Department of Homeland Security
Privacy Office

Report to the Public on Events Surrounding jetBlue Data Transfer

Findings and Recommendations[1]

February 20, 2004

Summary

A potential privacy violation involving the Transportation Security Administration ("TSA") (at the time, a division of the Department of Transportation, now a component of the Department of Homeland Security), was brought to the attention of this office in September 2003. The potential privacy violation involved the transfer of Passenger Name Records ("PNR") from jetBlue Airways to the Department of Defense, a transfer that occurred with some involvement by TSA personnel. While the incidents in question occurred during 2001 and 2002, preceding the creation of the Department of Homeland Security, the matter raises serious concerns about the proper handling of personally identifiable information by government employees now within the Department of Homeland Security. Accordingly, the Privacy Office conducted an investigation of the facts surrounding the transfer of data.

Background

The Department of Homeland Security Privacy Office was established in April 2003, pursuant to Section 222 of the Homeland Security Act, which requires the

[1] The Understanding of Facts and the Findings and Recommendations of this report will remain open for a period of 30 days following the publication of this Report, in order to provide a means of due process to participants who may wish to offer further clarifications, corrections, or otherwise augment the record reviewed by the DHS Privacy Office. If no new material information comes to light within that time, this report shall be deemed final in its current form.

Secretary to "appoint a senior official to assume primary responsibility for privacy policy."[2]

In the course of fulfilling the privacy policy and complaint resolution mandates of Section 222, the DHS Privacy Office receives and responds to complaints and inquiries from Members of Congress, representatives of advocacy organizations, representatives of foreign governments, and the citizens of the United States regarding the operations of the many components of the Department of Homeland Security.

The discovery in September 2003 of a potential privacy violation involving jetBlue Airways ("jetBlue"), the Department of Defense ("DOD"), and, possibly, the Transportation Security Administration, led to numerous inquiries to the DHS Privacy Office from individual members of the public, representatives of advocacy organizations, offices of Members of Congress, and the press, regarding involvement by TSA employees. The incidents in question took place during 2001 and 2002, when TSA was part of the Department of Transportation. However, as of March 1, 2003, the TSA is part of the Department of Homeland Security ("DHS" or "the Department").

Accordingly, the DHS Privacy Office responded to these inquiries with a statement that the DHS Privacy Office would investigate and report on any findings regarding possible involvement by TSA, now-DHS employees in these events. Following is that report.

Methodology

This report is not intended to comment on allegations involving jetBlue's activities or the activities of Department of Defense employees or contractors, which in these circumstances is beyond the statutory purview of the DHS Privacy Office.[3]

---

[2] Such responsibility includes:

(1) Assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;

(2) Assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974;

(3) Evaluating legislative and regulatory proposals involving the collection, use, and disclosure of personal information by the Federal Government;

(4) Conducting a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected; and

(5) Preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls, and other matters.

Homeland Security Act, Section 222; 6 U.S.C.A. § 142 (2003).

[3] The Findings and Recommendations take into account, however, the important role that the DHS Privacy Office should assume in leading discussions about, and the development of, best practices for data sharing

This report reflects the DHS Privacy Office's understanding of the events of 2001 and 2002 concerning the transfer of PNR from jetBlue Airways to the Department of Defense, based on reasonable efforts by the Privacy Office to determine the nature of these events as of February 20, 2004, and lays out specific recommendations, particularly concerning DHS policy on sharing personal data. Should further information come to light regarding these events, this report may be amended and its conclusions altered.

This report is based on a substantial document review by the DHS Privacy Office. These documents were obtained from a variety of sources: documents voluntarily provided by DHS employees and other Federal employees and civilians, documents requested from TSA by the DHS Privacy Office, documents provided by airline representatives and companies involved in these events, and public documents available on the Internet and elsewhere. The DHS Privacy Office thanks the TSA Administrator, the Deputy Administrator, and their staffs, for their assistance in obtaining necessary documents. The DHS Privacy Office further recognizes the work of our colleagues at the TSA FOIA office for their assistance in compiling documents for our review.

