Prepared Statement of
James X. Dempsey
Executive Director
Center for Democracy and Technology

before the

House Committee on Homeland Security
Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity

"Improving Pre-Screening of Aviation Passengers against Terrorist and Other Watch Lists"

June 29, 2005

Chairman Lungren, Ranking Member Sanchez, Members of the Subcommittee, thank you for the opportunity to testify today.

I am Executive Director of the Center for Democracy and Technology. CDT is a non-profit, public interest organization dedicated to promoting civil liberties and democratic values for the digital age. I am also privileged to serve as an associate member of the Markle Foundation Task Force on National Security in the Information Age. The Markle Task Force, co-chaired by Zoë Baird and Jim Barksdale, is comprised of leading experts from the fields of national security, technology, and privacy, including CDT's President Jerry Berman. Its members have extensive experience in and out of government at the federal and state level, in both the legislative and executive branches, from the administrations of Presidents Carter, Reagan, George H.W. Bush, Clinton, and George W. Bush. The Task Force has published two reports, "Protecting America's Freedom in the Information Age" (2002) and "Creating a Trusted Information Network for Homeland Security" (2003), available at http://www.markletaskforce.org. The Task Force, which is continuing its work, has offered concrete recommendations for strengthening national security while protecting civil liberties by creating a decentralized network for sharing and analyzing information within a framework of accountability and oversight. This testimony is based in large part on recommendations the Task Force submitted to the Transportation Security Administration in February of this year.

I. Background and Summary of Conclusions

Terrorists continue to target passenger airplanes. One element of a layered security system for air transport is the screening of passengers. Every day, over 1.5 million passengers board airplanes in the United States for domestic flights. It is infeasible to intensively scrutinize each of those passengers. To focus resources, it is necessary to make judgments about passengers before they reach the security checkpoint.

The Transportation Security Administration (TSA) is testing a proposed passenger screening system named Secure Flight. The system is mandated by Section 4012 of the

Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. No. 108-458). It would implement a recommendation of the 9/11 Commission.

Section 4012 of the Intelligence Reform Act requires TSA to "assume the performance of the passenger screening function of comparing passenger information to the automatic selectee and no fly lists and utilize all appropriate records in the consolidated and integrated terrorist watch list maintained by the Federal Government in performing that function." Section 4012 specifies that DHS must:

- include a procedure to enable airline passengers who are delayed or prohibited from boarding a flight because of the system to appeal such determination and correct information in the system;
- ensure that databases that will be used to establish identity of passengers will not produce a large number of false positives;
- establish an internal oversight board;
- establish sufficient operational safeguards to reduce the opportunities for abuse;
- implement substantial security measures to protect against unauthorized access;
- adopt policies establishing effective oversight of the use and operation of the system; and
- ensure that there are no specific privacy concerns with the technological architecture of the system.

Section 4012 also requires the Secretary of Homeland Security, in consultation with the Terrorist Screening Center, to "design and review, as necessary, guidelines, policies, and operating procedures for the collection, removal, and updating of data maintained, or to be maintained, in the no fly and automatic selectee lists."

In addition, section 522 of the fiscal year 2005 DHS Appropriations Act (Pub. L. No. 108-334), required the Government Accountability Office to assess 10 aspects of Secure Flight development and report to Congress, which GAO did in March of this year.[1]

On September 24, 2004, even before the Intelligence Reform Act was adopted, but after the report of the 9/11 Commission was widely endorsed, the TSA released three documents that outlined plans for testing Secure Flight. As detailed in a Privacy Act Notice, Privacy Impact Assessment, and Emergency Clearance Request (collectively, the "September 2004 Notices"),[2] Secure Flight would have three components:

- collection from the airlines of identifying information contained in the Passenger Name Records (PNRs) for matching against the consolidated watch list of the FBI's Terrorism Screening Center (TSC);

---

[1] U.S. Government Accountability Office, "Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed," March 2005, GAO-05-356.

