a parking ticket or a public library fine, it could then disclose all ASSR information concerning that person to the FBI.
In addition, several of the routine uses include uses relating to "national security." While the specified purpose of ASSR is "aviation security," not everything relevant to national security is a matter of aviation security. Thus, the broad, catch-all invocation of "national security" permits routine uses that do not relate in any way to aviation security. Such uses may be important and desirable, but they are not "routine." Because "national security" is such a broad concept, it also fails to constrain in a meaningful manner TSA's discretion to disclose information.

Policies and practices regarding storage, retrievability, access controls, retention, and disposal of records (E)

We are also concerned about the lack of description regarding policies and practices for ASSR. We are particularly concerned about "access controls" and "retention and disposal."

The regulations here specify minimum safeguards substantially weaker than industry best practices; for example, there is no requirement that storage be encrypted. This is more than a hypothetical concern; recent loss of medical data bundled with SSNs and other sensitive personal data of more than 562,000 military personnel, retirees, and family members by the TriWest Corporation, who was entrusted to maintain "a system of records under the Privacy Act" (see "Officials Say Troops Risk Identity Theft After Burglary," ***The New York Times***, By Adam Clymer, 12 JAN 03, p. 12).

It is well known that many federal agencies do not maintain good computer security. In 1998 the GAO failed seven of 24 major agencies [in computer security], including the DOL; DHHS; the DOJ; and the Office of Personnel Management, the personnel office for the entire federal government.
www.whitehouse.gov/**omb**/inforeg/fy01securityactreport.pdf

Moreover, "OMB's first report to Congress on government information security reform in February 2002 identified six common government-wide security performance gaps. These weaknesses included:
(1) Lack of senior management attention;
(2) Lack of performance measurement;
(3) Poor security education and awareness;
(4) Failure to fully fund and integrate security into capital planning and investment control;
(5) Failure to ensure that contractor services are adequately secure; and

(6) Failure to detect, report, and share information on vulnerabilities.[1]

Many of the Routine Uses require additional Safeguards. For example, what provisions are made for validating the legitimacy of both the request and the requestor under routine use (3)? Access may be limited to those who need to know, but they don't say anything that ensures that the files would be used for their intended purpose. For example, in the past the IRS has been the subject of scrutiny for allowing IRS employees to peruse taxpayer files unnecessarily. See Senator Grassley's 1997 press release for more information.
http://www.senate.gov/~grassley/releases/1997/pr4-28.htm

There are no Safeguards in place for information that is released under Routine Uses that is later found to be outdated or incorrect. The broad distribution envisioned by these rules could have devastating effects on people.

As to retention and disposal, we also believe that the ASSR notice is inadequate. The records of non-"deemed" individuals are purged "after" the individual's air travel is complete; but there is no mention of how long afterwards this must be completed. There is no mention of what happens to the record if the individual fails to show for part (or all) of a journey - will these records be purged upon the completion of the flights upon which the traveler had a reservation?

The retention requirements do not discuss whether records are removed from backups as well. If the records are not removed from backups, then they can be reconstructed easily, and so despite the "purging" are still effectively available in the system. Note that most information processing systems today do not support removing records from backups.

The records of a "deemed" individual may be retained for up to 50 years. This is a long time for someone to possibly end up on a "no fly" list, or on a list which causes them to be searched more thoroughly than everyone else.

The notice of "routine uses" does not meet the (a)(7) requirement

Sec. 552a(a)(7) of the Privacy Act defines a "routine use" as "a use of a record for a purpose which is compatible with the purpose for which it was collected." The

---

[1] STATEMENT OF MARK A. FORMAN, ASSOCIATE DIRECTOR FOR INFORMATION, TECHNOLOGY AND ELECTRONIC GOVERNMENT, OFFICE OF MANAGEMENT AND BUDGET, BEFORE THE COMMITTEE ON GOVERNMENT REFORM SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT, AND INTERGOVERNMENTAL RELATIONS, U.S. HOUSE OF REPRESENTATIVES November 19, 2002, http://216.239.39.100/search?q=cache:G0KZI0sY1vEC:www.cio.gov/documents/forman_testimony.pdf+OMB+%22Poor+security+education+and+ awareness%22&hl=en&ie=UTF-8

general rule is that “compatibility” goes beyond mere “relevance.” Britt v. Naval Investigative Service, 886 F.2d 544, 549-50 (3d Cir. 1989) ("[t]here must be a more concrete relationship or similarity, some meaningful degree of convergence, between the disclosing agency's purpose in gathering the information and in its disclosure."). Several of the “Routine Uses” of information described in these regulations go so far beyond the stated purpose of facilitating an aviation security-screening program or more generally ensuring aviation security that they should be regarded as “incompatible.”

