

# 14

## **Airline Industry Security**

Mark Prisman and David Johnston

### **Introduction**

The events of September 11, 2001 have brought about a very controversial issue regarding what is more valuable to society, privacy or security. Visions of two turbojet airliners crashing into the twin World Trade Center buildings in New York, combined with the fires started by another jet at the Pentagon, and the crashed jet liner in Pennsylvania all remain clear in the minds of our society. The events, transmitted through television, pictures and newspapers, have left an enduring fear. According to a recent Associated Press poll, 98% of Americans surveyed remembered exactly what they were doing on 9/11 when the hijackers flew jetliners into the World Trade Center (Dow Jones Newswire 2004, p. 1). In the post 9/11 era, means have been justified for doing whatever it takes to protect our nation from further terrorist attacks. However, on some levels this has meant an invasion of privacy which some citizens have become increasingly skeptical about. Before diving into these issues, the business implications the airlines have faced in recent years must be addressed and considered.

### **Overview of the Business Environment**

The airline industry works similarly to any other for-profit industry: costs need to be minimized, revenue needs to grow, and debt must be financed as cheaply as possible. In the aftermath of September 11, the major airline carriers United, American, and US Airways have all filed for bankruptcy. The main driving factors behind these bankruptcies included cost of security, fear of litigation by the families of those who perished on 9/11, and a decrease in demand for airline services. The airlines have been forced to raise costs in order to increase security personnel and other security upgrades along with the extra

costs of protecting itself from lawsuits. Declining revenue, as a result of decreased demand based on customer fear of traveling after September 11<sup>th</sup>, also has accelerated the descent of the largest airline carriers into the red. Also, airline corporate bonds have been reduced tremendously, making capital more expensive to acquire for airline companies. Lastly, security costs have increased for airline companies at a staggering rate and currently show no sign of relenting.

Historically, airlines had decided to outsource security since these services were expensive and not part of the core-competencies of many of the major airlines (Paul Seidenstat 2004, p. 280). As these services were outsourced so was the airline's commitment to providing the level of security that would be needed on September 11<sup>th</sup>. According to Paul Seidenstat, a professor of Public Finance and Management from Temple University, a significant gap existed between what screeners' job required of them and the training they received to perform those services. On top of poor training, screeners had tedious work, limited opportunities of promotion, and wages that were unusually low. This led several analysts to comment that retention of screeners was becoming increasingly difficult because screeners could quit and work at an airport fast food restaurant for higher wages (Paul Seidenstat 2004, p. 283).

It became obvious after the terrorist attacks that radical sweeping changes were needed to improve security throughout the airline sector with a major focus on airport security. The government appeared to be the authoritative factor the airlines desperately needed to decrease security costs and litigation. Through legislation, airline companies received financial backing, and the government took temporary control over many essential security duties across the nation's major airports. But this approach irritated customers as unpredictable waits turned some customers to look for other means of transportation. Also, issues of privacy quickly became a concern aimed at the government for several reasons due to distrust over personal information being shared with other entities without any control or knowledge of it. Many people believe government, public and private industries have not taken into consideration the privacy concerns of flying travelers. The degree of privacy a citizen is willing to exchange in order to travel has become the leverage point between privacy information needed to combat terrorism and the travelers' right to keep that information secret.

To protect the airline industry from vanishing, the U.S government created legislation to protect the airlines from possible lawsuits stemming from September 11<sup>th</sup>. Shortly after the attacks congress established the "seven billion dollar victims' compensation fund" and created additional red tape structures in order to discourage potential lawsuits. To date, 98% of victims have chosen to accept payment from the compensation fund rather than take the companies to court (Filipov et al. 2004, p. 2). The action of the U.S government in this particular case suggests a future proactive role of the government in protecting the airlines. However, because the government has stepped in and helped pay out damages by means of the victim's fund, the airlines involved in September 11<sup>th</sup> are being held less responsible, which possibly leads to less motivation for security changes within the industry. So a question that needs to be addressed is whether or not airline companies will

substantially change their mentality toward providing security measures if the perceived threat of financial harm due to a breach in security is less than the cost of providing these security services?

Although it appears that the U.S. government alone should shoulder the responsibility of public safety in flights, litigation has still proven to airline companies that the cost of neglecting any security is far greater than the cost of providing additional security. For example, Israel, a country under immense threat of terrorism, has proven that additional security costs are well worth the investment. Over the last few years, Israel has had a thriving airline industry while creating a security mechanism that has been able to prevent potential terrorist attacks coming into and out of the country (Robert Colman and David Fletcher 2003).

