Prepared Testimony and Statement for the Record of

Marc Rotenberg,
President, Electronic Privacy Information Center (EPIC)

Hearing on

"The Future of Registered Traveler"

Before the Subcommittee on Economic Security,
Infrastructure Protection, and Cybersecurity,
Committee on Homeland Security,
U.S. House of Representatives

November 3, 2005
311 Cannon House Office Building
Washington, DC

Mr. Chairman, Members of the Committee, thank you for the opportunity to appear before you today. My name is Marc Rotenberg and I am Executive Director and President of the Electronic Privacy Information Center in Washington, DC. EPIC is a non-partisan public interest research organization established in 1994 to focus public attention on emerging civil liberties issues. We are very pleased that the Committee is examining the privacy implications of the Registered Traveler program. I ask that my complete statement, EPIC's recent report on Registered Traveler, and our one-page summary of the ongoing problems with watch list errors be entered into the hearing record.[1]

In my statement today, I wish to call attention to three particular problems with the Registered Traveler program. First, the security watch lists on which the system is based are filled with inaccurate data. Documents obtained by EPIC under the Freedom of Information Act reveal that travelers continue to struggle with watch list errors.[2]

A second flaw in the program exacerbates this problem — the databases in the system are currently not subject to the full safeguards of the Privacy Act of 1974, as the TSA has sought wide-ranging exemptions for the record system and private companies are not generally subject to the Privacy Act. As a result, the legal safeguards that help ensure accuracy and accountability are simply missing from this system.

Third, the Registered Traveler program, if operated in the private sector, will become a textbook example of "mission creep"—the databases of personal information will be used for purposes other than aviation security.[3] We already know that the Computer Assisted Passenger Prescreening System 2 ("CAPPS 2"), the precursor to Registered Traveler, was to be used for purposes unrelated to terrorist screening. Because of this, Congress rightly chose to end the program.[4] This danger is even more "clear" with the Registered Traveler program, now under consideration by the Committee.

---

[1] EPIC, *Spotlight on Surveillance: Registered Traveler: A Privatized Passenger ID* (October 2005), available at http://www.epic.org/privacy/surveillance/spotlight/1005/default.html

[2] EPIC FOIA Notes, "Travelers Continue to Struggle with Watch list Errors," No. 8 (Sept. 27, 2005) available at http://www.epic.org/foia_notes/note8.html

[3] Systems designed to protect the country from terrorist acts are increasingly being used for many other purposes. Barry Newman, "New Dragnet: How Tools of War on Terror Ensnare Wanted Citizens: Border Immigration Officials Tap Into FBI Databases; Questions About Privacy," Wall Street J., Oct. 31, 2005, at A1.

[4] Matthew Wald & John Schwartz, "Screening Plans Went Beyond Terrorism: Air security program sank after it grew to include other needs," N.Y. Times, Sept. 19, 2004, at A25.

Last month, the federal government ended the test program for Registered Traveler.[5] Before the program goes forward, at least these three issues should be addressed.

TSA's Watch List Errors

The Registered Traveler system is based on the TSA's existing system of passenger screening lists. These same lists have been a constant source of errors and inaccuracies that inappropriately detain travelers, subject them to unnecessary searches, and sometimes prevent them from flying.

Senators Ted Kennedy and Don Young, for instance, have both been improperly placed on security watch lists. In hearings before this Subcommittee in March, Ranking Member Sanchez noted that many of her constituents had experienced unwarranted delays, questioning, and sometimes even the inability to fly, due to their names being mistakenly placed on screening lists.

Hundreds of other passengers have experienced the same or similar problems. Documents received by EPIC through the Freedom of Information Act revealed that, in the period from November 2003 to May 2004, over a hundred individuals complained of being placed on the lists in error.

