DEPARTMENT OF HOMELAND SECURITY

Docket No. DHS 2006-0077
Privacy Act; Redress and Response System of Records
and
Docket Number DHS-2007-0003
Privacy Act of 1974: Implementation of Exemptions; Redress and Response Records System

---

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

By notice published on January 18, 2007, the Department of Homeland Security ("DHS") announced it seeks to create the DHS Redress and Response Records System, which "maintains records for the DHS Traveler Redress Inquiry Program (TRIP)," also known as system DHS-ALL-005.[1] Under a second notice published the same day, DHS seeks to exempt this new records system from multiple requirements set out in the Privacy Act of 1974, 5 U.S.C. § 552a.[2] Pursuant to these notices, the Electronic Privacy Information Center ("EPIC") submits these comments to request DHS fully apply Privacy Act requirements of notice, access, correction, and judicially enforceable redress to TRIP and the underlying system of watch lists. Full application of the Privacy Act requirements to government record systems is the only way to ensure that data is accurate and complete, which is especially important in the context of watch lists, where mistakes and misidentifications are costly.

Introduction

EPIC has submitted a series of comments concerning traveler screening systems undertaken by federal entities. In December 2006, EPIC led a coalition of 29

[1] Dep't of Homeland Sec., *Privacy Act; Redress and Response System of Record*, 72 Fed. Reg. 2294 (Jan. 18, 2007).
[2] Dep't of Homeland Sec., *Privacy Act of 1974: Implementation of Exemptions; Redress and Response Records System*, 72 Fed. Reg. 2209 (Jan. 18, 2007).

organizations and 16 privacy and technology experts that urged DHS to curtail the Automated Targeting System, a federal database that creates secret, terrorist ratings on tens of millions of American citizens.[3] In May 2006, we urged Customs and Border Protection substantially narrow the Privacy Act exemptions prior to the revision and expansion of the Global Enrollment System, a database full of individuals' biometric and biographic data, which would be used to determine individual eligibility for the "Trusted Traveler" program.[4] In December 2005, EPIC urged DHS suspend the Registered Traveler program, a passenger prescreening program.[5] EPIC has commented upon many other traveler screening proposals, as well. EPIC also recently prepared an analysis of the problems with the proposed Traveler Redress Inquiry Program.[6] Now, we write to urge DHS to fully apply Privacy Act requirements of notice, access, correction, and judicially enforceable redress to TRIP and the underlying system of watch lists.

When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal data that federal agencies could collect and required agencies to be transparent in their information practices.[7] In 2004, the Supreme Court underscored the importance of the Privacy Act's restrictions upon agency use of personal data to protect privacy interests, noting that:

> "[I]n order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary . . . to regulate the collection, maintenance, use, and dissemination of information by such agencies." Privacy

---

[3] Thirty Orgs. & 16 Privacy & Tech. Experts, *Comments on Docket No. DH6-2006-0060: Notice of Privacy Act System of Records* (Dec. 4, 2006), *available at* http://epic.org/privacy/pdf/ats_comments.pdf.
[4] EPIC, *Comments on Docket No. DHS-2005-0053: Notice of Revision and Expansion of Privacy Act System of Records* (May 22, 2006), *available at* http://www.epic.org/privacy/airtravel/ges052206.pdf.
[5] EPIC, *Comments on Docket Nos. TSA-2004-19166 and TSA-2004-17982: Notice to Alter Two Existing Systems of Records; Request for Comments* (Dec. 8, 2005), *available at* http://www.epic.org/privacy/airtravel/profiling/rt120805.pdf.
[6] EPIC, Spotlight on Surveillance, *Problem-Filled Traveler Redress Program Won't Fly* (Nov. 2006), http://www.epic.org/privacy/surveillance/spotlight/1106/ (attached).
[7] S. Rep. No. 93-1183 at 1 (1974).

