epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Prepared Testimony and Statement for the Record of

Lillie Coney,
Associate Director, Electronic Privacy Information Center (EPIC)

Hearing on

"Ensuring America's Security: Cleaning Up the Nation's Watchlists"

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

September 9, 2008
311 Canon House Office Building
Washington, DC

Chairwoman Sheila Jackson Lee and Ranking Member Daniel E. Lungren, thank you for the opportunity to appear before you today. My name is Lillie Coney and I am Associate Director 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 holding this hearing on "Ensuring America's Security: Cleaning Up the Nation's Watchlists." The watchlist program is dysfunctional because it is a black box system. Information goes into the process, but not very much escapes, including when errors are made. Poor list creation and management not only cost taxpayers money, they may also deny individuals a fundamental constitutional right to travel.[1] I ask that my complete statement and our summary of the ongoing problems with watchlist errors be entered into the hearing record.

In my statement today, I wish to call your attention to three primary problems with the security watchlists. First, the databases in the system are not subject to the full safeguards of the Privacy Act of 1974[2], as the Transportation Security Administration (TSA) has sought wide-ranging exemptions for the record system and private companies engaged by the agency are not subject to the Privacy Act.[3] As a result, legal safeguards that help ensure accuracy and accountability in other databases are absent from the watchlist system.

The second flaw of the program aggravates the issue further – the security watchlists on which the system is based are riddled with inaccurate and obsolete data.[4] In September 2005, documents obtained by EPIC under the Freedom of Information Act revealed travelers' struggles with watchlist errors.[5] The situation has not changed materially and recent news continues to reveal more incidents of false positives and harrowing experiences of legitimate travelers.[6]

Third, the existence of the Registered Traveler program may become a textbook example of "Security Theater."[7] Further, the approach is triggering typical hallmarks of

---

[1] *Saenz v. Roe*, 526 U.S. 489 (1999)
[2] 28 CFR § 16.96(r)(1)
[3] Privacy Act Amendments 2005, EPIC, *available at* http://epic.org/privacy/laws/privacy_act.html
[4] Watchlist FOIA Documents, *available at* http://epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html/
[5] EPIC FOIA Notes #8, *available at* http://epic.org/foia_notes/note8.html/; and also see report "Audit of the US Department of Justice Terrorist Watchlist Nomination Process," Department of Justice Office of the Inspector General Audit Division, Audit Report 08-16, March 2008
[6] Drew Griffin and Kathleen Johnston, "Airline captain, lawyer, child on terror 'watchlist'", CNN, Aug. 19, 2008 *available at* http://www.cnn.com/2008/US/08/19/tsa.watch.list/. *See also* "Formal calls for probe into reporter's name on no-fly list", CNN, July 17, 2008 *available at* http://www.cnn.com/2008/US/07/17/watchlist.chertoff/index.html
[7] Bruce Schneier, "The Feeling and Reality of Security", Apr. 8, 2008 *at* http://www.schneier.com/blog/archives/2008/04/the_feeling_and_1.html (describing security

"mission creep" – the databases of personal information collected by private sector companies will be used for purposes other than originally intended – aviation security. The TSA has outsourced the vetting of bona fide air-travelers to Verified Identity Pass, Inc. (Verified ID), a privately held company running The Clear® Registered Traveler program (Clear).

For a year, San Francisco air travelers have been offered the option of enrollment in the Clear Registered Traveler Program at a cost of $128. Those who registered were given a biometric ID card that could be used to bypass regular security lines. In August of this year, Verified ID reported the theft of a laptop containing registration information from its San Francisco office. The agency for a short time prohibited Verified ID from registering new customers into the Registered Traveler program. Registered traveler schemes are all vulnerable to several serious flaws, including the example presented in this news item. Travelers who registered for the program may find themselves waiting in lines once again. Later, it was reported that the laptop was returned to the office it was stolen from.[8]

In order to ensure America's air travel security, the watchlist must not only be cleaned up of errors, the government must also ensure that inaccurate data is not entered into the database in the first place. Further, it must be transparent to the general public by: providing information on the existence of the watchlists; disclosing the penalties for being listed; publicizing the redress procedures; ensuring effective due process rights for travelers, and cleaning up the appeals process for agency decisions. Finally, each traveler denied the right to travel should have access to the courts.

