CENTER FOR DEMOCRACY and TECHNOLOGY

1634 Eye Street, NW Suite 1100
Washington, DC 20006
(202) 637-9800
Fax: (202) 637-0968
email: info@cdt.org

February 24, 2003

Department of Transportation
Documentary Services Division
Attention: Docket Section, Room PL401
Docket No. OST-1996-1437
SVC-124
Washington, DC 20590

COMMENTS OF THE CENTER FOR DEMOCRACY AND TECHNOLOGY
on Aviation Security Screening Records System, 68 Fed. Reg. 2101 (Jan. 15, 2003)

The Center for Democracy and Technology (CDT) takes this opportunity to express its concerns about the Transportation Security Administration's proposed Aviation Security Screening Records (ASSR) system. CDT believes that the notice published in the Federal Register on January 15, 2003, does not comply with the Privacy Act, because it is so vague and lacking in data use and retention guidelines that it is impossible to tell how the system will work, whether it will work, and whether the obvious harms to security and privacy that can flow from misuse or misinterpretation of personal data will be addressed and minimized. In these comments, CDT will set forth the factors and principles that CDT believes the TSA must consider – and publicly address – before it establishes the ASSR system of records. We believe that addressing these factors and principles in guidelines for the ASSR is necessary both to ensure the counter-terrorism effectiveness of the system and to protect as much as possible the privacy and due process rights of innocent air travelers.

In the wake of September 11, several government agencies have indicated their intent to draw on the types of information sources that TSA has pointed to here, such as "public source" and proprietary databases. Such uses of information are certainly important to both transportation safety and the broader fight against terrorism, but many questions need to be answered before any agency begins implementing specific data analysis activities. Indeed, just this month Congress demonstrated its concern about information analysis technologies by prohibiting deployment of the Pentagon's Total Information Awareness datamining program until the Defense Department provides further information to Congress about the uses and privacy implications of the program, and until Congress specifically authorizes that the program go forward.

There are six principles that CDT believes TSA should address before implementing any data access or data collection system like that apparently

contemplated for the ASSR. These principles are drawn from various sources, including the Privacy Act itself; Fair Information Principles that have been agreed upon by the federal government, privacy experts and industry groups;[1] and other guidelines for the use of electronic information in the law enforcement arena, such as the Justice Information Privacy Guideline.[2] These principles include:

- collection limitation;
- use and disclosure limitation;
- retention limitation;
- data quality;
- system security;
- enforcement and controls.

CDT believes that TSA must carefully apply these principles to each of the categories of information that TSA intends to use.

Collection Limitation

The collection limitation principle holds that no more data should be collected or accessed than is necessary to accomplish the legitimate purpose at hand, in this case screening air passengers.

TSA has yet to answer, except in the most general and broad terms, key questions about the categories of information it intends to collect or access, to whom that information will pertain, and what will be the standards for access or collection. It has provided only the most rudimentary description of the categories of individuals and categories of information covered by the ASSR system. The notice states that ASSR will contain information about all "[i]ndividuals traveling to, from or within the United States [ ] by passenger air transportation" as well as "individuals who are deemed to pose a possible risk to transportation or national security, a possible risk of air piracy or terrorism, or a potential threat to airline or passenger safety, aviation safety, civil aviation, or national security." It further states that ASSR will include "Passenger Name Records (PNRs) and associated data," passenger manifests, and for those deemed a potential risk to transportation security, "risk assessment reports; financial and transactional data; public source information; proprietary data; and information from law enforcement and intelligence sources."

---

[1] The Fair Information Principles include Notice, Choice, Access, Security and Enforcement. Those principles were developed for government and private entities that collect information about people, but were not specifically intended to govern information collected in the law enforcement or national security context. For the purposes of these comments, CDT has relied on those core principles but has modified them so that they are appropriate to the transportation security context.

[2] The Justice Information Privacy Guideline can be found at http://www.ncja.org/pdf/privacyguideline.pdf.