Even three years after 9/11, many airlines still have not been able to rise out of bankruptcy. It seems that, if airlines are to become profitable in the future, they will have to analyze the trade-offs between the high costs of security and the overall quality (timeliness) of the service delivered. In other words, the value proposition delivered to traveling customers must now focus on speed of service along with strict security measures. Combining these measures is becoming the most challenging and most rewarding models for differentiation in the airline industry today.

### **Frictionless Travel**

Anyone who has traveled commercial airlines knows how much of a time consuming process it can be to simply board the plane. During the 1990's, Delta Airlines and other carriers began a quest towards what they called "frictionless" travel. This included the development of curb side check-ins, Internet boarding passes, self-service ticketing kiosks and other time efficient innovations designed to simplify the travel experience. The near future called for "virtual airports" where passengers would be able to bypass ticket counters completely. The idea being developed at the time was for passengers to be able to buy tickets online and receive their seat assignments, and then print their own boarding passes from their home computer. A frequent flier program was being developed that allowed frequent fliers to use SkyMiles cards as boarding passes while being able to check in for flights through their cell phones. However, the events of September 11<sup>th</sup> halted the development of these ideas (Hirschman 2001).

The terrorist hijackings led to serious reconsiderations within the airline industry of when to continue with such simple means by which passengers could board an airplane. First, another issue had to be dealt with which involved figuring out what kind of person might be trying to board an aircraft (such as a possible terrorist). It was this change in mentality that has brought about new proposals and development towards the future business of airline security. So the challenges of the airline industry did not completely change but rather evolved into something bigger. Not only were there incentives to create a time-efficient process, but there were also incentives to somehow identify what kind of person was going to be boarding the plane. So, the current challenges being faced by airline security include to not only streamline

the process and eliminate long lines but to provide advanced security checkpoints to prevent further terrorist attacks.

Can high-tech tools directed towards simplifying travel and eliminating long lines coexist with proposed future airline security measures? An idea has been put forth by Northwest airlines to leverage frequent flier databases to the FBI's list of suspected terrorists so law enforcement can identify who is traveling at any time. This idea will allow participants in the program to be quickly sent through the screening process (Hirschman 2001).

### **Registered Traveler Program**

The Registered Traveler Program is being set up by the Plano-based Electronic Data Systems Corporation and Unisys Corporation in an effort to provide frequent fliers a shorter security process at the airport. The main initiative underlying the program is to get frequent fliers to volunteer for a criminal background check in exchange for a shorter security process at the airport. The program will require for a fingerprint and iris scan to be taken at the security stations to confirm identities. After the participants' identities are verified, they are allowed to pass through quicker security with lighter inspections. This program will essentially speed up airport traffic while letting guards spend more time screening people who are not providing extensive background checks (Harrison 2004).

To qualify for the program, the participant must be a frequent flyer of the participating airline and must travel at least once a week out of the selected airports. Participants will provide the Transportation Security Administration (TSA) with their name, address, phone number and date of birth and a fingerprint and iris scan. This data will be used by the TSA to check for police and other intelligence data on the passenger. Once approved, the participant will gain the priority to enter a special security lane at the airport. The passengers will still have to forego a metal detector but they will not be selected at random for a deeper search (Harrison 2004).

EDS is working with American Airlines Inc. to test the program at Boston Logan International Airport and Ronald Reagan Washington Airport under a \$1.31 million contract. Unisys' is running a similar test program under a \$2.47 million contract at George Bush Intercontinental Airport in Houston, along with the major airports located in Minneapolis-St. Paul and Los Angeles. Under these pilot programs every aspect from customer service to security is being assessed by the TSA. If the tests are successful, which is widely expected, the program is expected to go nationwide sometime in 2005 (Wilcox & Woods 2004). With the rollout of this program in the near future, a question arises of why privacy advocates are becoming increasingly concerned about its nationwide implementation and whether or not more people should be worried.

Currently, the Registered Traveler Program revolves around the use of a smart card that identifies a person to his/her fingerprint or iris scan. The smart card holds key information trackers on the card and uses these biotechnologies to check the passenger to the trackers. It has been reported that fingerprinting or iris scanning when used by the program has proven to be problematic in identifying individuals to the

smart card data. However, when the two security technologies are combined the probability of false negatives greatly decreases (John Croft 2004).