> Act of 1974, §2(a)(5), 88 Stat. 1896. The Act gives agencies detailed instructions for managing their records and provides for various sorts of civil relief to individuals aggrieved by failures on the Government's part to comply with the requirements.[8]

The Privacy Act is intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government[.]"[9] It is also intended to guard the privacy interests of citizens and lawful permanent residents against government intrusion. Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[10] It thus sought to "provide certain protections for an individual against an invasion of personal privacy" by establishing a set of procedural and substantive rights.[11] Adherence to these requirements is critical for a system such as TRIP and its underlying watch list systems.

The Supreme Court has long recognized that citizens enjoy a constitutional right to travel. In *Saenz v. Roe*, the Court noted that the "'constitutional right to travel from one State to another' is firmly embedded in our jurisprudence."[12] For that reason, any government initiative that conditions the ability to travel upon the surrender of privacy rights requires particular scrutiny. This concern is particularly relevant in the case of watch lists, which potentially impact millions of citizens. In Fiscal Year 2005, CBP alone

[8] *Doe v. Chao*, 540 U.S. 614, 618 (2004).
[9] S. Rep. No. 93-1183 at 1.
[10] Pub. L. No. 93-579 (1974).
[11] *Id*.
[12] 526 U.S. 489 (1999), quoting *United States v. Guest*, 383 U.S. 745 (1966).

"processed 431 million pedestrians and passengers, 121 million privately owned vehicles."[13]

I. Problems in Traveler Redress Procedures Remain Unresolved Under TRIP

Under the Aviation and Transportation Security Act of 2002, the Transportation Security Administration ("TSA") was authorized to maintain watch lists of names of individuals suspected of posing "a risk of air piracy or terrorism or a threat to airline or passenger safety."[14] Documents obtained in 2002 by EPIC from TSA under the Freedom of Information Act established that the agency administers two lists: a "no fly" list and a "selectee" list.[15] The lists are sent to the airlines, which run passenger names against the lists. When a passenger checks in for a flight, he may be labeled a threat if his name matches an entry on one of the watch lists, even if he is not the person actually on the list. A match to the "no fly" list requires the airline to notify TSA and to call a law enforcement officer to detain and question the passenger. In the case of a Selectee, an "S" or special mark is printed on the individual's boarding pass and the person receives additional security screening. Customs and Border Protection also uses the lists to screen travelers. Many travelers have reported problems with being mistakenly matched to names on watch lists.

TRIP is described as "a central gateway to address watch list misidentification issues, situations where individuals believe they have faced screening problems at immigration points of entry, or have been unfairly or incorrectly delayed, denied

---

[13] W. Ralph Basham, Comm'r, Customs & Border Prot., Dep't of Homeland Sec., *Statement at a Hearing on Customs Budget Authorizations & Other Customs Issues Before the Subcom. on Trade of the H. Comm. on Ways & Means*, 109th Cong. (July 25, 2006), *available at* http://waysandmeans.house.gov/hearings.asp?formmode=view&id=5160.
[14] Pub. L. No. 107-71, 115 Stat. 597 (2002).
[15] EPIC, *Documents Show Errors in TSA's "No-Fly" Watch list*, http://www.epic.org/privacy/airtravel/foia/watch list_foia_analysis.html.

boarding or identified for additional screening at our nation's transportation hubs."[16] However, because TRIP provides a central system for submitting, directing and tracking, but not resolving complaints, it fails to resolve the significant problems in current traveler redress procedures.

A. Federal Terrorist Watch Lists Are Full of Errors

In 2003, Homeland Security Presidential Directive No. 6 consolidated administration of the no-fly, selectee and other security watch lists under the jurisdiction of the Terrorist Screening Center.[17] When the Department of Justice Inspector General issued a report on the Terrorist Screening Center in June 2005, he found major concerns about, among other things, data accuracy and completeness.[18] The Inspector General "determined that the TSC could not ensure that the information in that database was complete and accurate."[19] He said, "Our review of the consolidated watch list identified a variety of issues that contribute to weaknesses in the completeness and accuracy of the data, including variances in the record counts between [two versions of the Terrorist Screening Database], duplicate records, missing or inappropriate handling instructions or categories, missing records, and inconsistencies in identifying information between TSDB and source records."[20]