The DHS Privacy Office further performed interviews with Department of Homeland Security employees, Department of Defense employees, Department of Defense contractors, jetBlue officials, other persons involved in these events, and citizens who claimed unique knowledge of the events.

This report is based entirely on information culled from these documents and interviews, and to the extent possible, independently verified by other persons with knowledge of these events.

Understanding of Facts

In the fall of 2001, following the horrific events of September 11, 2001, numerous private companies that designed or promoted novel technologies approached various Federal agencies with offers of assistance in the national response to these events and in waging the War on Terrorism. As the Department of Homeland Security did not yet exist, these offers of assistance were fielded by numerous other federal agencies with a nexus to defense, technology, commerce, or counter-terrorism.

One such offer was made by Torch Concepts of Huntsville, Alabama. Representatives of Torch Concepts approached the Department of Defense with an unsolicited proposal involving data pattern analysis, geared towards enhancing the security of military installations throughout the country and, possibly, internationally. To simplify, the proposal suggested that through analysis of personal characteristics of persons who sought access to military installations, the users of such a program might be able to predict which persons posed a risk to the security of that installation. This project

---

between the private and public sectors, particularly in the use of technologies that can have a substantial effect on the privacy of personal information about an individual.

arose out of a desire to prevent attacks on military installation, following the attack on the Pentagon.

Because DOD was interested in this proposal – which subsequently became known as the Base Security Enhancement Program--in March 2002, Torch Concepts was added as a subcontractor to an existing contract with SRS Inc., for the purpose of performing a limited initial test of this technology. A subordinate task order for the contract included a reference to using "P&R"—an erroneous reference to PNR, or passenger name records, as a possible data source for the test.

This reference to "P&R data" suggests that while Torch Concepts developed the idea and method for data analysis, their proposal depended on an outside source of data for operational completeness. Indeed, in seeking to perform testing of their concept, Torch Concepts sought access to a large, national-level database to be used in assessing the efficacy of their data analysis tool for assessing terrorist behavior. During late 2001 and early 2002, Torch Concepts apparently approached a number of federal agencies that operated national government databases containing personal information that Torch believed might be appropriate. These requests did not yield any data. Torch then sought other commercial sources of national characteristics, and began contacting data aggregators and airlines, as it was apparently believed that national airline passenger databases would contain adequate cross-sections of personal characteristics, and that airline passenger lists might yield appropriate analytical information. There are conflicting reports regarding whether the test would simply seek a cross-section of data, whether the test was directly aimed at analyzing information regarding airline passengers traveling within close proximity of a military installation, or whether the test reflected a more equal interest in base and airline security.

Torch Concepts, according to public documents, approached both American Airlines and Delta Airlines, but again their requests were rejected. Torch then sought assistance from Capitol Hill, entreating Members of Congress to intervene on their behalf with airlines or the federal agencies. At the same time, Torch was told by representatives of one or more airlines that the airlines would not engage in such sharing unless the Department of Transportation and/or TSA was consulted and approved of such data sharing.

In April 2002, Torch Concepts contacted the Department of Transportation ("DOT"), and a number of meetings followed during May and June, including meetings with representatives of the DOT Office of Congressional Affairs and several DOT program offices, including offices at the TSA responsible for development of the second-generation Computer Assisted Passenger Prescreening System ("CAPPS II"), and representatives of the Chief Information Officer's ("CIO") office at the Department of Transportation. The TSA Congressional Affairs office was involved due to the Congressional requests. At the time of these meetings, the CAPPS II program was in the most preliminary stages of development, the creation of the program having been announced in March 2002.

In July and August 2002, conversations between DOT, DOD, and Torch Concepts continued. While these conversations reportedly did touch on the concurrent development of CAPPS II, the purpose of these conversations reportedly was not to assist in CAPPS II development, and TSA officials purportedly stated during these conversations that the development of these projects should remain separate. DOT officials appear to have recognized similarities in the large-scale pattern analysis technology between the proposed CAPPS II and the technology offered by Torch, but that while the technology was similar, it was not precisely what was anticipated for CAPPS II. Thus, while they were interested in the results of the testing, it was not performed for their benefit or the benefit of the CAPPS II program. DOT/TSA officials purportedly made it clear in these meetings that the Torch Concepts project was necessarily separate from CAPPS II development, given the sensitivity of the impending contracting process associated with that program.