Privacy advocates have raised concerns about possible data that may be included on the card in the future. Consider, for example, that when registering for the Registered Traveler Program, the government also checks one's past criminal records. In the near future, this may indicate that airlines will begin barring convicted criminals of flying simply because the airlines are concerned about the safety of the flight. Over time, airline companies may even add value to the overall customer base by providing discounted prices for non-risk flyers, which discriminates against those passengers the airlines feel are a threat. Since differential prices based on customer preferences and profiles have in recent past become the norm, a scenario such as this should not seem too far fetched. Added benefits to the airlines include the use of collected data to provide value added services tailored to individual customers. For example, airlines could provide magazines that advertise heavily in optical lenses to a passenger who may have problems seeing. The ethical line is hard to draw when the apparent benefit to travelers, airline companies, and the government appear to be so high.

### **Exploitation of the Current System**

Questions remain about the use of data collection and distribution by the airlines. In the past, airlines have been more than willing to transfer data over to any government agency that has a perceived need of access. Recently, this has included government organizations such as NASA for unknown reasons. Unlike many other industries, privacy information can either be volunteered or forced by a subpoena from the government. Thus, issues of business propositions facing the airlines to sell away privacy data to commercial companies appear to a future concern.

Before the registered program began testing, a couple of attempts were made to expand government databases, in hopes of identifying terrorists before they boarded the plane. CAPPS II was the first of these programs that was to be initiated and implemented. CAPPS II stands for Computer Assisted Passenger Prescreening Program. The idea around the CAPPS II program was that by checking each passenger's address, name, phone number and date of birth, the airline could verify that the passenger was who they claimed to be (Wall Street Journal 2004, p. 10). Another aspect of this program allowed the airline to check the passenger against government databases and examine any connections to terrorist organizations that would alert the government and allow them to take preventative action. One of the largest problems facing the CAPPS II program regards the action the airlines would undergo when finding a suspicious traveler. In many cases, the airlines did not report the match to the government and in other cases the airlines did not properly remove the person from flying. CAPPS II ultimately met its demise when privacy advocate groups attempted to weigh down the airlines from privacy infringement lawsuits (*Wall Street Journal* 2004). Because the benefits of the program were overshadowed

by the costs due to these lawsuits, the program was abandoned by the airline companies.

As quickly as CAPPs II was abandoned, the government stepped up its use of the “no-fly list”. Like the CAPPs II, the no-fly list is intended to prevent potential terrorist attacks by checking travelers against a list of known terrorists. In stark contrast to CAPPs II, the no-fly list grew from 16 people in 2001 to over several thousand in 2004 (*Wall Street Journal* 2004, p. A10). In the no-fly lists case, it is important to note the shifting of responsibilities from corporate background checks to the government taking over the burden of verifying the passenger. Recently, a new program by the name of Secure Flight has emerged. The focus of this program is to expand airline-provided information to include additional items received in given months. The program will work in conjunction with the no-fly list but will delve deeper into a variety of data previously not available to be acquired through the CAPPs II program. Additional items included are forms of payment, travel itineraries, reservation dates, and traveling partners identified by bought tickets (*Information Week* 2004, pg 28).

There is a blurred line being drawn by the government. While corporations are required by law to have a privacy statement regarding intent to use a customer’s information, the government has no such boundary enclosing that right. The only safeguard passengers currently have over the abuse of governmental authority are the privacy rights watch dogs that have been challenging any security measures being put in place by either the airlines or the government.

To Americans who travel often, the registered traveler program has provided incentives that will produce private information in exchange for shorter security lines. Foreigners traveling to the U.S. may not be as privileged, as collection of this data has become a requirement by the U.S. government. The registered program type of security, if successful, may eventually become the standard in airports for travelers across the world. As security technologies progress, costs will be driven down on the machines needed to provide the scanning of the iris and fingerprints. At the current moment, airline companies have provided the capital needed to introduce the iris and fingerprint scanners into the market. The costs have been justified by the increase of value perceived by the customer through convenience and quickness of travel, and thus an increase of demand to the airline. However, since TSA retains control of security screeners, and other screening equipment, there will almost certainly come a time when iris and fingerprint scanning will fall into the responsibility of the federal government. The most likely moment to see a switch of this magnitude will be when airline companies decide that the Registered Traveler program no longer serves as a competitive advantage mechanism and will seek to outsource the service.

