



Secure Flight Report

DHS Privacy Office Report to the Public on the
Transportation Security Administration's Secure Flight
Program and Privacy Recommendations

December 2006



**Homeland
Security**



Report to the Public on the
Transportation Security Administration's
Secure Flight Program and Privacy
Recommendations

Privacy Office
U.S. Department of Homeland Security
Washington, DC

December 2006

TABLE OF CONTENTS

I.	SUMMARY	1
II.	BACKGROUND	2
III.	METHODOLOGY	2
IV.	OVERVIEW OF SECURE FLIGHT PRIVACY NOTICES	2
A.	THE FALL PRIVACY NOTICES	3
B.	THE NOTICE OF FINAL ORDER	6
C.	GAO CONCERNS	8
D.	REVISED NOTICES	9
V.	ANALYSIS	11
A.	NO "FIREWALL"	11
B.	TSA NEVER RECEIVED AUTHENTICATION SCORES AND CODES	12
C.	SOME INDIVIDUALS WHOSE DATA WAS OBTAINED FROM COMMERCIAL DATA BROKERS HAD NOT RECEIVED NOTICE	13
VI.	FINDINGS	13
VII.	RECOMMENDATIONS	14
VIII.	GOING FORWARD	15

I. Summary

The Department of Homeland Security (DHS) Privacy Office conducted a review of the Transportation Security Administration's (TSA) collection and use of commercial data during initial testing for the Secure Flight program that occurred in the fall 2004 through spring 2005. The Privacy Office review was undertaken following notice by the TSA Privacy Officer of preliminary concerns raised by the Government Accountability Office (GAO) that, contrary to published privacy notices and public statements, TSA may have accessed and stored personally identifying data from commercial sources as part of its efforts to fashion a passenger prescreening program.

These new concerns followed much earlier public complaints that TSA collected passenger name record data from airlines to test the developmental passenger prescreening program without giving adequate notice to the public.¹ Thus, the Privacy Office's review of the Secure Flight commercial data testing also sought to determine whether the data collection from air carriers and commercial data brokers about U.S. persons was consistent with published privacy documents.

The Privacy Office appreciates the cooperation in this review by TSA management, staff, and contractors involved in the commercial data testing. The Privacy Office wishes to recognize that, with the best intentions, TSA undertook considerable efforts to address information privacy and security in the development of the Secure Flight Program. Notwithstanding these efforts, we are concerned that shortcomings identified in this report reflect what appear to be largely unintentional, yet significant privacy missteps that merit the careful attention and privacy leadership that TSA Administrator Kip Hawley is giving to the development of the Secure Flight program and, in support of which, the DHS Acting Chief Privacy Officer has committed to provide Privacy Office staff resources and privacy guidance.

Set forth at the conclusion of this Report are privacy policy recommendations that, if instituted, should significantly raise privacy awareness and better assure that privacy notices to the public match operational plans for Secure Flight or any program at DHS. We believe that implementation of these recommendations will promote fuller achievement of privacy protections and build public trust in Departmental efforts to successfully launch a passenger prescreening program, as required under the Intelligence

¹ The Privacy Office documented earlier missteps in the Privacy Office's Report to the Public on Events Surrounding jetBlue Data Transfer, but did not conclude that TSA violated the Privacy Act. The DHS Office of Inspector General in its report issued in connection with its review of fourteen transfers of airline passenger data, including the jetBlue Data Transfer, noted that "TSA could have taken more steps to protect privacy," (OIG Report OIG-05-12, *Review of the Transportation Security Administration's Role in the Use and Dissemination of Airline Passenger Data*, March 2005, p. 40) but did not find any Privacy Act violations.

Reform and Terrorism Prevention Act² and the Department of Homeland Security Appropriations Act of 2005.³

II. Background

By law, DHS's statutorily-created Chief Privacy Officer⁴ has primary responsibility for, among other duties, assuring that personal information contained in a Privacy Act system of records is handled in full compliance with the fair information practices of the Privacy Act of 1974 and reporting on complaints of privacy violations.