As a result of these meetings, DOT/TSA officials agreed to assist the DOD-Torch project in obtaining the consent of an airline to share passenger data for the purposes of the Base Security Enhancement project. TSA officials contacted jetBlue Airways in New York, and began conversations with jetBlue regarding this project. TSA officials state that their understanding at this time was that the technology was intended to flag potential terrorists arriving by air in the areas near military bases. However, documents produced by DOD reflect a more general "base security" purpose. While one form of base security may have included preventing terrorist attacks by air directed at military installations, the overarching purpose was the prevention of unauthorized or unwanted entry onto military bases via a variety of forms of entry.

As a result of these conversations, on July 30, 2002, a relatively new employee of TSA sent jetBlue a written request that jetBlue provide archived passenger data to the Department of Defense for the Base Security Enhancement Program. This request does not appear to have been approved or directed by senior DOT officials. This request by TSA to jetBlue to retrieve personal records from its database and to share such data with DOD was significant, particularly as no airline had otherwise previously agreed to share data directly with DOD.

In August 2002, Torch Concepts was informed by Acxiom Corporation ("Acxiom"), a data aggregator serving as a contractor for jetBlue, that Torch would receive data from jetBlue; in September 2002, data was transferred from jetBlue to Torch Concepts. It is not clear the entire range of data elements that was included about each passenger, but, at a minimum, name, address, telephone, and some itinerary-related information was included. A total of five million records, representing over 1.5 million passengers, were transferred. The actual transfer of the data, was, in fact, accomplished between Acxiom (acting as a contractor for jetBlue) and Torch Concepts.[4] There does not appear to have been any fee paid by Torch Concepts for the transfer of the jetBlue passenger data. In October 2002, Torch Concepts separately purchased additional demographic data from the data aggregator, Acxiom.

[4] It should be noted that Acxiom later became a contractor for the CAPPS II program, but was not involved in CAPPS II at the time of this data transfer.

Torch Concepts documents reveal that the "five million P&R" (sic) records were inadequately diverse, as the passenger data on this airline represented only certain regions of the country and a limited flight pattern. The data is described in Torch Concepts document as "tourist-like passengers" with "limited origins and destinations," and lacking "passenger travel history." The demographics data purchased from Acxiom further revealed passenger name; gender; home specifics—whether a renter or owner; years at current residence; economic status/income; number of children; social security number; number of adults in household; occupation; and vehicles owned.

Torch Concepts used the Acxiom and jetBlue data to perform tests of the base security system. In doing so, Torch "de-identified" the data, or stripped it of name and other unique identifiers. According to Torch Concepts, all jetBlue data received for these tests were later destroyed, and hard drives containing any residual data were removed from use and given to legal counsel for safekeeping.

In spring 2003, Torch Concepts representatives appeared at a conference on homeland security technology in Alabama. This Southeastern Software Engineering Conference was sponsored by the National Defense Industrial Association (it has been incorrectly reported that this event was sponsored by the Department of Homeland Security). While the date on Torch Concepts' PowerPoint presentation was February 25, 2003, Torch Concept representatives state that the conference actually occurred in April. The presentation given by Torch Concepts at the Southeastern Software Engineering Conference revealed information previously set forth in this Report, and also included a chart of "anomalous demographic information for one passenger." This PowerPoint slide revealed, apparently without name, a number of addresses and social security numbers associated with one traveler. The concept for this presentation was entitled "Homeland Security Airline Passenger Risk Assessment." The focus of this presentation was not the Base Enhancement project that was the initial purpose of the project, but rather, a process of analyzing passenger demographics for risk assessment. The presentation concluded that "several distinctive travel patterns were identified," and that "demographic groupings appear common to each," and that "known airline terrorists appear readily distinguishable from the normal jetBlue passenger patterns." Further, the presentation stated that "if a more comprehensive P&R (sic) data base were available, it is expected that analysis could identify and characterize all normal travel patterns."