These descriptions fail to define, or set any limitations on, the expected collection of information. Establishing standards governing the collection of information is a prerequisite to establishing a new system of records consisting of personal information. First, a government agency that is collecting information should specify the purpose of the collection for each category of information that it is gathering.[3] Second, the data collector should not gather any personal information not directly relevant to the purpose of the collection. The purpose set out in the Privacy Act Notice – that "the system will be used to facilitate the conduct of an aviation security-screening program, including risk assessments to ensure aviation security" – is eminently legitimate, but there is no effort by the TSA to explain how the various kinds of information it seeks will be related and limited to that purpose.

In some contexts, the Fair Information Principles of Notice and Choice help to constrain the collection of information: People are given notice that the collector is gathering information about them, and they can exercise a choice about how the collector will use the information. TSA should first determine when individual notice is and is not feasible in the context of air passenger screening. For example, it may be entirely feasible to give passengers notice that certain name and address databases are being checked. This may give the passenger an opportunity to account for errors in those databases, if, for example, the passenger has recently moved.

Other constraints are normally placed on information collection, such as setting a standard that the collector must meet in order to obtain the information it seeks. For example, a police officer investigating a criminal case must show probable cause that a crime was or is being committed to obtain a search warrant, and a prosecutor can obtain personal records only on a showing of relevance. TSA should specify the standard that will govern its collection of information and must apply that standard to each category of information it seeks.

TSA also needs to provide more details about its intent to collect virtually unlimited categories of personal information about people "deemed to pose a possible risk to transportation security." The Notice does not even explain which comes first – data collection or risk assessment? It should be made clear on what basis, and by whom, a person will be deemed a possible risk, and whether the vast array of personal information identified in the Privacy Act Notice will be used to place someone in the "possible risk" category.

Finally, if TSA is drawing on third party data, it must consider whether that data is in fact relevant to the goal of airline safety. Much of the data in commercial systems was not originally collected for law enforcement or national security purposes. For example, commercial records intended to be used for direct marketing purposes may have little value for determining whether an individual is permitted to board an airplane.

[3] "Collection" of information refers both to initial collection and collection from other sources, such as databases created by other agencies and the private sector.

In our view, TSA must have a process for justifying that specific categories of information to be accessed by ASSR are necessary and relevant to the goal of screening air passengers.

Use and Disclosure Limitation

Next, TSA must ensure that its use of the information collected and its disclosure of that information to other public and private entities are limited to the purpose of airline security. With regard to the principles surrounding use and disclosure, CDT is particularly concerned with the broad and sometimes vague routine uses that TSA set out in its Privacy Act Notice.

The routine uses identified by the Privacy Act Notice contemplate sharing ASSR data with private contractors, a myriad of government entities, and airports and airlines. They raise serious concerns about how the broad categories of information to be collected by TSA will be used and to whom they will be disclosed.

CDT is concerned with the lack of clarity about TSA's own intended uses of the information it plans to gather. Based on the Privacy Act Notice, it is unclear whether: (1) TSA itself will determine that a particular passenger is a potential risk; (2) TSA will rely on other agencies to identify potential risks; or (3) both. The Notice does not explain what role, if any, the airlines will have in using or interpreting the data. Nor does the Notice explain how risk assessments, however developed, will be used: to subject checked baggage to more intensive searches, to divert certain passengers to more intensive physical screening, to deny passengers the opportunity to fly, or for other purposes. The failure to define the uses of the information makes it impossible to evaluate the likely privacy impact of the system, let alone to evaluate its effectiveness.

TSA should specifically delineate how it will use its risk assessments. It must explain the consequences of being "deemed" a risk. Under what circumstances will a passenger be subject to heightened scrutiny? Under what circumstances will a passenger not be permitted to board an airplane at all?

