

Admiral David Stone's Answer to Question #16 of Governmental Affairs Pre-hearing Questionnaire

16. According to press reports, American Airlines authorized its vendor, Airline Automation, to provide TSA with one week's worth of Passenger Name Record ("PNR") data on its customers. The vendor then reportedly provided the data to four companies competing for contracts with TSA: HNC Software, Infoglide Software, Ascent Technology, and Lockheed Martin.
- a. Did any TSA official ask American Airlines or its vendor to provide PNR data to the agency or to any of the four companies? If so, why?

Answer: In early 2002, the Transportation Security Administration (TSA), at the direction of the Deputy Secretary of Transportation, started to work with the DOT's Office of the Chief Information Officer to begin examining the feasibility of a successor system to the Computer Assisted Passenger Prescreening System (CAPPS). CAPPS was previously developed by Federal Aviation Administration (FAA) and currently is operated by the domestic airlines. The successor system, known as CAPPS II, was contemplated as a risk assessment system that ultimately would be owned and operated by the government. As a precursor to building such a system, TSA decided to enlist the assistance of private sector firms with risk assessment expertise in a proof of concept exercise. The purpose of this exercise was not to develop an operation-ready system for purchase by TSA, but to prove the feasibility of the concept of performing a risk assessment, based on airline reservation information.

On March 8, 2002, the FAA, on behalf of TSA, issued a Broad Agency Announcement (BAA) soliciting proposals for the development of a Risk Assessment Engine (RAE) prototype that would be capable of assigning risk to such areas as passengers, flights, airlines, and airports across the nation. Among the eligibility criteria specified in the BAA was the requirement that companies demonstrate their ability to link with airline computer reservation systems and extract passenger name records (PNR) for risk assessment.

In anticipation of awarding cooperative agreements to qualified firms, TSA took steps to ensure that the cooperative agreement recipients would have a single set of PNRs to work with in demonstrating the feasibility of the RAE concept. To that end, TSA began discussions with Airline Automation, Inc. (AAI), which managed PNRs for a number of large domestic airlines, including American Airlines (American) and Continental Airlines (Continental).

On May 8, 2002, TSA and FAA entered into cooperative agreements with HNC Software, Infoglide, Ascent Technology, and Lockheed Martin (the cooperative agreement recipients) to develop RAE prototypes. TSA planned to evaluate the prototypes as candidates for further use as a component of CAPPS II. During the course of the performance of the cooperative agreements, some of the recipients

told TSA they had difficulty in obtaining access to PNRs in order to demonstrate the capabilities of their prototypes to interface with airline reservation systems. This provided further impetus for TSA to arrange for the cooperative agreement recipients to have access to a single set of PNRs for purposes of the proof of concept.

To achieve this goal, TSA contacted American on May 20, 2002, and Continental, on May 22, 2002, to request that they each authorize AAI to provide PNRs to the cooperative agreement recipients for purposes of developing the RAE prototypes. American authorized AAI to provide PNRs for this purpose, but Continental did not. AAI, therefore, did not provide PNRs from Continental. AAI provided American PNRs to the cooperative agreement recipients on March 24, 2002, in a format that was not usable. AAI subsequently made American PNRs available to the cooperative agreement recipients and to TSA by loading them on a secure server in June of 2002. The cooperative agreement recipients used the PNRs in order to perform the RAE proof of concept. TSA never accessed the PNRs on the secure server. However, during the demonstrations of the RAE prototypes put on by each cooperative agreement recipient, TSA officials viewed presentations that included PNR data as part of the demonstrations. Confidentiality of PNRs was protected under non-disclosure agreements entered into by the various parties. I understand that PNRs used in connection with performance of the cooperative agreements have been returned, destroyed or otherwise secured.

During the course of performance of the cooperative agreements, some of the cooperative agreement recipients independently obtained PNRs other than the American PNRs supplied by AAI. The independent sources of PNRs that TSA is specifically aware of are: Delta Air Lines (through Delta's Airline Reservation System); Continental, America West Airlines, and Frontier Airlines (through EDS/Shares); JetBlue (through Acxiom); Galileo International; and possibly Apollo; TSA did not have access to these PNRs.

b. How did TSA and/or the companies use the data? Was it for a CAPPS II-related purpose?

Answer: In the initial stages of examining the feasibility of developing a successor to CAPPS, TSA decided to enlist the assistance of private sector firms with risk assessment expertise in a proof of concept exercise. The purpose of this exercise was to prove the feasibility of performing a risk assessment for passengers, based on airline reservation information. Ultimately, the successful demonstration of such a process could lead to the development of a commercial product that would become part of CAPPS II.