[2] Notice to Establish System of Records, Docket No. TSA-2004-19160, 69 Fed. Reg. 57345 (Sept. 24, 2004); Notice of Privacy Impact Assessment, Docket No. TSA-2004-19160, 69 Fed. Reg. 57352 (Sept. 24, 2004); Notice of Emergency Clearance Request, Docket No. TSA-2004-19160, 69 Fed. Reg. 57342 (Sept. 24, 2004).

- possible use of commercial databases of personally identifiable information to verify the information provided in the PNR; and
- use of "streamlined" behavior rules drawn from the current Computer Assisted Passenger Prescreening System (CAPPS I), which uses behavioral factors such as purchase of a one-way ticket to select passengers for enhanced scrutiny.

While use of commercial data and continued use of CAPPS I rules were not required in Section 4012, they have remained part of the Secure Flight plan and test. Moreover, in regards to the use of commercial data, it is now clear that TSA is examining not merely its value to verify identity but also its value in augmenting PNR information to make a better watch list match. Furthermore, while Section 4012 requires the government to bring "in-house" the process of matching passenger data with watch lists, TSA seems to be saying in its latest Secure Flight notice that it will also assume full responsibility for administering the behavioral rules of CAPPS. If so, this is a big change, with major implications for privacy, since application of the CAPPS behavioral rules would require the government to access much more personal information than required for watch list matching.

To test Secure Flight, TSA required airlines to turn over all Passenger Name Records (PNRs) from June 2004. TSA has been using this historical data to test the efficacy of its proposed system, including the possible use of commercial data, and to compare results under Secure Flight with results under the old CAPPS system. In general, passengers face no adverse consequences in the test phase, unless the search turns up a name on the watch list as having been on a flight last June, in which case the FBI will be notified. According to TSA, no such notification has been justified.

There are several commendable elements of TSA's process in developing Secure Flight:

- In response to congressional oversight and public criticism, TSA fundamentally re-examined the previous proposal for a new airline passenger security program, the second-generation Computer Assisted Passenger Prescreening System ("CAPPS II").
- After issuing an opaque Privacy Act notice on CAPPS II in January 2003, TSA took a more transparent approach, with both the CAPPS II notice of August 2003 and the Secure Flight notices of September 2004. This included the publication of a Secure Flight Privacy Impact Assessment (PIA) *before* going forward with the test phase, an important precedent within DHS and for other agencies.
- Before implementing a new passenger screening system, TSA is conducting testing to determine what is most effective. From the September 2004 Notices, it would appear that TSA has not prejudged the outcome of the testing.
- In its Secure Flight proposal, TSA appears to have dropped some of the most troublesome aspects of CAPPS II, including the probability-based review of all passengers based on unidentified government data to determine each passenger's "risk" score and the notion of using Secure Flight for purposes other than enhancing the security of domestic flights by identifying passengers who warrant further scrutiny prior to boarding an aircraft based on possible terrorist connections.

However, TSA stumbled badly when its testing procedures departed from the assurances it provided to Congress and the public in the September 2004 Notices. In particular, contrary to indications in the Notices, TSA and its contractors acquired and retained personal information from commercial databases, as TSA admitted in a revised notice issued earlier this month.[3] This misstep has once again cast doubt on the credibility of the government.

However, we must not let this controversy detract attention from much more important issues that remain unanswered about Secure Flight. Important efficacy, privacy and due process issues remain to be resolved before full implementation can begin. As the GAO found in its March 2005 report:

- "the effectiveness of Secure Flight in identifying passengers who should undergo additional security scrutiny has not yet been determined" (p. 27);
- "the accuracy of commercial data is uncertain" (p. 32);
- "key issues regarding how [PNR] data will be obtained and transmitted have not yet been resolved" (p. 29);
- "the ability of Secure Flight to make accurate matches between passenger data and data contained in the terrorist screening database is dependent on the quality of the data [in the screening database]. … the accuracy of this data has not been fully determined" (p. 6).