### **Future Implications**

In the long run, there are a few scenarios in which the registered programs become obsolete as a competitive advantage. One possible scenario revolves around the intense competitiveness of the industry. As companies look to shed costs they may decide that frequent travelers do not represent a highly profitable customer group. Their focus would possibly shift then to other products aimed at the much less frequent

business travelers who in their analysis are more profitable. In this way, the security technologies may be forced out because the costs of acquiring the machines and running them do not exceed the benefits of keeping the security measures running. Another scenario assumes that, since the government has a great deal at stake in identifying passengers from terrorists, an increase in government regulations will make it nearly impossible to operate in a profitable manner. When this happens, the government will have the flexibility to decide how many travelers to introduce to the program, assuming the majority of travelers have not already joined a registered program for swiftness of travel benefits.

It is important to note that many private companies have picked up security contracts across the U.S. airports. The important decision-making ability to decide who should be offered the "service," will eventually rest with the party providing the contract, currently the government. It has also been confirmed that the size of a database correlates strongly to misidentification of objects in the database (Mark Hall 2003). If the government or airline companies expand the database to the point where the use of smart cards are no longer required, then the rate of misidentifying passengers will increase dramatically.

Problems with the Registered Traveler program stem not from what it is capable of doing now, but by what it will be capable of accomplishing in the near future. For airlines to continue to push the privacy boundaries of its passengers, they will need to prove to the travelers that the benefits of providing information should be accompanied by trust in the airlines that the future consequences to privacy are not undermined. As communication between government agencies and the airline industry increase, so will the potential for privacy information to be used in a way that the customer may not be willing to accept.

For privacy advocates, ideally data needs to be separated as much as possible. Irrational decision making often occurs in business when conclusions are reached through data mining techniques to uncover items that are correlated to each other. Because correlation does not necessarily indicate causation between items, these relationships may change over time. The criminal barred from flying is an example of this. Correlation between an individual's past crimes and the risk he or she imposes on the airline would probably support the conclusion that the criminal should be barred from flying. An offense in the past however may not necessarily mean that he or she is a risk to fly now, especially if the offense is a minor misdemeanor. False data that creeps into databases overtime is another concern that airlines will have to deal with in the future. Such data that results in a business manager kept off a flight, may cost a company thousands of dollars, in wasted time, and may postpone a decision giving a competitor extra time to react. Discrimination has been a strong suit for the Registered Traveler program. Humans are bound to make decisions based on biasing factors such as race, gender, and sexual preferences. These are just a few issues that need to be considered regarding the effectiveness and efficiency of the Registered Traveler Program, and the benefits provided to the airline traveler. Summarizing these issues based on the PAPA standard, and defining the Privacy Act as it relates to the Registered Traveler

program will help to define the climate affecting travelers' rights concerning the future ethical challenges.

### **Privacy and Civil Liberty Implications**

The TSA is in the process of potentially launching the largest domestic surveillance system ever created, without the opportunity for informed public debate and Congressional scrutiny. Under the registered traveler program, the TSA is essentially expanding on to Aviation Security Screening Records (a passenger database) by increasing the amount of passenger data to be collected and stored for future use. The National Research Council commented that the program is a possible precursor to a widespread national ID program that involves serious privacy and civil liberty implications (Hoofnagle and Kshirsagar 2003).

### **The Privacy Act of 1974**

The Privacy Act of 1974 was established to deal with the concerns about how the creation and use of computerized databases might impact individuals' privacy rights. The provisions of the Act were set forth to guard an individual American's location, welfare, intentions, or problems from anyone, without the expressed consent of that individual, including congressional representatives (United States Department of Justice 2004). In other words, according to the Privacy Act, information that is not within the public domain is not to be released to anyone without written consent.

The Privacy Act carries four distinct provisions. First, it requires government agencies to show to an individual any records kept on him or her. Second, it requires government agencies to follow certain principals, called "fair information practices," when gathering and handling personal data. Third, it restricts how agencies can share individuals' data with other agencies. Foremost, it gives the individual the right to sue the government for violating these provisions.

### **Public Policy Issues of the Information Age (PAPA)**

The Department of Transportation has proposed to exempt the Passenger Database under the Registered Traveler Program from several record-keeping obligations enforced under the Privacy Act of 1974 (Hoofnagle and Kshirsagar 2003). Their argument is that since the program is being used for law enforcement purposes, exceptions must be allowed. As a result, the registered traveler program has brought about privacy, accuracy, property and accessibility issues that must be addressed to ensure individual rights provided by the Privacy Act of 1974 are not undermined.