For example, Routine Use (1) allows the use of this information in any situation where TSA becomes aware of a “violation or potential violation of civil or criminal law or regulation.” Routine Use (5) allows the use of this information if it is “relevant” to activities as broad as “issuing a license, contract, grant, or other benefit.”

The statutory requirement of compatibility requires “a dual inquiry into the purpose for the collection of the record in the specific case and the purpose of the disclosure.” Britt, 844 F.2d at 548-549. The routine uses noted above ((1) and (5)) are not compatible with the purpose of gathering the information in the first place. As we discussed above, Routine Use (1) is incredibly broad and on its face would permit disclosure of ASSR information to virtually any government agency upon mere "awareness" of a "potential" violation of a law or regulation.

At a minimum, the Routine Uses must be restricted to uses that directly related to facilitating an aviation security-screening program or more generally ensuring aviation security.

There is a substantial likelihood that ASSR violates (e)(2)

The ASSR would maintain much personal information such as: PNR “associated data”; risk assessment reports; financial and transactional data; public source information; proprietary data; and information from law enforcement and intelligence sources. The Act, however, imposes a duty on agencies to "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs." 5 U.S.C. § 552a(e)(2).

The basic purpose of (e)(2) is to “reflect[] the basic principle of fairness . . . that where government investigates a person, it should not depend on hearsay or ‘hide under the eaves,’ but inquire directly of the individual about matters personal to him or her.” S. Rep. No. 93-1183, at 47 (1974), reprinted in 1974 U.S.C.C.A.N. 6916, 6962.

The routine uses listed for the ASSR clearly may result in such adverse determinations. See, e.g., Routine Use (1) (potential violations of law); (5) (hiring or retention of an individual or issuance of a security clearance, license, contract, grant, or other benefit). There is no indication, however, that any of the information in the ASSR would be

collected “to the greatest extent practicable directly from the subject individual.”

There is a substantial likelihood that ASSR violates (e)(9) and (e)(10)

These two provisions of the Act require that an agency "establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance” and "establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

The ASSR notice is virtually silent on these issues. Instead, the notice simply states that "[t]he computer system from which records could be accessed is policy and security based with real-time auditing" and that "[I]nformation in this system is safeguarded in accordance with applicable rules and policies, including the Department's automated systems security and access policies."

The (k)(1) and (k)(2) exemptions are insufficiently supported

TSA claims that this system of records is exempt from various Privacy Act requirements pursuant to 5 U.S.C. §552a(k)(1) and (k)(2). Neither claim, however, is adequately supported. The instant notice is virtually silent on any justification. The separate notice of proposed rulemaking, at 68 Fed. Reg. 2002 (Jan. 15, 2003), merely states that ASSR would be for a security-screening system that "may be used, generally, to review, analyze, and assess threats to transportation security and respond accordingly." We believe that this does not constitute sufficient justification for the (k)(1) and (k)(2) exemptions.

Even if the (k)(2) exemption is justified, the stated access procedures are insufficient

The regulations claim exemption from record access procedures pursuant to 5 USC § 552a(k). However, 5 USC § 552a(k)(2) states that

> .... if any individual is denied an right, privilege, or benefit ... for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished such information to the Government under an express promise that the identify of the source would be held in confidence ....

The Routine Uses include several ways in which the information in this system may be

used to deny an individual access to a right, privilege, or benefit to which he would otherwise be available, so the access described in 5 USC § 552a(k)(2) must be provided.

The Record Access Procedures do permit a limited form of access: U.S. citizens and Permanent Resident Aliens may request access to records containing information they provided, and further state, “In the case of air passengers the data is contained in the passenger name record (PNR).” This falls short of the requirements under 5 USC § 552a(k)(2) in several ways; most important, there are substantial additional categories of information to which the individual is given *no* access whatsoever.

There is no indication in the regulations that any categories of information will be provided to the government from a source who is furnishing it under an express promise of confidentiality.

At a minimum, access to all data needs to be provided for all individuals in situations where they are denied access to rights, privileges, or benefits. If there are any categories of information which will be gathered with promises of confidentiality, those should be mentioned in the regulations as well.

The overbroad scope of the system, combined with the Privacy Act deficiencies noted above, is dangerous to privacy and other civil liberties

One of the goals of the Privacy Act was to prevent the federal government from maintaining in one place so much information about a person that that person could no longer maintain a realistic sense of privacy. S.Rep. No. 1183, 93d Cong., 2d Sess., *reprinted in* 1974 *U.S.Code Cong. & Admin.News* 6916, 6930 ("the creation of formal or de facto national data banks, or of centralized Federal information systems without certain statutory guarantees would ... threaten the observance of the values of privacy and confidentiality in the administrative process”). As Senator Percy, one of the Privacy Act's cosponsors, stated, "[w]hen personal data collected by one organization for a stated purpose is used and traded by another organization for a completely unrelated purpose, individual rights could be seriously threatened." 120 Cong.Rec. 36,894 (1974), *reprinted* in Ash v. United States, 608 F.2d 178, 180 (5th Cir.), *cert. denied*, 445 U.S. 965 (1980).