In particular, because expanded watch lists are the core of the proposed program, the fidelity, data quality and overall reliability of those watch lists will be very important. In June of this year, the Department of Justice Inspector General found that the Terrorist Screening Center could not ensure that the information in the watch list database was complete and accurate. The IG's report identifies a number of types of errors in TSC data.[4] While TSA has begun to develop its own redress procedures, it should work with other agencies to develop standards for watch listing and redress mechanisms so passengers will have the ability to challenge a watch list entry or an erroneous watch list match. Proper resolution of those issues will be critical to the success of any air passenger screening system, in terms of both enhanced security and protection of civil liberties. The Intelligence Reform Act required the Executive branch to develop criteria and minimum standards for watch listing. As far as we know, those criteria and standards have not been developed.

Moreover, the controversy over collection of commercial data in the test phase of Secure Flight must not obscure more important questions: Where are the results of the test of matching June 2004 PNR data against the watch list and how will the lessons learned from the test affect implementation of Secure Flight? What has TSA learned from its test of commercial data, and what does it intend to do with commercial data if Secure Flight is permanently implemented? What has TSA determined is the best method for matching names? What is the quality of PNR data and what is the best way for the government to get the minimum amount of data to make

---

[3] Notice to Supplement and Amend Existing System of Records and Privacy Impact Assessment, Docket No. TSA-2004-19166, __ Fed. Reg. ___(June 20, 2005).

[4] U.S. Department of Justice, Inspector General, "Review of the Terrorist Screening Center," June 2005, Audit Report 05-27, at p. xi.

reliable matches? These and other key questions should be the focus of Congressional and public oversight.

II. Watch Lists

TSA has accepted – and Congress has mandated - the recommendation of the 9/11 Commission that airline passengers should be screened against terrorist watch lists and the government, not the airlines, should perform that such screening. Secure Flight should be an improvement over the current CAPPS, because the watch lists should offer a particularity of suspicion that behavioral rules cannot, and because it is not desirable to disclose the watch list to airlines. Despite these advantages, however, Secure Flight will only be as good as the watch lists on which it is based and the way in which they are searched. The watch list to be used by TSA is a subset of the consolidated watch list (known as the Terrorist Screening Database (TSDB)) managed by the FBI's Terrorist Screening Center (TSC).

Watch list fidelity and data quality are critical to Secure Flight's success. "Fidelity" speaks to the robustness of entries: Do they contain enough information to resolve identity? "Data quality" refers to the accuracy, completeness and currency of the data. Related questions include: Are entries reviewed periodically for data quality? Has there been an evaluation of the reliability of criteria for designating individuals to the TSC watch list?

There should be a focus across the intelligence community on improving the quality of watch list entries. We appreciate that TSA does not create terrorist watch lists, but rather is a consumer of them. Nonetheless, Secure Flight will be the first time that the TSDB is used regularly to screen a significant portion of the U.S. public, and TSA will receive the brunt of the criticism if the watch list produces a significant number of false positives. Accordingly, TSA should play a lead role in developing and refining watch list standards.

Thus far, it is not clear whether there are adequate rules for watch list entries. While we understand the national security concerns associated with making public certain information about watch lists, we believe that, considering the critical importance of the watch listing process, the process and accountability measures associated with it should be publicly discussed.

Section 4012(c) of the Intelligence Reform Act requires the Director of National Intelligence, in consultation with the Secretary of Homeland Security, the Attorney General and the Secretary of State, to report to Congress in June 2005 on the criteria for placing names on the watch list, the minimum standards for reliability and accuracy of identifying information, the degree of information certainty and the range of threat levels to be associated with an individual on the watch list, and the range of consequences that are to apply to an individual, if located. As far as we know, that report has not been submitted.