It should be noted that DOD, TSA, jetBlue, and Acxiom do not appear to have been aware of this presentation at that time; the relevant parties neither participated in preparing the presentation, nor did they give their permission for the personal data disclosed in the Torch Concepts PowerPoint presentation. Of particular note, this presentation reveals that Torch Concepts believe it was "promised" the same data as was being used for CAPPS II. Upon clarification, Torch officials state that this comment meant that they understood they would receive PNR. Other parties to the conversations between DOT and Torch Concepts do not recall that any such promise relating to CAPPS II was made, particularly given the early stages of the CAPPS II program development at that time.

Almost a year after the data transfer, in the summer of 2003, DHS officials and others separately acknowledged that jetBlue had further agreed to test TSA's CAPPS II system. TSA employees had substantial communications with jetBlue, and a number of other airlines, throughout the development of the CAPPS II system. jetBlue, in particular, expressed an interest in participating in preliminary tests of this system for a variety of reasons, including a willingness to support homeland security efforts, given the impact of September 11, 2001, on their home base, New York. Further, jetBlue believed that its customer base was (and continues to be) disproportionately affected by the operation of the current CAPPS I system, which targets for secondary screening a number of behaviors which may be common to jetBlue customers.

During 2003, there were substantial delays in implementing testing of CAPPS II, including, not insignificantly, a realization by TSA employees during this period that the jetBlue privacy policy prevented such data sharing, and that jetBlue would need to take affirmative action to amend such policies before any testing began.

In late September 2003, members of the public, seeking to halt jetBlue's reported involvement in testing the CAPPS II system, engaged in substantial research regarding jetBlue's public activities. These parties were easily able to obtain the above-referenced PowerPoint presentation, which was available on the Internet at that time, and publicly alleged an improper data transfer to the Federal government of significant size and impact. In response, jetBlue Chief Executive Officer David Neeleman released a public statement that "Although I had no knowledge of this data transfer at the time it was made, I accept full responsibility for this action by our company." Further, Mr. Neeleman, while recognizing that the data transfer was a violation of the company's privacy policy, stated that "I can understand why the decision was made to comply with this request … in the wake of the September 11 attacks, and as New York's hometown airline, all of us at jetBlue were very anxious to support our government's efforts to improve security." In response to this disclosure, jetBlue stated publicly that it would not engage in any testing of the TSA's CAPPS II program.

With these revelations, the DHS Privacy Office began its investigation. The DHS Privacy Office has been in contact with representatives of TSA, DOT, DOD/Department of the Army, jetBlue, Acxiom, Torch Concepts. The DHS Privacy Office has participated in meetings on Capitol Hill, and has been contacted by staff of Members of Congress interested in the investigation, as well as members of the advocacy community and the press. The DHS Privacy Office has kept the DHS Inspector General apprised only of the existence of this investigation, but not its findings, until shortly in advance of the publication of this report.

In addition to the above, it is important to note what was not found. There is no evidence that jetBlue or Acxiom provided data directly to TSA or DOT in connection with these events. On the contrary, numerous parties confirmed that the data was provided by jetBlue (through its contractor, Acxiom) to Torch Concepts. Further, there is no evidence that Torch Concepts or DOD shared results of this testing directly with

DOT/TSA, or that DOT/TSA officials had specific knowledge of the exact purpose for or scope of the testing that was to be performed. There is no evidence at this time that DOT/TSA facilitated the sharing of data for this project from any other airline or other source. There is also no evidence that any privacy policy or Privacy Act impact was discussed in the meetings between DOT, DOD, and Torch Concepts.

The DHS Privacy Office is aware that TSA, while part of DOT and also while part of DHS, separately sought data from several airlines for the purpose of testing CAPPS II, and, that while initially several airlines expressed interest in sharing data, these offers were later rescinded. At this time, there is no evidence that CAPPS II testing has taken place using passenger data.