III. Methodology

The Privacy Office review included a thorough examination of documents as well as extensive interviews with TSA personnel and TSA contractors. At all times, TSA management, supervisors, staff, and contractors were completely cooperative and assisted in the review. The Privacy Office review determined pertinent facts and areas for needed improvement in operations to better safeguard individual privacy and strengthen public trust in the Secure Flight program.

IV. Overview of Secure Flight Privacy Notices

In the fall of 2004, TSA announced Secure Flight, a new airline passenger prescreening program. In brief, Secure Flight was narrowly tailored and designed to compare the identifying information of airline passengers contained in passenger name records (PNRs)⁵ to the identifying information of individuals contained in the Terrorist Screening Database (TSDB), a watch list maintained by the Terrorist Screening Center (TSC) containing identifying information about suspected and known terrorists. The purpose of this comparison was to assist TSA in preventing individuals, known to be or suspected of being engaged in terrorist activity, from boarding domestic passenger flights and, thus, to increase airline security and assist with DHS's larger mission of protecting the Homeland.

² The Intelligence Reform and Terrorism Security Act, Pub. L. No. 108-458, § 4012, 118 Stat. 3638, 3714-19 (2004).

³ The Department of Homeland Security Appropriations Act, 2005, Pub. L. 108-334, § 522(a)(8) requires TSA to satisfy and the Government Accounting Office to assess Secure Flight on ten areas of Congressional interest and report to Congress.

⁴ See Homeland Security Act of 2002, Section 222, 6 U.S.C. § 142.

⁵ These records are compiled by airlines and include, among other information, passenger name, reservation data, travel agency or agent, itinerary information, form of payment, flight number, and seat location.

As a prerequisite to testing the new program, TSA issued a Privacy Act System of Records Notice (SORN) (69 FR 57345 (Sept. 24, 2004)) explaining its intention to collect PNR and the uses that it would make of this information. TSA requested public comments on the SORN. TSA also published a Privacy Impact Assessment (PIA) covering the testing phase of the Secure Flight program. (69 FR 57347 (Sept. 24, 2004)) (These documents are referred to hereafter as the "Fall Privacy Notices.") With publication of the Fall Privacy Notices in the Federal Register, TSA followed the Privacy Act⁶ and the E-Government Act⁷ requirements for programs that collect, maintain, and use personally identifiable data. The intention of the Fall Privacy Notices was the same as any other notice in this context -- to inform the public and receive public comments about how the Government will collect, store, and use their information for a specific mission or program of a federal agency.

This section examines how each of the notices addressed the commercial data testing and the privacy and security protections TSA intended to employ. The notices provide an important tool for evaluating privacy practices for the Secure Flight program.

A. *The Fall Privacy Notices*

In its Fall Privacy Notices, TSA stated that it was establishing the "Secure Flight Test Records" system of records to compare the identifying information contained in passenger name records to the identifying information of individuals in the Terrorist Screening Database maintained by the Terrorist Screening Center.⁸ TSA also announced that it would conduct a separate "test of the use of commercial data to determine whether such use: (1) could accurately identify when passenger information is inaccurate or incorrect; (2) would not result in inappropriate differences in treatment of any protected category of persons; and could be governed by data security safeguards and privacy protections that are sufficiently robust to ensure that commercial entities or other unauthorized entities do not gain access to passenger personal information, or to ensure that the Federal Government does not gain access inappropriately to certain types of sensitive commercial data."⁹ For both tests, TSA announced it would issue an order to domestic airlines with flights operated under a full security program to submit to TSA a

⁶ The Privacy Act of 1974 requires agencies to publish a notice describing a record system from which information is retrieved by name or personal identifier whenever such a system is created or substantially revised.

⁷ The E-Government Act of 2002 requires agencies to conduct a privacy impact assessment before developing systems that collect, maintain or disseminate information in an identifiable form.

⁸ 69 Fed. Reg. 57345 (Sept. 24, 2004).