It is clearly preferable that watch listing standards be government-wide. In the absence of government-wide standards, TSA has adopted its own internal standards as to what constitutes an "adequate" watch list entry for purposes of Secure Flight. Such standards might include requirements like:

- There should be minimum fidelity standards before a watch list entry can be used. Each watch list entry used by TSA should contain enough identifying information so that the record can meaningfully be used for its intended purpose of identifying an individual. For example, TSA may require multiple data points, such as a first and last name as well as another piece of identifying information, such as date of birth. Name plus nationality or name plus gender is not enough.
- Each watch list entry used by TSA should be reviewed at least once a year by the agency that was responsible for its nomination to the list, to ensure that that the record still meets watch listing criteria and fidelity and data quality standards.
- To promote data quality and redress, each watch list entry should be traceable to a specific transaction (i.e., record) within the source agency, using an internal reference number or some other means of "tethering" the data, so that questions can be resolved and source system records can be reconciled with watch listing system records.

In addition, the use of any watch list for screening purposes depends on reliable match criteria. TSA should establish reliable matching criteria and should periodically reevaluate them.

Finally, as indicated in Section 4012(c) of the Intelligence Reform Act, another aspect of watch listing concerns the seriousness of the threat posed by a watch-listed individual and the different types of consequences that a person may face as a result of being placed on a watch list. An individual on a watch list should face consequences appropriate to the threat that individual is believed to pose. More than 200,000 people are listed in the TSDB – ranging from those known with certainty to be members of a terrorist organization to those suspected of having some tie to terrorism. The current situation is very confusing. Each of the international terrorist names included in the TSC database is assigned one of 25 different codes that describe how a specific individual is associated with international terrorism. Each of the domestic terrorist records is assigned one of three codes, which the DOJ IG concluded do not provide an adequate description. In addition, all entries are marked with one of four levels of "handling instructions," advising users what action to take when they encounter a watch listed person. On top of that, however, TSA draws a two-tiered distinction between "no fly" and "selectee." As a matter of policy, these distinctions and their basis need to be clarified.

III. Collection of Passenger Name Records

The Passenger Name Record (PNR) generated by airlines and reservation systems contains numerous pieces of information beyond the identifying information necessary to make a match for screening purposes, but, on the other hand, may not contain the data needed to make a reliable identification (e.g., the address and phone number on the PNR quite often is that of a travel agency, and date of birth is not included in the PNR). We understand that it would have been quite expensive for airlines to provide only certain PNR fields for the testing phase. Based, however, on the results of the test phase, TSA should determine exactly what data it needs to achieve the aviation security goal of Secure Flight. Then, if feasible, when Secure Flight is implemented permanently, TSA should collect from the airlines and reservations systems only those data elements that are necessary. One of the goals of the test phase should be to explore with the airlines and the reservations systems the feasibility of isolating and delivering to the government only those items of information for which the government has a justified need.

If TSA requires airlines to collect any additional information that they do not currently collect, such as date of birth, TSA should ensure that passengers are given notice about the reasons for the new collection of information. Alerting passengers to the purpose for which their information will be gathered – telling them that it is for security purposes as opposed to, say, marketing uses – should give law-abiding travelers an incentive to provide accurate information when booking air travel, enhancing privacy and effectiveness.

Also, if TSA requires airlines and reservation agents to collect information they do not currently collect, the airlines and other ticketing agents should be prohibited from retaining and using that data for any other purpose. While TSA has promised that it will not be compiling travel dossiers on passengers, neither should the travel industry be able to turn a TSA security order into an opportunity to compile new categories of information on air travelers for the airlines' or travel agents' own use.

TSA has announced that it intends to limit its retention of PNR data, but has not yet set specific retention periods. Once Secure Flight is implemented, TSA should not keep passenger data after a flight has safely completed its flight without incident, except that TSA may retain and disclose to the FBI and other relevant agencies the records of "reds" or no-flies who are not allowed to board and of "yellows" or selectees who are identified based on a watch list match but allowed to board after a more intensive search. Also, TSA should be able to retain data with the consent of any passenger who has invoked the redress process. These retentions and disclosures, which would have a sound predicate in the form of the match to the watch list, should be documented and auditable. Of necessity, given the verification process that should occur for every red and yellow, the TSC would receive (and should be able to retain) a record of the hit.