Findings

Although the events giving rise to the data transfer occurred in 2001 and 2002, prior to the establishment of the Department of Homeland Security, TSA, formerly within the Department of Transportation, is now a component of DHS. Accordingly, the Privacy Office devoted significant resources to examining this incident in an effort to understand precisely what occurred and why. Further, the Privacy Office will continue to devote significant attention to the establishment of internal controls and procedures to ensure that future activities of the department are guided by clear principles for the responsible use of personal information.

In connection with events that occurred in 2002 involving jetBlue, DOD, and TSA, the Department of Homeland Security Privacy Office finds that:

1. No Privacy Act violation by TSA employees occurred in connection with this incident. There is no evidence that any data were provided directly to TSA or its parent agency at the time, DOT. On the contrary, the evidence demonstrates that passenger data were transferred directly by jetBlue's contractor, Acxiom, to Torch Concepts. As a result, the Privacy Act of 1974, which regulates the Federal Government's collection and maintenance of personally identifiable data on citizens and legal permanent residents, does not appear to have been violated by TSA actions. Because TSA did not receive passenger data, no new system of records under the Privacy Act was established within TSA, nor was any individual's personal data used or disclosed by TSA, its employees or contractors, in violation of the Privacy Act.

2. The primary purpose for the data transfer was the "Base Security Enhancement Project." While the knowledge gained from testing the pattern analysis technology proposed for this project may have ultimately benefited other data analysis programs, including TSA's CAPPS II, such benefit was not the stated purpose of the base security enhancement project.

3. TSA employees were involved in the data transfer. Both documentary and verbal evidence indicate that TSA employees both facilitated contacts between the airline and DOD and failed to identify the privacy policy and privacy impact on individuals whose information might have been shared with the Department of Defense or its contractors.

4. TSA participation was essential to encourage the data transfer. As several airlines had refused to participate in this program absent TSA's involvement, it appears that, *but for* the involvement of a few TSA officials in these events, the data would likely not have been shared by jetBlue with the Department of Defense and its contractors.

5. The TSA employees involved acted without appropriate regard for individual privacy interests or the spirit of the Privacy Act of 1974. In doing so, it appears that their actions were outside normal processes to facilitate a data transfer, with the primary purpose of the transfer being other than transportation security. Such sharing exceeds the principle of the Privacy Act which limits data collection by an agency to such information as is necessary for a federal agency to carry out its own mission. While these actions may have been well intentioned and without malice, the employees arguably misused the oversight capacity of the TSA to encourage this data sharing.

Recommendations

1. *Corrective Action.* The TSA employees involved, must, at a minimum, attend substantial Privacy Act and privacy policy training and must certify such training to the satisfaction of the DHS Privacy Office.

2. *Referral to the Inspector General.* It is beyond the scope of the Privacy Office to determine whether these employees may have otherwise exceeded the normal scope of TSA operations. The above findings will be referred to the Department of Homeland Security's Inspector General for further review. After reviewing the results of the Chief Privacy Officer's report and the Inspector General's report, if any, other remedial action may be recommended if appropriate.

3. *Comprehensive Privacy Training.* This incident underscores that additional and systematic training is needed. The DHS Privacy Office has been analyzing current training efforts in an attempt to formalize privacy education and training across the Department. This process will continue. The DHS Privacy Office also encourages each directorate or related agency, such as the TSA, to evaluate its systemic education and training programs for new and existing employees.

4. *Establishment of Guidelines for Data Sharing.* While existing Privacy Act processes require government contractors to abide by Privacy Act rules, this matter presents a somewhat new situation involving cooperative sharing of data between the private sector and the federal government for security purposes. The DHS Privacy Office has begun, and will continue to establish clear rules for voluntary and compulsory data sharing with private-sector entities. Such rules will include (1) adequate oversight of such data sharing by senior officials of DHS agencies; (2) adequate review of the controlling private-sector privacy policies and applicable laws; and (3) documented compliance with the Privacy Act of 1974, among other matters.

Signed on this Day: _____

_____
by Nuala O'Connor Kelly
Chief Privacy Officer
U.S. Department of Homeland Security