Nor is removal from the watchlists a simple matter. Senator Kennedy was only able to correct this error after appealing directly to then-Homeland Security Secretary Tom Ridge. The vast majority of people affected by watchlist errors, needless to say, do not have this option. Instead, they face an opaque and arbitrary bureaucratic process, where they are never told the reasons for their being placed on the lists, and therefore have little idea how to correct false information about themselves or distinguish themselves from a suspect with a similar name.[6]

The provisions surrounding Registered Traveler databases are no better. Although Verified ID claims that "members" of the program will be provided with the identification information in the private database, the most pertinent information will not be revealed to those people who provide information to the Registered Traveler system.[7]

For instance, if an applicant is denied membership, or if a member's status on the watch lists changes, the individual is never told why he has been deemed a potential security risk. Furthermore, applicants who have supplied sensitive personal information

---

[5] Sara Kehaulani Goo, "Registered Traveler Test is Ending Inconclusively: Airport Security Scheme Lacks Broad Support," Wash. Post, Sept. 27 at A15.

[6] The issue of redress procedures was considered in a 2004 report on Registered Traveler, but never resolved. Transportation Security Administration, *Registered Traveler Pilot: Privacy Impact Assessment* 6 (June 24, 2004).

[7] Clear Registered Traveler at http://flyclear.com/

to the program are not assured of access to the information that the system has on them, and therefore have no way of ensuring either the accuracy or the security of their data.

Lack of Privacy Act Safeguards

These problems are all the more serious because the Registered Traveler system is not subject to most of the critical privacy safeguards required by the Privacy Act of 1974. Congress passed the Privacy Act in response to concerns that the rapid growth of government databases could have negative effects on the personal privacy and civil rights of citizens. After intensive study, extensive hearings, and careful consideration, Congress adopted the Privacy, Act, which requires government agencies to limit the collection, sharing, and use of individuals' personal information. The Act also requires that agencies give individuals the right to access, and correct, information that the government collects about them.

For all practical purposes, the Registered Traveler Program withholds these rights from individuals. In this case, we have two separate databases, each of which sidesteps Privacy Act responsibilities.

In the case of a private partner, the data collected from passengers is stored in a separate, private database. As a private entity, the partner is not covered by any of the requirements of the Privacy Act. When TSA says that its contractors must abide by the Privacy Act, this is only with regard to the information flowing from the TSA to the contractor, not for this separate, private database of personal information collected and kept by the private company. Thus, the only guarantee of privacy that passengers have comes from the company's own broad assurances.

In removing Privacy Act safeguards from the private-sector database, applicants are not only denied the ability to access and correct records, they also are subject to the sharing of their personal information. The data collected from applicants includes some of the most sensitive information that one can collect about a person: Social Security numbers, fingerprint and iris scans, photographic reproductions of drivers licenses, passports, and birth certificates. This information requires limits on its use and sharing mandated by law. Registered Traveler evades this responsibility by having passengers initially submit data to private partners.

The privacy policy of Verified ID states that data is shared only with the TSA, and no other agencies. Yet a look at the Privacy Act notice by the TSA quickly reveals that TSA is prepared to share passengers' personal information with a wide array of other agencies, whether federal, state, local, international, or foreign. The standards for this sharing are alarmingly low—the TSA must be aware only of an *indication* of a *potential* violation of civil or criminal laws or *regulations*.

The TSA's own database, which does fall under the scope of the Privacy Act, does little more than give a cursory nod to its requirements. TSA has exempted itself

from the Privacy Act's requirements for accounting for disclosures, access to records, and even the requirement that the information in the database be *necessary* and *relevant*.

By exempting Registered Traveler from the access to records requirements, TSA prevents users from requesting any information that the TSA may be keeping on them. As I have already noted, this access requirement is crucial in any system that is to respect the rights of individuals. Without meaningful access to the files kept on them, individuals have no recourse if inaccurate, incomplete, or fraudulent information about them is kept in the system. A person with a faulty file will not only lack the opportunity to correct it, she will never learn that it is faulty in the first place, and be unable to clear her name.

It is significant that the Department of Homeland Security Data Privacy and Integrity Advisory Committee recently prepared a report on the use of commercial data for passenger screening and recommended strict limitations on the use of commercial data for passenger screening.[8] As the Committee noted, "False positives can create adverse consequences for misidentified individuals, ranging from missing a flight to being denied a security clearance or a job."[9]

There is also ample precedent for imposing privacy obligations on the private sector. Consider determinations that are made by banks and other financial institutions about a consumer who seeks a home loan. If a loan application is denied, the consumer is entitled to know the basis for the decision. The reason, not surprisingly, is that mistakes are made, names are confused, incorrect data is used, information is transposed, unsubstantiated allegations are left unchallenged.