IV. Use of Commercial Data

Databases held by commercial entities contain a vast amount of data possibly relevant to screening activities, but they also pose challenges in terms of relevance and reliability. TSA and other policymakers, through a process with some transparency and outside input, need to make an assessment of what commercial data would be relevant to passenger screening. In the test phase, TSA has been exploring two potential uses of commercial data: (1) to augment PNR data with additional identifying information: and (2) to verify the identity of passengers. TSA should take a skeptical approach to the use of commercial data in the Secure Flight program, particularly regarding whether the identity scores provided by searching commercial data will significantly enhance TSA's certainty about passengers' identities.

If TSA decides to use commercial data in connection with Secure Flight, it should be on the basis of a finding that the use of commercial data would give additional certainty about the identities of a substantial number of passengers or a more reliable watch list match. Some questions to be considered during testing include:

- What minimum amount of information is required to even test a person for a true identity likelihood score using commercial databases?

- How many people, when providing true identifying information, fail to correlate with commercial databases? For example, what percentage of people flying to, from or within the United States will not have adequate information about them in commercial databases to do identity verification?
- How much reliability does the identity verification process add?
- Will identity verification work with individuals who have privacy concerns and use a different address (e.g., PO Box) than what appears on their driver's licenses, who legitimately have multiple addresses and phone numbers or whose addresses do not match because they use a different billing address for their credit cards?
- What consequences can flow from a poor "identity" score (as opposed to a watch list match)? Will a poor identity score in and of itself suggest a threat to aviation and trigger secondary inspection?

If TSA decides to use commercial data in Secure Flight, then a number of additional privacy protections will need to be implemented. First, TSA should clarify what passenger-provided information will be disclosed to commercial data aggregators. As explained above, passenger PNRs often provide sensitive and/or irrelevant information. TSA should not pass information on to commercial vendors without justification, and it should specify in advance which items of information it will be disclosing to the commercial aggregators.

Second, TSA should, to the maximum extent possible, specify what commercial information its vendors will rely on for the passenger identity verification process. TSA has made clear that neither it nor its commercial vendors will use credit scores, but it has been silent on what information they would rely on. While there are national security concerns at stake, it may be possible to reveal what *commercial* data is being used. One approach to these kinds of issues is to require the commercial data aggregators who are government contractors to make available for free upon request (maybe just once a year) all data they have on an individual for review and correction, the same way they are required to under the Fair Credit Reporting Act. This is in keeping with the commercial data aggregator's interest in having accurate information. Alternatively, the TSA could be required to use aggregators that can guarantee reconciliation accuracy with their data source providers. The transparency into what is used would reveal sources such as public records, credit headers, phone books, driver's licenses, etc. In any case, the consumer should be able to request what information the TSA uses and its source, with instructions on how to remedy inaccuracies (at the source system). In this regard, providing travelers with notice and access to their data may increase the reliability and accuracy of the sources that TSA employs. TSA could include language in its contracts with commercial data vendors that provides for passenger access to and correction of that data directly or through the Passenger Advocate Office that TSA will establish.

Third, TSA should make clear that commercial vendors will, by contract, be prohibited from retaining any airline passenger data other than minimum amounts of data for audit and accountability controls or using it for any purpose other than testing for Secure Flight.

Finally, TSA should develop standards for assessing and verifying the accuracy of the commercial data on which it relies. TSA might base such standards on the answers to the following types of questions: (1) How often are the data updated? (2) How complete is the

information? (3) How accurate is it? (4) How do the data sources protect against and/or mitigate the possibility of identity theft?

V. Redress and Oversight

Redress and oversight are important aspects of any decision making process based on personally identifiable information. As TSA implements Secure Flight, redress will be a major issue.