---

[16] Press Release, Dep't of Homeland Sec., *DHS to Launch Traveler Redress Inquiry Program*, Jan. 17, 2007 [hereinafter "DHS Press Release about TRIP"], *available at* http://www.dhs.gov/xnews/releases/pr_1169062569230.shtm.
[17] Homeland Sec. Presidential Directive/HSPD-6, *Subject: Integration and Use of Screening Information* (Sept. 16, 2003), *available at* http://www.whitehouse.gov/news/releases/2003/09/20030916-5.html.
[18] Dep't of Justice, Inspector Gen., Audit Div., *Audit Report No. 05-27: Review of the Terrorist Screening Center* 66-67 (June 2005), *available at* http://www.usdoj.gov/oig/reports/FBI/a0527/final.pdf.
[19] *Id*. at xi.
[20] *Id*. at 66.

In February 2006, there were 325,000 names on the watch lists, according to the National Counterterrorism Center.[21] Last year, the director of TSA's redress office revealed that more than 30,000 people who are not terrorists have asked the agency to remove their names from the lists since September 11, 2001.[22] Last month, the head of TSA said that the watch lists were being reviewed, and he expected to cut the list of names in half.[23] However, he has not disclosed details, such as what the criteria would be for removing a name or when the review would be complete. These reports show that the watch lists are rife with mistakes and "false positives."

Federal officials claim that passenger prescreening program Secure Flight will help solve these problems.[24] Under Secure Flight, the responsibility for checking airline passenger names against expanded the watch lists be removed from the airlines and handed over to the federal government. However, a Government Accountability Office ("GAO") report and testimony found that TSA approved Secure Flight to become operational last September despite inconclusive risk assessments and 144 known security vulnerabilities.[25] In addition to criticizing Secure Flight's lack of privacy and security safeguards, GAO noted that the documents underlying the program "contained

---

[21] Walter Pincus & Dan Eggen, *325,000 Names on Terrorism List*, Wash. Post. Feb. 15, 2006.
[22] Anne Broache, *Tens of thousands mistakenly matched to terrorist watch lists*, CNet News.com, Dec. 6, 2005.
[23] Edmund S. "Kip" Hawley, Assistant Sec'y, Transp. Sec. Admin., Dep't of Homeland Sec., *Testimony at Hearing on Aviation Security: Reviewing the Recommendations of the 9/11 Commission Before the S. Comm. on Commerce, Science & Transportation*, 110th Cong. (Jan. 17, 2007), *available at* http://commerce.senate.gov/public/_files/TestimonyofMrHawley.pdf.
[24] Dep't of Homeland Sec., Privacy Office, *Report Assessing the Impact of the Automatic Selectee and No Fly Lists on Privacy and Civil Liberties as Required Under Section 4012(b) of the Intelligence Reform and Terrorism Prevention Act of 2004* 4-5 (Apr. 27, 2006) [hereinafter "Privacy Office Report on Watch Lists"], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_nofly.pdf.
[25] Cathleen Berrick, Dir., Homeland Sec. & Justice, Gov't Accountability Office, *Statement at a Hearing on TSA's Secure Flight and Registered Travelers Programs Before the S. Comm. on Commerce, Science & Transportation*, 109th Cong. (Feb. 9, 2006), *available at* http://www.gao.gov/new.items/d06374t.pdf.

contradictory and missing information."[26] Last February, the head of the Transportation Security Administration told a congressional committee that Secure Flight was suspended for a comprehensive review of the program's information security measures after the GAO report showed the program was riddled with problems.[27]

B. Travelers Face Significant Problems When Attempting to Resolve Mismatches to Watch lists

There have been myriad stories about mistakes associated with the watch lists, with sometimes chilling results. An April 2006 report by the Department of Homeland Security's Privacy Office on the impact of the watch lists explained that "individuals who are mistakenly put on watch lists or who are misidentified as being on these lists can potentially face consequences ranging from inconvenience and delay to loss of liberty."[28] The report described complaints "alleg[ing] misconduct or disrespect by airline, law enforcement, TSA or CBP officials" toward people mistakenly matched.[29] According to the Privacy Office:

> reported experiences of individuals whose names appear to match names on the No-fly and Selectee lists can be trying and unpleasant. Complaints filed with CRCL have alleged that individuals have experienced long delays, have been separated from members of their family and given no explanation or conflicting explanations about what is going on. Some complaints alleged that officers have asked […] whether one traveler knew anyone at his mosque who hates Americans or disagrees with current policies, targeted a traveler for additional screening because she wore traditional Muslim attire and told another traveler that he and his wife and children were subjected to body searches because he was born in Iraq, is Arab, and Muslim.[30]

---

[26] *Id*.
[27] Edmund S. "Kip" Hawley, Nominee for Assistant Sec'y of Homeland Sec., Transp. Sec. Admin., Dep't of Homeland Sec., *Testimony at Hearing on TSA's Secure Flight and Registered Travelers Programs Before the S. Comm. on Commerce, Science & Transportation*, 109th Cong. (Feb. 9, 2006).
[28] Privacy Office Report on Watch Lists at i, *supra* note 24.
[29] *Id.* at 18.
[30] *Id.*

Also, documents recently obtained by EPIC under the Freedom of Information Act show nearly a hundred complaints from airline passengers between November 2003 and May 2004 about the government's traveler screening security measures.[31] The complaints describe the bureaucratic maze passengers encounter if they happen to be mistaken for individuals on the list, as well as the difficulty they encounter trying to exonerate themselves through the redress process. One person named in the documents, Sister Glenn Anne McPhee, U.S. Conference of Catholic Bishops' secretary for education, spent nine months attempting to clear her name from a TSA watch list. The process was so difficult, Sister McPhee told a reporter, "Those nine months were the closest thing to hell I hope I will ever experience."[32]

Last month, at a hearing of the Senate Commerce Committee, Sen. Ted Stevens complained that his wife, Catherine, is frequently mismatched to the watch list name "Cat Stevens."[33] Senators Ted Kennedy and Don Young are among those who have been improperly flagged by watch lists.[34] Sen. Kennedy was able to resolve the situation only by enlisting the help of then-Homeland Security Secretary Tom Ridge.

In 2005, Congress ordered the Government Accountability Office to investigate TSA's airline passenger screening programs. GAO found significant problems with handling of personal information and violations of privacy laws.[35] In September, GAO

---

[31] Dep't of Homeland Sec., Transp. Sec. Admin., *Complaint Log,* Nov. 2003 to May 2004, obtained by EPIC through FOIA litigation, *available at* http://www.epic.org/privacy/airtravel/foia/complaint_log.pdf.
[32] Ryan Singel, *Nun Terrorized by Terror Watch*, Wired News, Sept. 26, 2005.
[33] Beverley Lumpkin, *Aviation Security Chief Says No-Fly List is Being Reduced by Half*, Associated Press, Jan. 18, 2007.
[34] *See, e.g.,* Sara Kehaulani Goo, *Committee Chairman Runs Into Watch-List Problem*, Wash. Post, Sept. 30, 3004; Leslie Miller, *House Transportation Panel Chairman Latest to be Stuck on No-Fly List*, Associated Press, Sept. 29, 2004; Shaun Waterman, *Senator Gets a Taste of No-Fly List Problems*, United Press Int'l, Aug. 20, 2004.
[35] Gov't Accountability Office, *Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices,*

reviewed the watch list system and found "about half of the tens of thousands of potential matches sent to the center between December 2003 and January 2006 for further research turned out to be misidentifications."[36] According to the GAO, these misidentifications are a significant problem, and they:

> highlight the importance of having a process -- often referred to as redress -- for affected persons to express their concerns, seek correction of any inaccurate data, and request other actions to reduce or eliminate future inconveniences. Similarly, such a process would apply to other persons affected by the maintenance of watch list data, including persons whose names are actually on the watch list but should not be ("mistakenly listed persons") as well as persons who are properly listed.[37]

The current redress process requires individuals to contact the screening agency that processed them.[38] TSA has the Traveler Identity Verification Program; CBP asks individuals to contact its Customer Satisfaction Unit; and the State Department sends inquiries to the director of Information Management Liaison. The processes are all similar to the TSA process. Under TSA's program, the affected individual fills out a Traveler Identity Verification form and submits identity documents to the agency: either "a copy of your U.S. passport OR copies of three of the following: Driver's License; Birth Certificate; Voter Registration; Military ID Card; Visa; Naturalization Card; Government ID Card."[39]

After submitting this additional information, then TSA "will use this information in deciding whether the person's name should be put on a cleared list -- which airlines are to use for distinguishing the individual from persons who are in fact on the No Fly or

---

but Has Recently Taken Steps to More Fully Inform the Public, GAO-05-864R (July 22, 2005), *available at* http://www.gao.gov/new.items/d05864r.pdf.