A watch list system is necessarily open to such abuse and any benefits that might result must be weighed against the very real harms to innocent individuals. A privatized watch list system opens the door to the routine stigmatization of a large percentage of the American public with no effective means of redress.

"Mission Creep"

The breadth and scope of the information to be kept in the Registered Traveler data base leads to another significant concern—that this program will begin to accumulate other uses for which it was not originally approved or intended. Such "mission creep" leads to further privacy risks.

Mr. Brill has suggested that his identification component of the program be used not only in airports, but also as a means to control access to sports arenas, power plants, and even office buildings. Just this week Mr. Brill announced that his company had

---

[8] Report of the Department of Homeland Security Data Privacy and Integrity Advisory Committee, *The Use of Commercial Data to Reduce False Positives in Screening Programs* (Sept. 28, 2005).

[9] *Id*. at 2.

entered into agreements with Hertz, the rental car industry leader, and Cendent, an Internet management travel company.[10]

Should those who rent cars or book air travel on the Internet be concerned that if they do not first get Mr. Brill's gold star, they may soon face higher prices for travel or additional questions from the rental company? And what about people who travel infrequently, or whose personal information may be more difficult to verify? Database errors also tend to fall disproportionately on minority communities and those whose names are easily misspelled or mispronounced.

The TSA has indicated that it will combine Registered Traveler with at least six other databases under the office of Screening Coordination and Operations. The agency has not specified how it intends to protect privacy rights in this amalgam of databases. If a person provides personal information to an agency for a specific purpose, he generally expects the agency to limit its use of the information to that purpose.

The risks of mission creep are not theoretical. The TSA has itself suffered from this problem, as indicated by its misuse of passenger data in the CAPPS II program. TSA documents obtained by EPIC under the Freedom of information Act clearly showed that TSA has considered using information gathered for the CAPPS II program for reasons beyond its original purposes. For example, TSA stated that CAPPS II personal data might be disclosed to federal, state, local foreign, or international agencies for their investigations of statute, rule, regulation, or order violations. Congress rightly put an end to that program.[11]

But at least that program was limited to law enforcement conduct. There appear to be no "clear" limits to Registered Traveler.

Recommendations

The privacy of individuals in the United States is a fundamental right that should not be sacrificed for mere convenience. In protecting these rights, I urge you to consider the following:

1. The TSA watch lists have widespread problems, flagging as security risks a minimum of hundreds of passengers who pose no threat. A system based around these watch lists and integrated with other systems of records will only exacerbate the problems that have been well documented.

---

[10] Verified Identity Pass, Inc., "Press Release," (Nov. 1, 2005) available at http://www.verifiedidpass.com/news_pr_110105.html

[11] Former Secretary of Homeland Security Tom Ridge acknowledged that the CAPPS 2 program was "dead" in mid-2004. Ryan Singel, "Passenger Screening System Dead," Wired (July 15, 2004), available at http://www.wired.com/news/privacy/0,1848,64227,00.html.

2. The Privacy Act creates critical and necessary safeguards not simply to protect privacy, but also to ensure accuracy and accountability. Any government-approved security system that keeps personal information on individuals should meet the Privacy Act requirements for necessity, relevance, and openness, including individual access and correction. It should be made clear that these requirements apply whether the information originates with the agency or with information provided by the individual. It should also not be subject to broad exceptions like those the TSA has set forth in its notices.

3. There are real risks in a database accumulating unintended uses with unforeseen consequences. The end result is often an unwieldy tool that performs poorly, operates inefficiently, and violates privacy. I urge you to mandate any system designed for aviation security be restricted to that purpose, and not become a system for tracking individuals or controlling their ability to travel in going about their daily business.

Congress was wise to discontinue the Registered Traveler program last month. The program should not go forward until these problems are resolved.

Thank you for the opportunity to appear here today. I will be pleased to answer your questions.