Major federal privacy laws offer sound models for Secure Flight redress procedures. As reflected in the Privacy Act, the Fair Credit Reporting Act, and other privacy laws, redress typically includes the following elements:

- Notice of the fact of an adverse decision and of the procedure for challenging it;
- Access to the information on which the decision is based;
- An opportunity to correct erroneous information and an obligation by the decision-maker to correct or delete information that is erroneous, which is premised on the ability to trace information to its source for verification;
- Procedures for ensuring that erroneous information does not re-enter the system;
- Obligations on data furnishers to respond to requests for reconsideration of data and to take corrective action when justified; and
- Independent administrative or judicial review and enforcement.

TSA has already committed to developing a "robust review and appeals process" to protect passengers' ability to seek redress where incorrect information or inferences cause them to be subjected to heightened scrutiny. As part of that process, TSA has indicated that it will create a Passenger Advocate Office, which will act on behalf of passengers and investigate complaints. The proposed Passenger Advocate is a desirable component of a passenger redress process, but TSA will need to flesh out the procedures that will govern the Passenger Advocate's review of passengers' complaints. It will be critical to the success of any new program that individuals have a meaningful process for challenging their "yellow" or "red" designations.

As noted above, we believe that TSA should not keep data on cleared passengers after a flight is successfully completed. For the relatively small number of passengers who may complain due to being selected for whatever reason, TSA should be able to preserve data if a passenger makes a complaint at the airport at the time of screening.

The Intelligence Reform Act requires TSA to establish a timely and fair process for individuals identified as a threat to appeal to TSA that determination and to correct any erroneous information. The process must include the establishment of a method by which TSA will be able to maintain a record of air passengers and other individuals who have been misidentified and have corrected erroneous information. To prevent repeated delays of misidentified passengers and other individuals, the TSA record shall contain information to authenticate the identity of such a passenger or individual.

Particularly in the context of individuals who appear to be a risk because of a watch list match, TSA must work closely with TSC to ensure that people are not mistakenly flagged on a repeat basis. As we already have seen, there will be innocent individuals with the same or similar names as people on the watch list. Such mistakes must be investigated and rectified quickly so that the affected individuals are not repeatedly flagged and delayed. This will require TSA to work closely with TSC and various intelligence agencies.

Passengers should have the ability to challenge the Passenger Advocate's decisions. First, passengers should be able to mount an administrative appeal within TSA or the Department of Homeland Security, perhaps to the Privacy Officer. Second, given that the right to travel is at stake, judicial review should also be available once administrative appeals are exhausted. In some cases, judicial review might require special *ex parte* procedures to deal with classified information, but such procedures have been successfully implemented in other contexts. *See, e.g.,* Classified Information Procedures Act, Public Law 96-456.

In addition to redress, TSA should implement other oversight mechanisms. Auditing should be an important part of the Secure Flight system. The DHS Inspector General, the Privacy Officer, and the Civil Rights and Civil Liberties Officer should jointly conduct an annual audit of the system's operations. Of necessity, the auditors should have security clearances enabling them to access all relevant information, including classified data. The auditors could conduct spot checks of actual screenings and retain some passenger records for the duration of the audit process as well as examine the aggregators' datasets. To the extent an audit report relies on classified information, portions of the report may need to remain classified, but much of the audit reports could be made public.

TSA also should implement a real-time auditing function to monitor who accesses the system. TSA and TSC both must implement a documented information security program (to protect the data) and data governance models (to control access to the data and ensure access and modification are auditable). Such audit trials are crucial to prevent abuse and internal security breaches, ensuring that only authorized personnel are accessing the system and that they are using it only for authorized purposes.

Other forms of independent oversight of Secure Flight are also essential to an effective privacy protection scheme. TSA should report annually and publicly to Congress, including (1) an explanation of the Secure Flight privacy policies; (2) a description of how those policies have been implemented; (3) a list of the types of passenger complaints that have been filed, with descriptions of how they have been resolved; (4) changes that TSA is making to minimize any identified problems; and (5) the ratio of hits, no hits, and disposition results to allow evaluation of the false positive counts. Other oversight mechanisms that TSA should consider are independent evaluations of the program by outside auditors and periodic consultations with privacy advocates.