### **Privacy**

Under the Privacy Act, an agency is required to "maintain in its records only such information about an individual as is relevant and necessary" to achieve the stated purpose (United States Department of Justice 2004). Surprisingly, the TSA has exempted the Registered Traveler Program from this provision without explaining why collecting irrelevant information would be beneficial to the program (Sobel et al. 2004, p. 13-14). This open ended method of data collection

contradicts objectives set forth by the Privacy Act and raises many questions concerning the privacy of participants.

Personal information stored in the registered traveler system can include any of the following: full name, current home address, current home phone number, current cell phone number, social security number, date of birth, place of birth, nationality, gender, prior home addresses, arrival date in US, digital photo, biometric reference, unique identification record number, Registered Traveler (RT) eligibility status, and information provided by Federal, State, and local government agencies and foreign governments that is necessary to carry out a security evaluation (Walters 2004). If the person is determined to be a risk, then the database can include information gathered on that person from "risk assessment reports; financial and transactional data; public source information; proprietary data; and information from law enforcement and intelligence sources (Hoofnagle and Kshirsagar 2003, p. 2).

The Privacy Act places restrictions upon agency use of gathered personal information. These restrictions protect the privacy of individuals by regulating the collection, maintenance, use, and distribution of personal information. However, the TSA's privacy notice exempts the system from these protections of the Privacy Act (Sobel et al. 2004). Considerations should be determined as to whether or not the Registered Traveler Program should be able to claim these exemptions from the Privacy Act.

### **Accuracy**

Complementary to the right to access information is the right to correct it. The Privacy Act calls for maintaining government records about individuals with such accuracy, relevance, timeliness and completeness necessary to assure fairness to individuals in making determinations about them (United States Department of Justice 2004). However, the TSA has exempted the Register Traveler program from these Privacy Act requirements that describe the government's duty to allow citizens to confront the accuracy of information enclosed in their records (Sobel et al. 2004). These requirements include correcting identified inaccuracies swiftly, making notes of requested amendments within the records, and establishing actions to handle disputes between the agency and the individual as to the accuracy of the records (United States Department of Justice 2004).

In place of the judicially enforceable right to correction set forth in the Privacy Act, "the TSA has established its own discretionary set of procedures for passengers to contest the accuracy of their records" (Sobel et al. 2004, p. 12). The method set forth for contesting records follows closely to the "notification procedure" used to gain access to personal records. It has been reported by the TSA that "they have the discretion to correct erroneous information upon a passenger's request, but they have no obligation to do so" (Sobel et al 2004, p. 12). Although passengers will have the right to judicial review, the effectiveness of this provision is restricted because the TSA has exempted the system from access, correction, and relevance requirements set forth by the privacy act. In other words, the right to judicial review is limited which, for all

practical purposes, makes challenging the accuracy of the system ineffective.

The TSA has not provided any information as to why judicially enforceable Privacy Act correction procedures would be inappropriate in the context of the Registered Traveler program. Limiting individuals the right to ensure the system contains accurate, relevant, timely and complete records increases the probability that the Registered Traveler program will be an error-prone system with inaccurate and outdated information (Sobel et al. 2004).

### **Property**

Registered Traveler (RT) Operations Files is the system name of the passenger database compiled under the Registered Traveler Program and was published in the Federal Register on June 1, 2004 (Dean and Kelly 2004). These records are maintained in the Office of Information Technology at the TSA Headquarters in Arlington, Virginia and at other various TSA field offices, and the records are protected from unauthorized access through administrative, physical, and technical safeguards (Walters 2004). According to the Registered Traveler Pilot Privacy Impact Statement, "the data will be encrypted using National Institute of Science and Technology (NIST) and Federal Information Security Management Act (FISMA) standards." TSA is currently in the process of developing a retention schedule to determine how long records will be maintained (Dean and Kelly 2004).

The system can be utilized by a wide range of entities depending on the circumstance. These entities include but are not limited to the US Department of Transportation, airports and aircraft operators, the Department of State, international and foreign governmental authorities, authorized law enforcement, the Department of Justice in review, congressional offices, and to the Attorney General of the United States (Walters 2004). Records can be stored on magnetic disc, tape, digital media, CD-ROM, bar code, magnetic stripe, optical memory stripe, disk, integrated circuit chip, and other approved technologies (Walters 2004). Even though external protection seems to be secure under what is revealed under the Privacy Impact Statement, one must understand that there is always the threat of damaged or abused property from insiders which include a wide variety of entities.