The scope of the system is overbroad

The regulations propose storing a virtually-unlimited amount of information, about every air traveler, with extremely broad disclosure. In short, the regulations essentially describe a system of records that can track any information about any air travel passenger, and can

be disclosed to a huge number of people in virtually any circumstance. This is very problematic for several reasons. Two will be discussed in more detail below: risks to individuals' privacy increase with the amount of information being stored and disclosed; and the lack of effective safeguards increases the risk to other civil liberties as well.

The system procedures and safeguards are inadequate to protect privacy and civil liberties

One of the basic principles of fair information practices is access. But ASSR provides very limited access by individuals to access or contest records "containing information they provided." Virtually none of the information discussed in the "Categories of Records" section falls into this category; for example, PNRs and reservation information are provided by the airlines, proprietary data is provided by some vendor; etc. As noted earlier, we believe this violates the (e)(2) requirement. We note here that, as a result, ASSR takes on a certain "Alice in Wonderland" quality: the system assesses persons as threats, but provides only grudging access to the information on which that assessment is based.

The obvious problem here is inaccurate data. We believe that any system whose raison d'etre is to generate suspicion about individuals is unfair unless individuals have a reasonable opportunity to dispel that suspicion.
Recently, the Privacy Commissioner of Canada, George Radwanski, delivered a report to the Canadian Parliament describing his concerns about a similar piece of legislation. He states:

> "The more information government compiles about us, the more of it will be wrong.
>
> That's simply a fact of life.
>
> Several years ago, after the existence of Human Resources Development Canada's "Longitudinal Labour Force File" was brought to light by my predecessor, many people demanded to see the information that had been held about them. They were astonished by the number of factual errors. That was only a research database, so its inaccuracies probably would have remained relatively benign even if it had not been dismantled.
>
> If information that is actually about someone else is wrongly applied to us, if wrong facts make it appear that we've done things we haven't, if perfectly innocent behavior is misinterpreted as suspicious because authorities don't know our reasons or our circumstances, we will be at risk of finding ourselves in trouble in a society where everyone is regarded as a suspect. By the time we clear our names and establish our innocence, we may have suffered irreparable financial or social harm.

> Worse yet, we may never know what negative assumptions or judgments have been made about us in state files. Under exemptions to the general right of access under the *Privacy Act*, Canadians do not have the right to see the personal information that the Government holds about them if it pertains to national security or an ongoing investigation.
>
> The bottom line is this: If we have to live our lives weighing every action, every communication, every human contact, wondering what agents of the state might find out about it, analyze it, judge it, possibly misconstrue it, and somehow use it to our detriment, we are not truly free."
> http://www.privcom.gc.ca/information/ar/02_04_10_e.asp#overview

This is precisely the problem with these proposed regulations: people will never know what kinds of negative assumptions have been made about them because of inaccurate data and they will never have the means to clear their names.

In any case, information provided by the data subject is rarely the problem. Problems occur when information is added to a file which the data subject has not seen nor has any chance to contest. For example, information that is proprietary in nature or relates to law enforcement or intelligence may include information that has been obtained from an Internet Service Provider about the data subject's web browsing habits. URLs and other information may be included – but because many people may use the same computer, it may be very difficult to ensure that the data collected and placed in the database actually is associated with the data subject.
In the case of this information being disclosed for court, administrative, adjudicative, or tribunal bodies, the rules do not provide any mechanism for the data subject to get access for this information.

Additionally, the risk of identity theft increases with each disclosure of personal information. As discussed above, information gathered includes financial and other transactional information. When combined with the aforementioned lack of safeguards, this can lead to unscrupulous individuals taking advantage of their privileged ability to access this information. According to testimony to the U.S. Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information, Beth Givens, Director of the Privacy Rights Clearinghouse testified that many cases of identity theft are "inside jobs" (see http://www.privacyrights.org/ar/id_theft.htm and "Identity Theft [is] More Often an Inside Job: Old Precautions Less Likely to Avert Costly Crime, Experts Say," ***The Washington Post***, by Jay Mathews, 3 DEC 2002, Page A1).