With regard to TSA's disclosure of information to other entities, TSA must evaluate each potential disclosure based on the purpose of the ASSR system in order to determine what information will be disclosed to whom. For example, based on the purpose of the ASSR, it is unclear when it would be necessary to disclose a passenger's financial data to an airline or airport. To what end might those entities use such information? TSA should establish standards for assessing whether particular information should be disclosed to a particular entity. The Privacy Act itself provides some specific scenarios in which an agency may share information, but in several instances the TSA contemplates going further than those explicit Privacy Act exemptions. For example, the Privacy Act allows a data collector to provide information to law enforcement officials upon a written request for specific information, *see* 5 U.S.C. § 552a(b)(7); TSA indicates that it will volunteer potentially vast amounts of information to law enforcement officials under Routine Uses 1 and 7. TSA must clearly explain how it will decide whether to provide other agencies and private entities with access to its information. Vague assertions about "security" are simply inadequate.

In sum, TSA should answer these questions about its use and disclosure of information before moving forward with the ASSR system of records:

1. How will TSA itself use the information it learns through the ASSR system, and what standards will govern?
2. For each potential disclosure, what standard must TSA meet in order to go forward?
3. Does each use and disclosure of information flow directly from the stated purpose of TSA's data collection?
4. Are TSA's use and disclosure of the information consistent with the purpose of the initial data collector?
5. Who within TSA and related federal contractors has access to what information, and how is that decision made?
6. Are there any circumstances under which individuals can be notified what information about them will be or has been shared?

Retention Limitation

TSA has provided insufficient information about its retention policies. The Privacy Act Notice indicates that for those passengers not deemed a possible risk, "records will be purged after completion of the individual's air travel to which the record relates." This is a sound principle, for it would prevent the unnecessary retention of data, and we urge that it be retained.

For those passengers deemed a possible risk, data will be maintained for up to 50 years. The 50-year retention period raises concerns. TSA should define exactly what information is retained. For example, if an individual is deemed a security risk when she arrives at the airport because she purchased a one-way ticket with cash just hours before the flight, exactly what information does TSA retain, and what information can it use again? Does the fact that TSA once deemed a person a security risk mean that TSA is more likely to view that individual as a threat the next time she arrives at the airport?

However, TSA should consider how its retention policies relate to its auditing and complaint procedures, which will be addressed further below. TSA must strike a balance between purging its records when possible, and maintaining an audit trail. If a passenger is subjected to a higher level of security scrutiny every time he goes to the airport and believes that treatment is improper, the passenger should have the ability to obtain information to challenge TSA's basis for treating him as a potential risk. But if TSA has purged all information from its records, there is no way to address and remedy complaints.

Data Quality

TSA's Privacy Act Notice fails even to mention a key component of all information systems, and particularly one that will "mine" third party data: data quality. Data quality includes the accuracy and completeness of data, as well as whether it is up-to-date. Evaluating and maintaining data quality is a central issue for a system

like ASSR – one that can seriously impact both the efficacy of the program and the civil liberties of airline passengers.

In other contexts, data quality is often maintained by allowing individuals to have access to the data so they can identify errors. In fact, TSA contemplates allowing individuals to have access to third party information that they themselves provide to TSA and to seek amendment of that information. However, TSA also intends to utilize information obtained from third parties. CDT recognizes that in some instances there may be security concerns with allowing individualized access to that information, but TSA should consider providing at least some such access as part of its complaint procedures.

Given the many sources of information identified by the Privacy Act Notice, and assuming individualized access will be limited, it is imperative that TSA establish data quality standards and auditing mechanisms. Both commercial databases and government databases have severe data quality problems. TSA should understand, for each source of information, the degree of accuracy and completeness of the data, and how often the information is updated. If TSA acquires data quality assurances from third parties, it should set up an auditing mechanism to test the data quality, and should consider imposing negative consequences where data fails to meet certain standards. TSA also must understand that the currency of data will vary depending on whether TSA is dipping into third party databases when it needs certain information, or is acquiring the databases at a particular point in time. If the latter, it must track the date it acquired the information and make provisions for updating it.