⁹ 69 Fed. Reg. 57345, at 57346.

limited set of historical PNRs that cover domestic flight segments completed in the month of June 2004.¹⁰

In its SORN, TSA stated that it would not have access to the commercial data: “TSA will not store the commercially available data that would be accessed by commercial data aggregators.”¹¹ Additionally, the PIA accompanying the SORN assured the public that “[t]esting will be governed by strict privacy and data security protections. TSA will not store the commercially available data that would be accessed by commercial data aggregators.”¹² The PIA also said that to address the privacy and civil liberties concerns raised by using commercial data, TSA would:

1. Only test the use of commercial data, deferring any decision on its use until after completing the testing and analysis and promising to issue a new SORN if a decision was made to use commercial data;
2. Not assume that the result of comparison of passenger information to commercial data is determinative of information accuracy or the intent of the person who provided the passenger information;
3. Apply stringent data security and privacy protections, including contractual prohibitions on commercial entities’ maintenance or use of airline-provided PNR information for any purposes other than testing under TSA parameters; strict firewalls between the government and commercial data providers; real-time auditing procedures to determine when data within the Secure Flight system has been accessed and by whom; strict rules prohibiting the accessing or use of commercially held personal data by TSA.¹³

The notices also addressed data access and retention.¹⁴ The SORN stated that although the system was exempt from record access procedures under 5 U.S.C. 552a(k), all persons could request access to information about them contained in a PNR by writing to

¹⁰ Id.

¹¹ Id., at 57346. This sentence is admittedly very awkward. It is not clear what it means by “the commercially available data that would be accessed by commercial data aggregators.” Is it referring to the fact that the aggregators would access their own databases and that TSA would not have access to those databases or that TSA would not access the commercial data that it received from the data aggregators?

¹² 69 Fed. Reg. 57353 (Sept. 24, 2004).

¹³ 69 Fed. Reg. 57355 (Sept. 24, 2004).

¹⁴ 69 Fed. Reg. 57345, at 57438 and 69 Fed. Reg. 57352, at 57354.

the TSA Privacy Officer.¹⁵ Such requests would be granted “[t]o the greatest extent possible and consistent with national security requirements.”¹⁶ Nevertheless, no mention was made regarding access to any commercial data collected during the testing of the program because TSA did not expect government employees to access commercial data records.

As to data retention, the SORN and PIA stated that TSA was working with the National Archives and Records Administration (NARA) to obtain approval of a records retention and disposal schedule and that TSA was proposing a short retention schedule.¹⁷ The PIA stated that TSA would retain the information it collected “for a sufficient period of time to conduct and review the Secure Flight test and in the event where a request for redress must be resolved.”¹⁸

Nevertheless, none of the initial notices provided any details on the types or categories of personal information that TSA or its contractor would collect from the commercial data providers. The SORN did provide a general description of the fields of information found in PNRs,¹⁹ but the only descriptor of what commercial data would be collected was listed in the SORN’s “Categories of Records in the System” section as “[a]uthentication scores and codes obtained from commercial data providers.”²⁰

The Privacy Office understands that the descriptor “authentication scores and codes” was drawn from the earlier design for CAPPS II, which called for TSA to provide PNR data to the commercial data providers for analysis, and the data providers would only return authentication scores and codes to indicate confidence levels for PNR matches. Therefore, the plain reading of the Fall Privacy Notices was that TSA would only receive scores and codes and no commercial data.

¹⁵ TSA did not issue an exemption rule and in the Final Notice supported access consistent with law enforcement and national security concerns.

¹⁶ 69 Fed. Reg. 57345, at 57348.

¹⁷ 69 Fed. Reg. 57345, at 57348.

¹⁸ 69 Fed. Reg. 57352, at 57354.

¹⁹ 69 Fed. Reg. 57345, at 57346. Although PNR data may vary among the airlines, the SORN stated that it includes, among other information: (1) Passenger name; (2) reservation data; (3) travel agency or agent; (4) travel itinerary information; (5) form of payment; (6) flight number; and (7) seating location.