[36] Gov't Accountability Office, *Terrorist Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public,* GAO-06-1031 (Sept. 2006), *available at* http://www.gao.gov/new.items/d061031.pdf.

[37] *Id*. at 2.

[38] *Id*. at 55-56.

[39] *Id*. at 62.

Selectee lists," the GAO said.[40] However, according to the director of TSA's redress office, "some customers (air passengers) call and complain about having problems even though they have taken the necessary steps to be placed on the cleared list."[41]

Complaints about the failure of TSA safeguards are numerous. For example, at a House subcommittee hearing on March 2, 2005, Rep. Loretta Sanchez reported that many of her constituents continue to face lengthy delays, questioning, and at times are prohibited from boarding flights because they are misidentified as people sought on watch lists. Her constituents continue to face these roadblocks even after they apply for, receive and then display to screener and airport personnel the official federal government letters that establish their innocence.[42]

C. TRIP Fails to Resolve Problems in Current Redress Procedures

Removal from the watch lists is not a simple matter. The vast majority of people affected by watch list errors face an opaque and arbitrary bureaucratic process. They are never told the reasons for their being placed on the lists.

Under TRIP, an individual with a redress request will be asked a series of questions so that TRIP can "assess the information provided and identify the most appropriate DHS component to address the request."[43] Though TRIP "will coordinate and process the intake and close-out requests for redress or assistance," the various DHS components, such as TSA or Customs and Border Protection, "will continue to maintain

---

[40] *Id*. at 34.
[41] *Id*.
[42] Shaun Waterman, *No Redress Mechanism in New DHS Terrorist Screening Office*, United Press Int'l, Mar. 2, 2005.
[43] Dep't of Homeland Sec., *Privacy Impact Assessment for the DHS Traveler Redress Inquiry Program (DHS TRIP)* 8 (Jan. 18, 2007) [hereinafter "TRIP Privacy Impact Assessment"], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhstrip.pdf.

responsibility for resolving the requests."[44] TRIP is merely a system to receive and direct redress requests; it is not a system to process the requests. TRIP does not address the myriad problems in current redress procedures that innocent travelers mistakenly matched to watch lists must face.

II. The Only Way to Solve "False Positive" Problem Is to Fully Apply Privacy Act Obligations to Watch List Systems

Homeland Security Secretary Michael Chertoff recently discussed the citizens' right to redress in cases where they are mistakenly listed as "threats" on the Transportation Security Administration's "no-fly lists." He said, "we don't conduct court hearings on this" because "first of all, almost all the information is classified; second, because I'm quite sure that the 19 hijackers, if we could replay history, would have contested being on a no-fly list, and we're not about to let them do that; and third, because we would be inundated with proceedings."[45] Secretary Chertoff is correct: if citizens had the right to sue to ensure that their records are correct, that they are not mistakenly matched to or listed on watch lists, then the department would be inundated – and innocent citizens would be cleared of the "threat" label. Full application of the access and correction requirements of the Privacy Act of 1974 would ensure accurate data and resolve the "false positive" problem.

A. TRIP Fails to Follow Access and Correction Procedures Required Under the Privacy Act of 1974

The Department of Homeland Security proposes to exempt the program from Privacy Act of 1974 requirements that an individual be permitted access to personal information, that an individual be permitted to correct and amend personal information,

[44] *Id*. at 2.
[45] Michael Chertoff, Sec'y of Homeland Sec., *Remarks at the Federalist Society's Annual Lawyers Convention*, Nov. 17, 2006, *available at* http://www.dhs.gov/xnews/speeches/sp_1163798467437.shtm.

and that an agency assure the reliability of personal information for its intended use.[46] DHS will allow individuals the right to access and correct "information submitted by and collected from individuals or their representatives in the course of any redress procedure associated with [TRIP]"; however, it will not allow access to any other data.[47] This is small consolation, considering individuals already would have access to the data they submitted, and they would need to be able to access and correct other data gathered about them to ensure the data's accuracy and completeness.