Where data quality is uncertain or inadequate, TSA must be prepared not to use that information, or it must establish verification procedures. Where there are multiple sources for the same data, TSA must rely upon the "best" information available, as defined by its data quality standards.

Thus, TSA must answer these questions about data quality before moving forward with the ASSR system of records:

1. For each source of information, how accurate, complete and up-to-date is the information?
2. What methods will be used to ensure data quality?
3. What data quality standards will govern for purposes of gathering data, using data and disclosing data?
4. How often is each data source updated?
5. How is each use and disclosure of the information affected by the quality of the data underlying that use or disclosure?

System Security

As TSA already recognized in its Privacy Act Notice, it must ensure the security of its system from both internal and external threats – particularly given the sensitive nature and breadth of the information it intends to collect. A security strategy must address unauthorized access to and use of the information, as well as unauthorized destruction and modification of the information. TSA must carefully consider which

employees and contractors should have access to the system and on what basis, and (as the Privacy Act Notice appropriately indicates it will) should track the users of the system. TSA also must protect against external threats, both in terms of cybersecurity and physical security.

In the case of data retained on persons deemed to be risks, TSA should pay particular attention to establishing safeguards against the misuse and improper disclosure of information that it intends to keep for 50 years. CDT understands that in the law enforcement, national security and intelligence contexts, information is often kept for far longer periods of time than in other settings. But where agencies keep information for long periods of time, they should have strict standards to protect against improper use and dissemination of the information.

Enforcement and Controls

TSA should design ASSR to facilitate enforcement of privacy principles, including by auditing adherence to system guidelines. This principle involves several interrelated issues, including setting up complaint procedures, establishing audit trails to protect against unauthorized access and misuse, and creating audit mechanisms to ensure that privacy principles are being enforced.

First, TSA should establish a complaint process. Passengers need to understand enough about TSA's risk assessment program to realize that if they are being diverted to a higher level of security screening each time they fly, it may be due to erroneous information in TSA's system. To exercise their due process rights, passengers need some form of notice that a screening process is occurring, as well as information about how to file a complaint. The Privacy Act Notice addresses passengers' ability to contest records containing information that they themselves provide to TSA (although it is unclear what this information might include), but it does not provide for any complaint process where TSA evaluates them based on information obtained from third parties. Given the potential problems with data quality addressed above, this is a significant issue that TSA has yet to address. If TSA intends to rely on data from third parties, it must provide some form of complaint and amendment process.

Second, TSA should consider establishing audit logs, both to facilitate the complaint process and to allow for audits of system use. However, TSA should recognize that creating audit trails can be a double-edged sword because the audit trails themselves sometimes become a new source of information. Logging each query made in the system allows auditors to review how the system is being used, but it also allows the results of those queries to become a separate intelligence source. TSA must carefully consider the auditing issue to balance these competing concerns.

Third, TSA should enforce its privacy rules, and ensure that the system designers fully understand them. TSA might consider naming a high-level Privacy Officer with the primary responsibility of establishing, reviewing and enforcing privacy standards.

Thus, TSA must answer these questions about enforcement and auditing mechanisms before moving forward with the ASSR system of records:

1. What is the complaint process for individuals who believe that TSA has erroneous information about them or has treated them improperly?
2. How will TSA set up its auditing mechanism both to protect against misuse of the system and to ensure that the audit trail itself does not become yet another system of records?
3. How will TSA enforce its privacy rules? Who is responsible for ensuring that the system is designed to protect individual privacy?

Conclusion

TSA has much work to do before moving forward with this program. Its Privacy Act Notice leaves a multitude of fundamental questions unanswered. CDT urges TSA to consider establishing a clear set of privacy rules based on the foregoing principles before implementing the ASSR system of records. We would be happy to aid TSA in that process.

Respectfully submitted,

James X. Dempsey, Executive Director
Lara M. Flint, Staff Counsel
Center for Democracy and Technology
1634 I Street, NW, Suite 1100
Washington, DC 20006
(202) 637-9800
http://www.cdt.org