Although TSA had access to PNRs that AAI placed on a secure server, TSA never actually accessed them, and therefore, did not use PNRs for any purpose. However, during the demonstrations of the RAE prototypes put on by each cooperative agreement recipient, TSA officials viewed presentations that included PNR data as part of the demonstrations. The cooperative agreement recipients

used PNRs to develop their RAE prototypes in furtherance of their cooperative agreements with TSA.

- c. Which, if any, of the four companies possessed PNR data while performing contract work for TSA? If so, was the work related to CAPPS II?

Answer: For purposes of developing a risk assessment prototype, the four companies were working with TSA pursuant to cooperative agreements, not contracts. The purpose of TSA's relationship with these four companies was not to contract for the procurement an operation-ready system. As a precursor to any government contracting effort, TSA sought to research the feasibility of performing a risk assessment for passengers using airline reservation information as the basis for the assessment. Ultimately, the successful demonstration of such a process could lead to the development of a commercial product that would become part of CAPPS II. In the course of performing under the cooperative agreements, all four cooperative agreement recipients possessed PNR data.

- d. Did TSA or any of the companies create a system of records as defined by the Privacy Act (5 U.S.C. 552a(a))? If not, please explain how the collection and use of the information does not meet the Act's definition of a system of records.

Answer: My understanding is that at the time that TSA was involved in ensuring that cooperative agreement recipients had access to passenger name data (PNRs), which was prior to the existence of DHS, personnel at TSA evaluated the matter and believed that their actions were fully in compliance with the Privacy Act. No System of Records Notice was written. TSA facilitated the transfer of the PNR data to be used as a data set, rather than to be retrieved by name or personal identifier. The data set was to be used for the purpose of testing the functionality of a "Risk Assessment Engine Prototype" for identity-based security threat assessment technologies. Since the information was not to be accessed or retrieved by name or personal identifier to make individual determinations, TSA believed that it did not need to publish a system of records notice under the Privacy Act. Additionally, they believed that even if testing constituted a Privacy Act system, it could be covered by a pre-existing system of records applicable to the program.

I appreciate that since the time of TSA's assessment, further questions have been raised about these PNR transfers. Also since that time, DHS was established by Congress and TSA, formerly under the Department of Transportation, became a component agency of DHS. As you may know, the Chief Privacy Officer at the Department of Homeland Security has initiated a comprehensive examination of the circumstances surrounding TSA's involvement in the data sharing from airlines that took place before TSA's integration into DHS. I fully endorse this examination for the lessons that can be learned and I am assisting in every way possible. Based on that review, I commit to you that I will use my leadership role

to expeditiously take appropriate steps as warranted. On that note, let me further assure you that as Acting TSA Administrator, with the fullest support from Secretary Ridge, Deputy Secretary Loy, and Under Secretary Hutchinson, I tasked a senior level TSA team to begin intensive efforts for TSA-wide privacy training. I have also hired a TSA Privacy Officer to assist with all TSA privacy related policy and program reviews, in collaboration with the DHS Chief Privacy Officer. All of these initiatives have been accomplished, with full participation by TSA staff. I have the highest confidence in my senior management and staff, and I commend their ongoing positive reception of privacy compliance and sensitivity as integral to carrying out TSA's part in the Department of Homeland Security mission. It is one of many reasons why, if confirmed, I look forward to leading the TSA team within the Department of Homeland Security.

- e. TSA has requested PNR data from JetBlue (on behalf of an Army contractor) and from American Airlines. Has TSA requested that any other airlines provide PNR data?

Answer: As discussed below, TSA requested PNR data from three other companies unconnected to specific investigations: Continental Airlines, Delta Air Lines, and Sabre. In addition, in the spring of 2003, TSA obtained PNRs from JetBlue in order to determine whether changes could be made to the CAPPs system that would address what appeared to be a disproportionate impact of that system on passengers of certain airlines. TSA used the information contained in the PNRs supplied by JetBlue to test the application of a modified risk assessment algorithm for CAPPs. The PNR data was not provided to any other party. TSA has retained the PNRs because of a pending FOIA request that is broad enough to encompass this data.

On May 22, 2002, TSA requested PNRs from Continental Airlines for use by the cooperative agreement recipients in developing RAE prototypes. Although TSA and Continental executed a non-disclosure agreement in contemplation of Continental providing PNRs for this purposes, Continental ultimately did not provide any PNRs.