If, upon completion of the redress process, the individual is not "cleared," not given a letter declaring she is not the person named on the watch list, she "may have the opportunity to submit supplementary information based upon the redress procedures, if any, of the component/agency responsible for handling the request."[48] Also, "an individual will be notified in the disposition letter sent by DHS TRIP or the DHS component/agency whether he or she may request to have the resolution reconsidered."[49]

> DHS does say, however, that it:
>
> > will examine each separate request on a case-by-case basis, and, after conferring with the appropriate component or agency, may waive applicable exemptions in appropriate circumstances and where it would not appear to interfere with or adversely affect the law enforcement or national security purposes of the systems from which the information is recompiled or in which it is contained.[50]

Considering the breadth of the "routine uses" listed below by the agency, it is difficult to imagine a case in which DHS would judge it feasible to allow an individual full access to her watch list file.

---

[46] 72 Fed. Reg. at 2209, *supra* note 2; TRIP Privacy Impact Assessment at 12, *supra* note 43.
[47] 72 Fed. Reg. at 2209, *supra* note 2.
[48] TRIP Privacy Impact Assessment at 13, *supra* note 43.
[49] *Id*.
[50] 72 Fed. Reg. at 2210, *supra* note 2.

DHS has identified 10 categories of "routine uses" of personal data that will be collected and maintained in the program's system of records. In one category, DHS anticipates disclosure:

> E. To an appropriate Federal, State, territorial, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and disclosure is appropriate to the proper performance of the official duties of the person receiving the disclosure.[51]

Another category allows disclosure:

> F. To an appropriate Federal, State, territorial, tribal, local, international, or foreign government intelligence entity, counterterrorism agency, or other appropriate authority charged with investigating threats or potential threats to national or international security or assisting in counterterrorism efforts, where a record, either on its face or in conjunction with other information, identifies a threat or potential threat to national or international security, which includes terrorist activities, and disclosure is appropriate to the proper performance of the official duties of the person receiving the disclosure.

These categories are so broad as to be almost meaningless, allowing for potential disclosure to virtually any government agency worldwide for an array of actual or potential undefined violations. With such an array of national and international agencies and myriad cases "where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law," it is difficult to imagine a scenario where full disclosure to the individual "would not appear to interfere with or adversely affect the law enforcement or national security purposes of the systems from which the information is recompiled or in which it is contained," and DHS would choose to waive the Privacy Act exemptions it seeks.

[51] 72 Fed. Reg. at 2297, *supra* note 1.

The agency also proposes to disclose all or a portion of the records or information contained in the system outside of the DHS when "it is suspected or confirmed that the security or confidentiality of information in the system of record has been compromised" and for other purposes.[52] While we support notification to affected individuals in the case of security breaches, this routine use would stand the presumption of the Privacy Act on its head. Instead of the agency informing the individual of information in the possession of the agency that could have an adverse impact, DHS would distribute the information widely across the federal government while keeping it secret from the individual whose interests are supposed to be protected by the Privacy Act.

B. Reasons for Exempting TRIP and Watch List Systems From Privacy Act Requirements Are Specious

DHS seeks to exempt TRIP and the underlying watch list systems from Privacy Act obligations ensuring judicially enforceable rights of access and correction. These obligations include:

- an individual may request access to records an agency maintains about him or her;[53]
- an individual may seek judicial review to enforce the statutory right of access provided by the Act;[54]
- an agency must correct identified inaccuracies promptly;[55]
- an agency must make notes of requested amendments within the records; and[56]
- an agency must establish procedures to handle disputes between the agency and individual as to the accuracy of the records.[57]

The Privacy Act imposes these obligations to allow citizens to ensure the government fulfills the requirement to "maintain all records which are used by the agency