²⁰ 69 Fed. Reg. 57345, at 57347.

B. The Notice of Final Order

On November 15, 2004, TSA published a Notice of Final Order for Secure Flight Test Phase (“Final Notice”),²¹ which responded to approximately 500 comments filed regarding the Fall Privacy Notices and the request to OMB for approval of a proposed order to collect PNRs from air carriers to test the Secure Flight program. The Final Notice discussed the public comments received to the proposed notice and provided instructions to air carriers on submitting the required PNRs by November 23, 2004.

Even more clearly than in the Fall Privacy Notices, the Final Notice stated, “TSA will not receive the commercially available data that would be used by commercial data aggregators.”²² Repeating much of the language from the proposed SORN, the Final Notice assured the public that the program would emphasize privacy. To commenters who expressed concern that TSA’s access to commercial information would “open the door to abuse of individuals’ privacy rights and possible theft of their personal information,”²³ TSA responded:

*TSA’s testing of commercial data will be governed by stringent data security and privacy protections, including: contractual prohibitions on commercial entities’ maintenance or use of PNR information for any purposes other than testing under TSA parameters; strict firewalls between the government and commercial data providers; real-time auditing procedures to determine when data has been accessed and by whom; and strict rules prohibiting the access or use of commercially held personal data by TSA. TSA will not have access to or store the commercially available data that would be used by commercial data aggregators.*²⁴

This language is very clear – TSA would not access, use, or store the commercial data; however, the Final Notice signaled that TSA’s contractors would handle the commercial data. In fact, the Final Notice indicated that TSA would have strong contractual requirements in place to deter weak data handling practices by contractors. The PIA had already said that TSA contractors involved in the testing of Secure Flight were

²¹ 69 Fed. Reg. 65619 (Nov. 15, 2004).

²² Id.

²³ Id., at 65622.

²⁴ Id.

contractually and legally obligated to comply with the Privacy Act in their handling, use, and dissemination of personal information in the same manner as TSA employees.²⁵

The description in the Final Notice regarding the commercial data was somewhat confusing and did not clarify what commercial data would be used in the testing. TSA stated that testing would provide “information about the feasibility and efficacy of using commercial data, such as credit card numbers, to gauge the accuracy of passenger information and reduce false positive matches to information in the TSDB...”²⁶ At the same time, however, the Final Notice did not specify what commercial data would be used in testing. This was not surprising given that at the time of drafting the Final Notice, TSA had not determined what types of commercial data it would use. TSA did assert in the Notice that it would not have access to individuals’ credit histories, medical records, or other personal records.

Importantly, the Final Notice made no mention of collecting authentication scores and codes. As discussed below, the early drafts of the Statement of Work for the testing program, which were developed after the Fall Privacy Notices, made clear that the contractor would ingest the commercial data and did not mention receiving scores and codes. The Final Notice simply said in its “Findings” section that TSA would test whether comparing passenger information to other commercially available data can enhance TSA’s ability to identify passenger information that is inaccurate or incorrect.²⁷

In addition to addressing concerns about the commercial data, commenters raised serious concerns about data retention, the Privacy Act exemptions, access and redress. TSA responded with assurances that the program was “a limited, reasonable security screening measure” and “will not impose an unconstitutional burden on an individual’s right to travel or exercise other Constitutional rights.”²⁸ TSA was more explicit in the Final Notice about its retention policy, stating that for purposes of the testing phase of the program, it was seeking approval from NARA to destroy PNRs used for the test after the test was completed.²⁹ TSA affirmed it did not need to retain passenger information and assured the public that the Secure Flight program would destroy passenger information shortly after completion of the passenger’s itinerary. The Final Notice countered requests to narrow the Privacy Act exemptions by making a commitment to transparency,

²⁵ 69 Fed. Reg. 57352, at 57354.

²⁶ 69 Fed. Reg. 65619, at 65622.

²⁷ *Id.*, at 65626.

²⁸ *Id.*, at 65620.