The Privacy Act 1974

The protection of privacy is hardly a new problem. An 1890 journal article written by American lawyers Samuel Warren and Louis Brandies entitled the "Right to Privacy," captured the attention of law scholars, legislators, and the public. This law journal article has been cited and debated for over a century, and has guided the establishment of laws and international norms that restrain the power of technology and human curiosity to encroach on an individual's "right to be let alone."[9]

In 1948, the right of privacy found a place in international law through its adoption into the Universal Declaration of Human Rights.[10] Article 12 states:

---

countermeasures intended to provide the feeling of improved security while doing little or nothing to actually improve security)

[8] "Laptop with traveler info likely stolen, returned," Marcus Wholsen, Business Week, August 2008, *available at* http://www.businessweek.com/ap/financialnews/D92GO1A00.htm

[9] Samuel Warren & Louis Brandies, The Right to Privacy, 4 Harvard Law Review 193 (1890).

[10] Universal Declaration of Human Rights, adopted and proclaimed by General Assembly resolution 217 A(III) on December 10, 1948, *available at* http://www.un.org/Overview/rights.html .

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

The "Digital Information Age," ushered in a much-needed expansion of the fundamental human right of privacy. During the 1960s and 1970s, interest in the protection of privacy rights increased with the arrival of the information technology revolution. Congress in its wisdom acted not in the wake of disaster, but prospectively to address the real threats posed by powerful computer systems. The Federal Privacy Act established the right of citizens to be free from government abuse and misuse of personal information, and the right to be informed of the actions taken by the federal government on their behalf.

The Privacy Act of 1974 was passed in response to concerns about how the creation and use of computerized databases might impact individuals' privacy rights. However, its scope was limited to federal government agencies. It safeguards privacy of federal government-held records through the creation of four procedural and substantive rights in personal data. First, the Privacy Act requires government agencies to show an individual any records kept on him or her. Second, it requires agencies to follow certain principles, called "fair information practices," when gathering and handling personal data.[11] Third, it places restrictions on how agencies can share an individual's data with other people and agencies. Fourth and finally, it allows individuals to sue the government for violating the provisions of the Act.

There are, however, several exceptions to the Privacy Act. For example, government agencies that are engaged in law enforcement can excuse themselves from the Act's rules. Agencies have also circumvented information sharing rules by exploiting a "routine use" exemption. In addition, the Act applies only to certain federal government agencies (except for Section 7's limits on the Social Security Number (SSN) that applies to federal, state, and local governments). Aside from Section 7, the Privacy Act does not cover state and local governments, though individual states may have their own laws regarding record keeping on individuals.

In August 2007, The Department of Homeland Security published in the Federal Register its "Privacy Act of 1974; Implementation of Exemptions; Security Flight Records.[12] The Federal Register notice states that the agency is claiming the exemption of agency conduct under the Privacy Act, which include the statute's core privacy protections. DHS is exempting itself from Privacy Act requirements that its records on individuals are accurate; that the data collection is limited to only information that is relevant, and that US citizens be afforded due process rights to appeal agency decisions.

---

[11] Fair Information Practices, EPIC, http://epic.org/privacy/consumer/code_fair_info.html

[12] Federal Register, Department of Homeland Security, TSA 49 CFR Part 1507, Privacy Act of 1974: Implementation of Exemptions; Secure Flight Records, pg. 48397-48400, August 23, 2007, *available at* http://edocket.access.gpo.gov/2007/E7-15963.htm

The agency message on privacy for those visiting the TRIP web site is published on a page titled "Step 2: How to Use DHS TRIP." The information provided under the sub-heading DHS TRIP and Your Privacy does not disclose that the agency is claiming a wide range of exemptions from the Privacy Act. It states:[13]

> The Department of Homeland Security safeguards the privacy of any personal information that you provide in your inquiry to DHS TRIP. This information will be protected and will only be shared in accordance with the provisions of the Privacy Act of 1974 (5 U.S.C. § 552a) and as provided in the Privacy Impact Assessment published for DHS TRIP.