In February 2002, TSA directed Delta Air Lines to provide PNRs to the U.S. Secret Service in connection with security preparations for the Salt Lake City Winter Olympics, which was a National Special Security Event. The U.S. Secret Service used the PNRs (transmitted through ARINC) to alert the agency to the travel plans of individuals of known protective interest. The records were stored in a stand-alone computer located at the Intelligence Division Duty Desk. Although a non-disclosure agreement signed by Delta Air Lines and USSS stated that PNRs might be disseminated to InRange Technologies Corporation, PNRs were not shared with any parties outside the U.S. Secret Service and were disposed of after the event.

In February 2003, TSA requested PNRs from Delta Air Lines for use by IBM Global Services, which was under contract to TSA to develop an airline data

interface that would serve as the conduit through which PNR data would flow between the CAPPs II risk assessment engine and the airlines. On February 27, 2003, Delta transmitted an unknown number of what TSA and IBM thought were actual PNRs, but that Delta has since advised were artificial PNRs created by Delta engineers. On March 3, 2003, Delta requested that the data be deleted, and that request was honored that same day.

In May of 2003, TSA received a computer disk containing an unknown number of PNRs from Sabre in contemplation of using them to test existing components of the CAPPs II system. TSA returned the disk in September of 2003. While the disk was in TSA's possession, no one read the PNRs or otherwise attempted to obtain access to any information on the computer disk.

- f. How does TSA plan to obtain PNR data to test CAPPs II? Is it considering promulgating new rules or issuing a security directive?

Answer: TSA plans to use the Notice of Proposed Rulemaking (NPRM) vehicle to seek public comment on the collection of Passenger Name Record (PNR) data for the operation of the CAPPs II program, and would likely issue an order compelling the collection of historical PNR data for testing purposes simultaneously with publication of that NPRM. Each of these documents would require regulated parties to take reasonable steps to ensure that passengers are provided notice of the purpose for which the information is collected, the authority under which it is collected, and any consequences associated with a passenger's failure to provide the information.

- g. When will CAPPs II testing begin and what safeguards could you put in place to ensure that the PNR data collected for testing purposes will be handled in a way that protects the privacy of airline passengers?

Answer: TSA is currently working with a number of contractors, privacy advocates and other stakeholders as well as meeting internally to discuss the data security and integrity aspects of CAPPs II. We are ensuring a very deliberative process to make certain that both the Information Technology as well as the Policy components are well-planned before any testing of the system is considered.

Currently, only TSA personnel and entities holding Top Secret level clearances and have a strict "need to know" will be considered for access to the CAPPs II system. All personnel and/or entities requiring access to the system will be vetted by the TSA and a risk assessment will be conducted on all individuals intending to connect to the system. Further, all entities will be subject to a Memorandum of Understanding (MOU) outlining roles, responsibilities, rules of behavior and consequences resulting from non-compliance with the MOU with respect to access to the system. To ensure compliance with the MOU and other agreements, extensive oversight, monitoring, and auditing of the system will be conducted by

the Office of National Risk Assessment (ONRA) Information Systems Security to ensure compliance with established system rules of behavior.

The Information Systems Security Officer (ISSO) will preside over all the auditing and information systems, ensuring compliance with the above-mentioned standards of protection. In addition the ISSO will provide for the protection of information systems against unauthorized access and ensure that safeguards are implemented for the protection of the integrity, availability, and confidentiality of Information Technology resources.

One of the auditing safeguards that TSA will rely upon for CAPPS II is software called Radiant Trust™. Radiant Trust™ maintains audit trails of who accessed the system and the time/date as well as keeping records of all system activity. Working with other security programs, Radiant Trust™ will detect any security violation, performance problems and flaws in applications. Furthermore, the system access controls on Radiant Trust will be strict. A two-person approval process will be necessary to ensure that access is given to authorized personnel only.

CAPPS II testing will not begin until security systems to ensure protection of the data are fully in place.

h. Do you agree with the steps TSA has taken thus far to secure PNR data to develop or test CAPPS II?

Answer: To date, TSA has not secured PNR data to test CAPPS II. As noted in my responses to Question 11 above, there are a number of formal steps that we must go through before we are in a position to receive PNR data. We are also currently developing our security program to ensure the integrity of the data once it is collected. Until we are confident that both the security system and redress procedures meet privacy and security muster, we have no intention of collecting PNR data for any reason.