²⁹ *Id.*

asserting that “[t]his transparency will serve to prevent so-called “mission creep.”³⁰ Commenters seeking greater access to information in the system of records were advised that TSA supported individuals’ access to records about them in the system to the greatest extent feasible, consistent with law enforcement and national security concerns.

Commenters were particularly critical that the Secure Flight Program had not provided for a redress process for passengers who believed they had been unfairly or inaccurately singled out for additional screening as a result of matching the PNRs to information in the TSDB. In the PIA and in the Final Notice, TSA recognized this need and committed to developing a “robust redress program,” but since TSA was only testing the Secure Flight concept and the PNRs were for flights that had already been completed, no passengers would need a redress process during the testing phase.³¹

TSA acknowledged in the Final Notice that its Secure Flight program was at the earliest stages of development and that the test phase would determine the program’s operations and policies.³² Commenters, not surprisingly, were pressing for more details about the program and its information practices. TSA promised that it would engage in a public rulemaking process if the test phase demonstrated that the program was feasible. The Final Notice also clarified that the carriers were only to provide PNRs in which all segments were completed in June 2004 and gave air carriers directions on providing the PNRs. It did not provide any further details about the use of commercial data or the methodology of the commercial data test.

C. GAO Concerns

In June 2005, as part of its routine oversight of the Secure Flight program, the GAO reviewed the commercial test procedures and informally shared the results of its review with TSA. This review followed up on briefings by TSA in 2004 and 2005 on plans for commercial data testing for the program. Concerned about GAO’s conclusions, the TSA Privacy Officer informally reported the preliminary GAO findings to the DHS Privacy Office. The Chief Privacy Officer, in keeping with her statutory authority, informed the Secretary of the Department that she would undertake a review of the commercial data test and its operational conformance or non-conformance with the prior Privacy Notices. Shortly thereafter, TSA, on its own, initiated a new public notice “to supplement and amend” the Fall and Final Notices to provide additional detail about the Secure Flight program, particularly the commercial data test.

³⁰ Id., at 65621.

³¹ Id., at 65622.

³² 69 Fed. Reg. 65619, at 65623.

D. Revised Notices

On June 22, 2005, TSA proactively published a notice “to supplement and amend” its initial SORN and PIA for the Secure Flight Test Phase (“Revised Notice”).³³ The Revised Notice provided additional details regarding the testing program and announced that TSA would not assert any Privacy Act exemptions for the system. The additional details included that: (1) TSA’s contractor, EagleForce, had purchased and held commercial data used in the testing; (2) the contractor had purchased commercial data not only about the June 2004 travelers, but about other individuals whose names were variations on the June 2004 travelers for analytical purposes; and (3) the PNRs had been enhanced by extracting selected items of information from the commercial data purchased and inserting it in the PNR. Augmentation was only done where specific data (address, date of birth, and gender) was missing from one of the 42,000 sample records. This publication came shortly before the GAO issued its report on TSA’s use of personal information during the Secure Flight Program Testing, hereinafter the “GAO Report.”³⁴

The Revised Notice described the role of the TSA contractor and its purchase and handling of the commercial data. TSA revealed that EagleForce obtained commercial data from three commercial data aggregators – Acxiom, Insight America, and Qsent. Specifically, EagleForce provided each of the aggregators a list of names and name variants derived from the PNRs that comprised the sample set of records used for testing (42,000) and requested only certain data elements.³⁵ One of the commercial data providers submitted Social Security numbers (SSNs) due to the way the company packaged its data. Additionally, another commercial data provider submitted longitude and latitude data elements that EagleForce did not request. EagleForce never uploaded the SSNs or the longitude and latitude data elements submitted by the data providers.

Another TSA contractor, IBM, prepared two statistically significant samples of PNRs for the commercial data testing. One sample consisted of approximately 17,000 PNRs drawn from a cross section of air carriers. A second sample consisted of approximately 24,000 PNRs that contained dates of birth. These sample data sets were stored on CD-ROMs,

³³ 70 Fed. Reg. 36320 (June 22, 2005).