There is a fundamental failure to adhere to the Privacy Act in the current system used by the DHS's online Traveler Redress Inquiry Program (TRIP). TRIP is a one stop voluntary program to provide a means for individuals to request redress who believe they have been (1) denied or delayed boarding transportation due to DHS screening programs, (2) denied or delayed entry into or departure from the United States at a port of entry, or (3) identified for additional (secondary) screening at our Nation's transportation facilities, including airports and seaports.[14]

First, the Privacy Act requires that data collection be limited to only what is "relevant and necessary." However, the TRIP program does not perform a critical process to determine if the collection of information is necessary.[15] Second, the data collected should be specific to the kind of problem the traveler may have experienced. Third, the information collected must only be used to resolve the problem. Once the travel issue is identified, and if necessary investigated data not needed should be discarded from the system. TRIP does not distinguish between frequent travelers and infrequent travelers. All air travel experiences are not equal—some like members of Congress may travel on average 30-40 weeks out of the year. Very infrequent air travelers may travel once over several years.

Prior to collecting personally identifiable information from travelers DHS's TRIP process should first separate the subjective from objective travel experience of the respondent Second, there are several points in airport traveler processing that passengers may experience problems: the ticket counter or ticket kiosk, the security screening to enter gate areas, and the boarding process to enter a airplane. A series of questions could help navigate inquires to relevant information such as why repeated request to re-enter a magnetometer might happen, why fluid containers above a certain size will prompt secondary screening, why laptops left in carryon luggage will promote a secondary screening process.

---

[13] Department of Homeland Security, How to Use DHS TRIP, Section: DHS TRIP and Your Privacy, *available at* http://www.dhs.gov/xtrvlsec/programs/gc_1169826536380.shtm

[14] Transportation Security Administration, Department of Homeland Security, DHS Traveler Redress Inquiry Program (DHS TRIP), Contact: James Kennedy, January 18, 2007

[15] Lillie Coney, This Testimony, Attachment A, House Committee on Homeland Security, Subcommittee on Transportation, Security, and Infrastructure Protection, September 9, 2008, also see: http://www.dhs.gov/xtrvlsec/programs/gc_1169673653081.shtm

There is no link on the DHS homepage to the One-Stop Travelers' Redress web page. Further the online process does **not** include an automated routing method to guide the respondent through the process. The program page has three options "Should I Use DHS TRIP," "How to use DHS TRIP" and "After your inquiry."[16] The actual online application starts with a series of questions that include "Do you feel you were discriminated against; Do you believe that the US Government's record of your personal information is inaccurate; You were unfairly detained; You could not print a boarding pass; You were delayed or detained; You were told: your fingerprints were incorrect, your photo did not match, your information was incomplete or inaccurate, you are on a no fly list; You want to amend a travel record or Ensure your biometric record created by US-VISIT is removed.[17]

The series of questions conflates the US-VISIT process with the typical US citizen's experience with domestic air travel. The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) is an integrated government-wide program intended to improve the nation's capability to collect information about foreign nationals who travel to the United States, as well as control the pre-entry, entry, status, and exit of these travelers. The US-VISIT system of data collection does not include US citizens. If DHS has access to biometric data on US citizens, or dossiers then that should be disclosed to Congress and to the traveling public. In any case, there should be two distinct systems one for US citizens and one for non-citizens.[18] Each system should appropriately eliminate air travelers who are not subject to a watchlist error or mismatch issue. Then—and only then, should the agency seek to collect personally identifiable information from respondents. The TSA's Federal Register notice, of August 23, 2007, regarding exemptions, sought to disregard the data collection limitations provided for by the Privacy Act. For this reason, we caution that the agency should be required to follow all Privacy Act provisions as it relates to the management of the watchlist program and especially with regard to the collection of information from air travelers.