[52] *Id*.
[53] 5 U.S.C. § 552a(d)(1).
[54] 5 U.S.C. § 552a(g)(1).
[55] 5 U.S.C. § 552a(d)(2)(B), (d)(3).
[56] 5 U.S.C. § 552a(d)(4).
[57] 5 U.S.C. § 552a(f)(4).

in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination."[58]

In large part, the agency justifies the exemptions, because:

> making available to a record subject the accounting of disclosures from records concerning him or her would specifically reveal any investigative interest in the individual. Revealing this information could reasonably be expected to compromise ongoing efforts to investigate a known or suspected terrorist by notifying the record subject that he or she is under investigation. This information could also permit the record subject to take measures to impede the investigation.[59]

However, if an individual has been told at the airport that she has been matched to a name on a watch list, then she already knows that she is under investigation. If the individual is an actual terrorist, then she would hardly choose to file a redress request. The deliberate obfuscation of information does not help the terrorists, but instead frustrates the innocent citizens who apply for redress because they are mistakenly matched to or mistakenly listed on the watch lists.

DHS seeks to justify the exemption from the obligation to ensure accuracy, relevance, timeliness and completeness in the records by claiming, "because many of the records in this system coming from other system of records are derived from other domestic and foreign agency record systems and therefore it is not possible for DHS to vouch for their compliance" with these requirements.[60] So, even though the records may be irrelevant, untimely, incomplete and inaccurate, DHS does not allow an individual to access or correct any data other than the data the individual has submitted herself.

---

[58] 5 U.S.C. § 552a(e)(5).
[59] 72 Fed. Reg. at 2211, *supra* note 2.
[60] *Id*.

C. Full Application of Privacy Act Obligations Is the Only Way to Ensure Accurate and Complete Data for Screening Programs

The Department of Homeland Security proposes to exempt TRIP and the underlying watch list databases from the Privacy Act requirements allowing individuals judicially enforceable rights to access information about them contained in the system, and to request correction of information that is inaccurate, irrelevant, untimely or incomplete. However, DHS does not create an alternative venue for access or correction of data for which the agency has admitted it cannot "vouch for their compliance" with these requirements. Instead, the agency asks citizens to rely on the fact that "DHS has implemented internal quality assurance procedures to ensure that data used in the redress process is as thorough, accurate, and current as possible."[61]

We have already explained above the many problems that have occurred even with DHS's "internal quality assurance procedures." The Government Accountability Office has found significant problems with handling of personal information and violations of privacy laws by DHS; tens of thousands of people have applied for redress after being mistakenly matched; the bloated watch lists are being cut in half; and other problems. The current system is not working.

In the Privacy Impact Assessment for TRIP, the Department of Homeland Security discussed the accuracy of data collected from individuals seeking redress. "Because the individual provides the information about him or herself directly, the likelihood of erroneous [Personally Identifiable Information] is greatly reduced."[62] We agree. The only way to ensure the accuracy, timeliness, relevance and completeness of the data used is to allow individuals to access, review and correct their records. DHS

[61] *Id*.
[62] TRIP Privacy Impact Assessment at 6, *supra* note 43.

must fully apply the Privacy Act of 1974 obligations upon TRIP and the underlying watch lists systems.

Conclusion

When announcing the Traveler Redress Inquiry Program, Homeland Security Secretary Michael Chertoff said, "Ensuring that personal information is accurate and complete allows us to focus fewer resources on legitimate travelers and more resources on national security and law enforcement issues."[63] The only way to ensure that the personal data is accurate and complete is to apply all Privacy Act obligations to government record-keeping systems, including the no-fly and selectee lists. If a person is placed on one of these watch lists, he should know why and be able to challenge the determination. EPIC urges the Department of Homeland Security to apply all Privacy Act requirements to TRIP and the underlying watch list databases.

Respectfully submitted,

Marc Rotenberg
Executive Director

Melissa Ngo
Director, Identification and
Surveillance Project

ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, N.W.

[63] DHS Press Release about TRIP, *supra* note 16.

Suite 200
Washington, DC 20009
(202) 483-1140

Attachment