³⁴ U.S. Government Accountability Office, *Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information During Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public*, GAO-05-864R, July 22, 2005, posted at <http://www.gao.gov/new.items/d05864r.pdf>

³⁵ 70 Fed. Reg. 36320, at 36322. The data elements received were: first name; last name; middle name; date of birth; name suffix; second surname; spouse first name; gender; spouse first name; gender; second address; third address; plus-four portion of Zip code; address type (residence, business, or mailing address); latitude of address; and longitude of address. Not all of the data providers provided each of these elements.

and TSA hand delivered them to EagleForce along with unparsed copies of other June 2004 PNR data. Although EagleForce received PNR data originally parsed by IBM and TSA, it reparsed the PNR data to pull out the data elements it needed for testing and took the sample data sets and created up to 20 variations of individuals' first and last names, generating about 240,000 name variations derived from the 42,000 names in the two sample sets of PNRs. The Revised Notice stated that the original PIA and SORN had not discussed this process because, "TSA had not developed its test plan with this level of detail at the time the documents were published."³⁶

In addition, EagleForce used certain records obtained from the three commercial data aggregators to enhance the sample PNR data by filling in with missing data. For example, if a PNR in the sample data did not have the subject's full name, date of birth, address, gender, or one of the other fields of data that EagleForce had requested from the commercial data aggregators, EagleForce attempted to pull that data from the commercial data to "enhance" the PNR. EagleForce then produced CD-ROMs containing the enhanced PNRs and provided them to TSA for use in watch list match testing. IBM, as a TSA contractor, was given the CD-ROMs containing the enhanced PNRs for a limited period to determine whether using commercial data to enhance passenger information could lower the number of false positive or false negative matches against the watch list (TSDB). The Revised Notice also revealed that TSA stored the CD-ROMs in a controlled access safe when they were not in use. The PIA assured the public that the information collected had only been shared with TSA employees and contractors with a "need to know" to conduct the required testing, and that "[a]ll TSA contractors involved in the testing of Secure Flight are contractually and legally obligated to comply with the Privacy Act in their handling, use and dissemination of personal information in the same manner as TSA employees."³⁷

As part of the Revised Notice, the revised PIA enumerated a number of data security controls to protect the PNR and commercial data, including: compliance with FISMA requirements; chain-of-custody procedures for the receipt, handling, safeguarding, and tracking of access to PNR data; non-disclosure agreements and document handling training for EagleForce employees; creation of a secure facility to house the testing at TSA's Annapolis Junction, Maryland office; and password protection and secure file cabinets.³⁸

The Revised Notice stated that TSA had determined that the records in the system were covered by NARA General Records Schedule (GRS) 20, which applies to electronic

³⁶ Id., at 36322.

³⁷ Id., at 36323.

³⁸ Id.

files/records created solely to test system performance, as well as hard-copy printouts and related documentation for the electronic files/records. Under GRS 20, an agency may delete or destroy such records when the agency no longer needs them for administrative, legal, audit, or other operational purposes. TSA stated that it had destroyed some of the original PNRs provided by the air carriers and planned to destroy the remaining PNRs and commercial data in its possession or in the possession of EagleForce as testing activities and analyses were completed.³⁹ The Privacy Office understands that the contracts with the commercial data providers require the commercial data to be destroyed when the contracts are completed.

V. Analysis

TSA made efforts to account for the privacy and security of the data it collected and used as part of the commercial data test for Secure Flight, particularly by setting forth strict information security procedures; however, the 2004 notices did not track the changes in the collection and use of commercial data in the test program, primarily because the commercial data test, as described in those notices, did not match the actual commercial data test that was conducted.

The inconsistency between the descriptions in the 2004 notices and what occurred in the actual test was clearly not intentional, but appears to be the result of either a misunderstanding of the test protocols or a change in circumstances between what was intended to be tested at the time the various notices were published and the actual design of the test when it was finalized. The Privacy Office learned during this review that the PIA of the Secure Flight commercial data test was published before the Statement of Work and testing protocols were completed and the initial PIA was not revised as the testing design evolved.