DHS Must Increase Watchlist Transparency

One of the principle protections offered by the Privacy Act and fair information practices is transparency. Transparency is a key component of a functioning healthy democracy. It can be translated into public policy decisions that allow citizens, policymakers, and the media to assure themselves that a local, state or federal government agency is functioning as intended. [19]

---

[16] Department of Homeland Security, One-Stop Travelers' Redress, available at http://www.dhs.gov/xtrvlsec/programs/gc_1169673653081.shtm

[17] Department of Homeland Security, Traveler Inquiry Form, available at http://www.dhs.gov/xlibrary/assets/DHSTRIP_Traveler_Inquiry_Form.pdf

[18] Department of Homeland Security, One-Stop Travelers' Redress, available at http://www.dhs.gov/xtrvlsec/programs/gc_1169673653081.shtm

[19] EPIC, Litigation Under the Federal Open Government Laws (FOIA) 2006, web page, available at http://www.epic.org/bookstore/foia2006/ .

Efforts to provide due process by DHS must remove ambiguity that may currently exist in the minds of agency administrators regarding their obligations to make public information related to watchlists and prohibitions on travel. EPIC filed a court challenge to an attempt by the Transportation Security Administration to withhold a Privacy Impact Assessment from the public, which was in violation of federal law.[20] EPIC requested the Privacy Impact Assessments from the TSA under the Freedom of Information Act, and received heavily redacted documents from the agency in its reply.[21] EPIC sued the agency for full disclosure of the documents as required by the E-Government Act. The TSA argued that the Federal Privacy Act and the E-Government Act, which requires publication of Privacy Impact Assessments, were segregated.

Watchlist Errors

The watchlists are comprised of entries derived from multiple sources.[22] However, as the process of compiling the lists is unknown, methods of quality control at this stage are unclear and unknown. What have learned through reports from the Department of Justice's Inspector General is troubling. For example, watchlist "nominations" from FBI field offices were "often incomplete or contained inaccuracies."[23] Further, there is confusion among recipients of FBI terrorist-related intelligence reports, who thought that the information received was official watchlist nominations--when they were not.[24] Senators Ted Kennedy and Don Young, for instance, have both been improperly placed on the lists in error. Catherine Stevens, wife of Alaska Sen. Ted Stevens have also faced difficulties.

The Inspector General of the US Dept. of Justice found that the Terrorist Screening Center ("TSC") is relying on two interconnected versions of the watchlist database. As a result, not only were names missing from the frontline personnels' computers, but also the numbers of duplicate records have significantly increased since the last review.[25] Further, the TSC had not taken adequate steps to ensure that the content of the two databases was identical. In brief, the Inspector General found that the methodology adopted by the FBI to nominate new names was flawed.[26] The Inspector General concluded that this procedure resulted in the TSC being "unable to ensure that consistent, accurate, and complete terrorist information is disseminated to frontline screening agents in a timely manner. Moreover, the TSC determined that the Terrorist Screening Database contained over 2,000 watchlist records that did not belong in the

[20] EPIC v. US Transportation Security Administration, Civil Action No. 03-1846 (CKK), available at http://www.epic.org/privacy/airtravel/pia_order.pdf , August 2, 2004.
[21] EPIC, Alert e-Newsletter, Volume 11.18, available at http://legalminds.lp.findlaw.com/list/epic-news/msg00164.html , September 24, 2004 .
[22] "Follow-up Audit of the Terrorist Screening Center" Audit Report 07-41, Sept. 2007, US Dept. of Justice, Office of the Inspector General, Audit Division *available at* http://www.usdoj.gov/oig/reports/FBI/a0741/final.pdf
[23] *Id*
[24] *Id*
[25] *Id.*
[26] *Id* at page 12.