VI. Scope

Over the course of the evolution of CAPPS II and Secure Flight, there has been uncertainty about the mission that a passenger screening system should serve. In the spring of

2003, then-TSA Administrator Admiral James Loy assured Congress and the public that CAPPS II would be used only to identify foreign terrorists and prevent them from boarding airplanes, because foreign terrorists were the source of the threat to aviation security. Subsequently, TSA proposed broadening CAPPS II's purposes to include identification of domestic terrorists and those associated with domestic terrorist organizations as well as certain criminals and possibly immigration law violators.

In the September 2004 Notices and in the June 2005 Notice, TSA refocused on the threat of terrorism. The task of creating an effective system to screen passengers against terrorist watch lists is so urgent and so challenging that it is preferable at this point for TSA not to pursue the additional and separate task of identifying other criminals not believed to pose a threat to aviation.

Like CAPPS II, the proposal for Secure Flight includes not only foreign terrorists, but also members of domestic terrorist groups – i.e., members of radical organizations like the KKK, anti-government militias, or certain radical environmental activists. It might be sensible to include domestic terrorists in Secure Flight if there is evidence that particular individuals or discrete groups pose a threat to civil aviation. In the absence of intelligence suggesting that particular individuals or groups are a threat, the expansion of Secure Flight into the realm of domestic terrorism raises a host of difficult issues that TSA appears not to have confronted. It could ultimately place TSA in the role of having to evaluate the political activities of Americans. The FBI's definition of who is a domestic terrorist has often been quite broad. In the absence of a specific threat, does the term "domestic terrorist" include all members of a environmental group, when a few of those members that have engaged in illegal acts and have been investigated by the FBI as domestic terrorist organizations? Does it include an anti-abortion activist who breaks the law by blocking access to abortion clinics or who may be organizationally or ideologically related to those who have killed doctors or committed arson at clinics, which some have called terrorism? Does it include protesters against the war in Iraq, whom the FBI interviewed in advance of the Republican National Convention?

Furthermore, each added function puts further pressure on the system: more false positives, diversion of screener resources, loss of screener confidence in system results, and the risk of public disapproval. Accordingly, TSA should limit screening of passengers for associations with purely domestic terrorist organizations to those situations, if and when they arise, when information indicates that specific individuals or discrete groups pose a threat to civil aviation.

VII. Privacy Act

The Privacy Act offers a sound framework for a number of issues posed by Secure Flight. In the September 2004 Notices, TSA proposed exempting the Secure Flight test data from various Privacy Act provisions. Moreover, TSA had indicated that it would invoke blanket exemptions for full implementation of CAPPS II.

In the Notice issued last week, TSA announced that it would not pursue its Privacy Act exemptions. We commend this decision, and we urge that it be followed in the implementation

of Secure Flight as well. TSA has always said that it plans to provide access to certain unclassified records such as PNR and the ability to correct them, as an important element of the integrity of the system. There seems to be, on the current record, no valid reason to take a exemption from the Privacy Act provisions on access and right to correct. If there are specific concerns that TSA has about application of the Privacy Act to Secure Flight in the implementation phase, it should identify them so they can be addressed based on a public dialogue.

Conclusion

We firmly believe that a passenger screening system can be designed that that both enhances security and protects civil liberties. Developing sound privacy rules and sticking to them is crucial to the success of such a program. To facilitate public trust in the system that is eventually implemented, we encourage TSA to make public as much as possible about the results of Secure Flight testing and TSA's decisionmaking process. We look forward to working with TSA and the Congress.

For further information:

James X. Dempsey
Center for Democracy & Technology
1634 I Street N.W.
11th Floor
Washington, DC 20006
(202) 637-9800 x 112
http://www.cdt.org