A. No "Firewall"

In its SORN and PIA, TSA repeatedly asserted that it would apply "strict firewalls" between the government and commercial data providers so that no commercial data would enter government space; however, these strict firewalls were based on the notion that the contractor hired to perform the commercial data test would serve as the "firewall" between the commercial data and TSA.

It is understandable how this notion could have developed; EagleForce was contracted to operate the commercial test, but to do so, it needed to obtain commercial data from other companies. It therefore amounted to a "middleman" between TSA and the commercial data. In fact, EagleForce representatives reportedly went to great lengths to prevent TSA staff from accessing the commercial data.

³⁹ Id., at 36324.

The EagleForce contract with TSA contained a standard Privacy Act provision as required by the Federal Acquisition Regulation. This provision states that:

*The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. § 552a) and applicable agency regulations.*⁴⁰

This language is consistent with subsection (m) of the Privacy Act requiring that: "[w]hen an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such a system." In other words, when operating a system of records, EagleForce stands in the shoes of TSA and is obligated to follow the Privacy Act. The fact that EagleForce had access to the commercial data did not create a firewall between TSA and the data, because EagleForce's access to the commercial data amounted to access of the data by TSA.

B. TSA Never Received Authentication Scores and Codes

One of the reasons TSA may have believed that EagleForce would operate as a firewall is that the Secure Flight SORN and PIA stated that a category of records to be collected for the program consisted of "authentication scores and codes." This category suggests that the purpose of using a contractor to conduct the commercial data test would be to insulate TSA from access to any of the commercial data. All that TSA would receive from the commercial data test would be an authentication score (a confidence level for the accuracy of the PNR-watch list matching) or code (indicating the data element against which the PNR did not match).

Whatever the preliminary design of the commercial data test, by the time the contract with EagleForce was finalized, it was clear that TSA would receive commercial data, not merely authentication codes and scores. EagleForce "enhanced" the PNR data with commercially available data in order to expand the information available for watch list matching. For example, if a PNR from the historical data did not have an individual's full name, date of birth, or address, EagleForce extracted this information from the commercial data it had obtained from the three data brokers⁴¹ and enhanced the PNR with these missing data elements in order to increase its reliability when matched against the watch list. EagleForce produced CD-ROMS with the enhanced PNRs and provided those CD-ROMS to TSA for watch list comparisons. The commercial data, part of the "enhanced" PNR, made its way directly to TSA, contrary to the express statements in the Fall Privacy Notices about the Secure Flight program. At TSA, the CD-ROMs were used

⁴⁰ EagleForce Contract at 55.

⁴¹ *Supra* note 35.

by its contractor to analyze whether the addition of commercial data reduced the number of false positives or false negatives in matching exercises against the Federal watch list.

C. *Some individuals whose data was obtained from commercial data brokers had not received notice*

EagleForce augmented the historical PNR with up to 20 variations of the first and last names for each individual whose historical PNR was used in the sample data sets. This was intended to mask the individual identities prior to obtaining commercial data from the three brokers, and so was thought to be privacy enhancing. Unfortunately, because the augmentation process resulted in the creation of names associated with real individuals, EagleForce, and ultimately TSA, obtained commercial data on those individuals as well as on those in the historical PNR.⁴² These additional individuals, therefore, had no notice because the 2004 notices only stated that TSA would collect and use the data of airline passengers that flew during the month of June 2004.

VI. Findings

As ultimately implemented, the commercial data test conducted in connection with the Secure Flight program testing did not match TSA's public announcements. Part of the reason for this discrepancy is the fact that the Fall Privacy Notices were drafted before the testing program had been designed fully. However well-meaning, material changes in a federal program's design that have an impact on the collection, use, and maintenance of personally identifiable information of American citizens are required to be announced in Privacy Act system notices and privacy impact assessments. In addition, not meeting these requirements can significantly impair a program's credibility.