database"[27] in the first place and included some records that were inappropriately maintained without any watchlist designation.[28] The Inspector General's report details deterioration in the quality of the database arising from and perpetuated by the fact that the database grew from 150,000 in April 2004 to 724,442 in April 2007. With such a high rate of increase, and poor algorithms, the record-by-record review could not be completed within the timeframe.[29]

Even with such official reports, the database continues to be plagued with problems. The United States Government Accountability Office also concluded that "lacking clearly articulable principles, milestones, and outcome measures, the federal government is not easily able to provide accountability and have a basis for monitoring to ensure (1) the intended goals for, and expected results of, terrorist screening are being achieved and (2) use of the list is consistent with privacy and civil liberties."[30] In recent glaring examples, a lawyer, an airline captain and a child were found to be on the terror watchlist.[31] In another case, an investigative reporter for CNN found his name on the TSA watchlist after he completed his investigation of the TSA.[32]

There must be a clear statutory definition of the words "terrorism," and "terrorist," as well as the phrase "terrorist organization."[33] Without clear definitions, these designations could be misused, such as in the past when the word "subversive" was used to justify actions taken against some civil rights activists, civil liberty groups and others who were engaged in lawful pursuits. Currently, each agency uses its own definitions for these terms, which means a moving bar exists for inclusion of names on watchlists.

It is therefore respectfully urged that methods of nomination of names into the database be scrutinized, people be given further information about the processes involved instead of filling out lengthy questionnaires providing personal information, and additional steps be taken to ensure the information in the database is accurate, timely and amenable to correction.

Recommendations

- DHS should employ the expertise of a human factors expert to revamp the TRIIP query process to help eliminate the data collection process to only those affected by watchlist issues.
- The agency should be prohibited from exempting itself from Privacy Act enforcement obligations.

---

[27] *Id.*
[28] *Id.* at page 13.
[29] *Id*. at page 41.
[30] United States Government Accountability Office, "TERRORIST WATCHLIST SCREENING: Opportunities Exist to Enhance Management Oversight, Reduce Vulnerabilities in Agency Screening Processes, and Expand Use of the List", Oct. 2007, *available* http://www.gao.gov/new.items/d08110.pdf
[31] *See supra* note 5
[32] "Formal calls for probe into reporter's name on no-fly list", CNN, July 17, 2008 *available at* http://www.cnn.com/2008/US/07/17/watchlist.chertoff/index.html
[33] "GAO, Terrorist Watchlist Screening, GAO-08110, October 2007

- The process for Citizens and non-citizens should be clear and governed by a series of questions. The information presented should make it clear if it is intended for a citizen or non-citizen. The information collected should only apply to that category.
- Respondents should be told their rights and protections afforded to them.
- Over collection of data should be prohibited.
- Agency personnel, airlines, and contractors should be held accountable by Privacy Act civil and criminal penalties or held to contract obligations with the equivalent effect.

Conclusion

It is necessary to first analyze at what points travelers are stopped by the watchlist. The first point of interaction is at the check-in or obtaining of a boarding pass. If the passenger is on the so-called "Selectee" list, she will be subjected to additional screening. However, the collection of a ticket or boarding pass may be disassociated with the actual screening process. The next point where her identification is checked is at the entry to the security screening area. Boarding passes are taken or checked at the gate prior to boarding. When a traveler experiences difficulty in the airport screening, baggage check-in, security screening, or during the flight boarding process, it is important to differentiate between something they are asked to do that is different from other passengers. Further, it is vital that all other possible explanations for the different treatment be eliminated before asking the respondent for personally identifiable information.

It is our hope that the work set forth by this committee will lead to a more just, fair, privacy centric, and transparent watch list program.

Thank you,

Lillie Coney
Associate Director
EPIC
1718 Connect Avenue, NW
Washington, DC 20009
coney@epic.org