Moreover, disposition of risk assessment reports once they have been compiled is another issue. Since the Privacy Act doesn't limit the sharing of opinions without data attached, it seems likely that the reports could be disseminated quite broadly to the detriment of the data subject – much in the same way the FBI has lost control over some of their "no fly" lists. The result is that people don't know how to get off of a "no fly" list. For one example of this, see
http://www.newyorker.com/talk/content/?020513ta_talk_mcnamer to read about one

woman's experience of not being able to get off of a "watch" list. She never knows when she gets to the airport what kind of security measures she will have to endure because her name resembles the name of a known criminal. As discussed in "Post-Sept. 11 Watch List Acquires Life of Its Own FBI Listed People Wanted for Questioning, But Out-of-Date Versions Dog the Innocent," by Ann Davis, Staff Reporter of The Wall Street Journal, 19 NOV 02), this is not an isolated problem.

Finally, the system raises significant constitutional issues regarding the right to travel. Fundamental to a democratic society is the ability to wander freely freely and anonymously without being compelled to divulge information to the government about who we are or what we are doing. See Papachristou v. City of Jacksonville, 405 U.S. 156, 164 (1972); Brown v. Texas, 443 U.S. 47, 52-53 (1979); Hutchins v. Dist. of Columbia, 188 F.3d 531, 537 (D.C. Cir. 1999) (right to "interstate travel is a fundamental right subject to a more exacting standard" than ordinary due process scrutiny).

The ASSR system clearly affects the right to interstate travel, and it does so in a vague and open-ended way that raises constitutional concerns. See, e.g., Kolender v. Lawson, 461 U.S. 352, 36162 (1983) (California statute requiring an individual who loitered or wandered the streets to produce "credible and reliable" identification to an officer upon request of a police officer was unconstitutional on vagueness grounds); Lawson v. Kolender, 658 F.2d 1362, 1366-67 (9th Cir.1981) ("serious intrusion on personal security outweighs the mere possibility" that identification might lead to arrest), *aff'd on other grounds*, 461 U.S. 352 (1983). Of particular concern here is that air passenger information is being collected without any sort of particularized suspicion.

ASSR will not be useful for its intended purpose

Since the information stored for any non-deemed individual (PNRs "and associated data", and potentially any reference to the individual in reservation and manifest information) is purged after the completion of the individual's air travel, it does not improve screening and risk-assessment beyond today's level.

Data Quality

A major reason that ASSR will not be useful for its intended purpose is the low quality of the data in the system.

The information stored for "deemed" individuals contains substantial information that is likely to be incorrect. A recent PIRG study illustrated that records kept by credit bureaus (a highly regulated industry) on individuals have up to a 70% error rate – and 30% of those are serious enough to prevent an individual form obtaining credit. See http://www.pirg.org/reports/consumer/mistakes/page1.htm for more details. Given those statistics, it would seem highly likely that data collected from data aggregators (a non-regulated industry), or from public records is likely to have substantially more errors than data collected by credit bureaus.

Information in risk assessment reports is divided into two categories: the risk assessment report, and the data that was used to make the risk assessment.

With regard to the risk assessment report, several questions arise. What are the criteria used to decide whether one is a risk, who evaluates the criteria, and if intelligence information is included in the risk assessment report, how does the agency plan to eliminate bias?

With regard to the data that is used to populate the risk assessment report, similar questions arise. What kinds of activities constitute "risky" behavior? Data that has been scooped up by law enforcement in the past include such activities as those who like to scuba and those who like to order pizza via credit card. In addition, police often target specific groups for extra surveillance and inject their own biases into their reports. See "They Know When You Are Sleeping" http://www.thenation.com/doc.mhtml?i=20030127&s=pollitt that discusses the types of "extremist" organizations listed in police files: the "American Friends Service Committee, the Rocky Mountain Peace and Justice Center and NARAL".

Some travelers may be reluctant to disclose accurate travel information knowing that this information will be compiled in a government database for unspecified future investigative purposes; this may actually lead to a situation worse than the current one.

Entering erroneous and biased data into a surveillance system this vast, particularly where the data subject has no ability to correct or contest the data, should be avoided at all costs.

Conclusion

We have grave concerns about the privacy and civil liberties of citizens once this rule has been implemented. Because the proposed rule impacts the rights of every single person who uses the air transportation system, we believe that notice to the public should not only be written in a clearer style, but the time period that the public has to comment should be much longer.

In addition to the serious notice deficiencies, we have substantive concerns about the proposed rule, which we've detailed in our comments.

For all of these reasons, we request that the proposed regulations be withdrawn.

Sincerely,

Beth Givens Privacy Rights Clearinghouse

Katherine Albrecht CASPIAN

Richard Sobel Cyber Privacy Project

Michael Stollenwerk

Lee Tien Electronic Frontier Foundation

Deborah Pierce PrivacyActivism

NB: For contact purposes, please contact: Lee Tien Senior staff attorney Electronic Frontier Foundation 454 Shotwell Street San Francisco, California 94110 (415) 436-9333 x 102 (voice) (415) 436-9993 (fax) tien@eff.org