The creation of an effective program requires contributions from operational personnel as well as policy and legal advisors. To be most successful, all groups must have effective communications and coordination. Given the disparity between the published Fall Privacy Notices that explained the commercial data test for Secure Flight and the actual testing program that was conducted, it seems readily apparent that closer consultation and better coordination at key decision points between the Secure Flight program office and TSA legal, policy, and privacy offices was needed. While this may have been due to short deadlines and resource constraints, the end result was that TSA announced one testing program, but conducted an entirely different one.

To TSA's credit, after being informed of this significant discrepancy, TSA revised and reissued the SORN and PIA to reflect more closely the testing program's conduct. Additionally, throughout the commercial data test, TSA made the security of the commercial data a high priority. TSA expressly prohibited the commercial entities

⁴² EagleForce sent the three commercial data providers 240,000 name variations which returned a combined total of 191 million records, many of which, however, were duplicate records.

involved in testing from maintaining or using the PNR for any purpose other than Secure Flight testing, and it instituted real-time auditing procedures and strict rules for TSA access to the data. This was certainly challenging given the complex and changing nature of the program.

Whatever the causes, however, the disparity between what TSA proposed to do and what it actually did in the testing program resulted in significant privacy concerns being raised about the information collected to support the commercial data test as well as about the Secure Flight program. Privacy missteps such as these undercut an agency's effort to implement a program effectively, even one that promises to improve security.

VII. Recommendations

Based on its extensive review of the commercial data test, the Privacy Office offers the following recommendations for Secure Flight. These can also serve as guideposts for any Departmental initiative that involves the collection, use, and maintenance of personally identifiable information:

1. Privacy expertise should be embedded into a program from the beginning so that program design and implementation will reflect privacy-sensitive information handling practices.
2. Programs should create a detailed "data flow map" to capture every aspect of their data collection and information system life cycle. Such an exercise will help produce accurate public documents explaining program compliance with the fair information practices principles of the Privacy Act of 1974, which must guide collection and use of personally identifiable data in the government space.
3. Good communications and collaborative coordination between operational personnel and policy, privacy, and legal advisors are essential in order to ensure that key documents explaining an information collection program are accurate and fully descriptive.
4. Programs that use personal information succeed best if the public believes that information to be collected is for a necessary purpose, will be used appropriately, will be kept secure, and will be accessible for them to review. To obtain such public trust requires the transparency and accountability that can be reflected in careful drafting of publicly available SORNs and PIAs.
5. Privacy notices should be written and published only after the design of a program or a program phase has been fully described in writing and decided upon by authorized program officials;
6. Privacy notices should be revised and republished when program design plans change materially or a new program phase is going to be launched; and

7. Program use of commercial data must be made as transparent as possible and explained in as much detail as is feasible.

VIII. Going Forward

It is the mission and the privilege of the DHS Privacy Office to assist the Department in securing the homeland while protecting individual privacy rights. The Privacy Office works closely with privacy officers in DHS components and directorates and with DHS program staff to provide internal guidance and counsel regarding the collection, use, and maintenance of personal information. We are committed to ensuring that all DHS programs reflect the responsible and respectful use of personal information.

Our role is not only to inform, educate, and lead privacy practice within the Department, but also to serve as a receptive audience to those outside the Department who have questions or privacy concerns about Departmental programs or operations. In this ombudsman-like role, we turn a neutral and critical eye on DHS programs in order to review and respond to complaints, as statutorily required, and to analyze how we as a Department are doing in our efforts to integrate privacy protections into our programs. It was in the spirit of this ombudsman-like function that we undertook this review of Secure Flight. We consider our recommendations as a way to provide effective counsel to TSA, or to any DHS program, to ensure that agency efforts to protect the homeland can be successfully implemented.

We look forward to working with all DHS programs from their earliest inception to ensure that Federal privacy protections are appropriately embedded in DHS initiatives. In that spirit, we are working closely with TSA to provide ongoing guidance on how to build privacy into each step of the Secure Flight Program as it moves forward to address the concerns raised in this review.