### **Access**

The Privacy Act allows any person to request access to his or her own records being maintained by an agency. It also enforces agencies to publish a notice of the existence of records in the Federal Register along with a notice of the procedures that need to be taken in order to obtain access to the information (United States Department of Justice 2004). The TSA has assigned a manager to take the responsibilities of handling notification requests, access requests, and the contesting of records. The TSA has also provided that an individual wishing to access his or her information within the system must follow the steps set forth in the "notification procedure". This procedure requires a written letter to the system manager including "full name, current address, date of birth, and a description of the information being asked for, which must include the time frame during which the record(s) may have been

generated" (Sobel et al. 2004, p. 9). However, the notice does not include a time frame for when the system manager must respond to requests nor does it provide any kind of guarantee that requests will actually be considered (Sobel et al. 2004). In other words, even if appropriate steps are followed in the request for access, there is no guarantee that the TSA will produce the records for the individual. The TSA has not provided an explanation as to why restricted access is necessary for facilitation of the Registered Traveler Program (Sobel et al. 2004).

Most of the people who will want to access their records will be those who have been denied entry into the program. However, under the proposed limited access, these people will have minimal opportunity to review their records and contest any errors they might find. For example, if an applicant is denied Registered Traveler status based on inaccurate information, it remains unclear to what recourse the person can have with limited access to records. The TSA's access provisions are, therefore, in direct conflict with the goals set forth by the Privacy Act to provide citizens with "an enforceable right of access to personal information maintained by government agencies" (Sobel et al. 2004, p. 11).

### **Conclusion**

While the Registered Traveler Program seeks to improve security and reduce inconveniences for participating travelers, it also raises several policy and implementation issues. According to the US General Accounting Office (GAO), many stakeholders believe that the registered traveler program will enable the TSA to more efficiently use its limited resources by "more cost-effectively focusing its equipment and personnel needs to better meet its security goals" (US General Accounting Office 2002, p. 17). However, other stakeholders believe that "less stringent screening for some travelers could weaken security by introducing vulnerabilities into the system" (US General Accounting Office 2002, p. 17). For example, terrorists could potentially spend time in the US building up a law-abiding record to become registered travelers in order to take advantage of less stringent security screening.

Normative ethics is described as "the set of premises used to decide whether an action or decision is right or wrong" (Wood-Harper et al. 1996, p. 70-71). The consequentialist (or teleological) class of normative theory, which applies to implementation of the Registered Traveler Program, evaluates the rightness of an action based on the outcome that action will produce. However, according to Wood-Harper et al. problems arise when applying teleological theory to technology related actions because new technologies rarely have the consequences their inventors envisioned. Such was the case with the Internet as the originators foresaw it as a tool for the exchange of information, rather than a medium for a virtual society (Woods-Harper et al. 1996).

Similar to the Internet, the Registered Traveler Program will most likely expand beyond its specific purpose. Such a program could, potentially, become an enhanced customer service package for travelers used to speed up the check-in procedures at airports and to track frequent flier miles. Stakeholders interviewed by the GAO identified potential law enforcement uses, such as "collecting information obtained during background checks to help identify individuals wanted

by the police, or tracking the movement of citizens who might pose criminal risks" (US General Accounting Office 2002, p. 21). Representatives of air traveler groups that were interviewed envisioned "extensive marketing uses for data collected on registered travelers by selling it to such travel-related businesses as hotels and rental car companies and by providing registered travelers with discounts at these businesses" (US General Accounting Office 2002, p. 21).

The Registered Traveler Program has also raised many non-security related issues involving privacy concerns. Civil liberty advocates have expressed concerns that if the program is eventually used for purposes beyond security, information will become unprotected and privacy will be further exploited. Many stakeholders have stated their beliefs that pressures will be put on those who are not a part of the program to apply because of its advantages (US General Accounting Office 2002). This widespread participation could, in effect, lead to a national identity card which would forever change the world we live in today.

So in making a decision to participate in the Registered Traveler Program, an individual must face the dilemma of short-term versus long-term decision making. Choosing to participate will provide short term benefits such as being able to use faster security checkpoints at various airports. However, with widespread participation, this benefit will gradually fade away because everyone will, once again, experience the same amount of wait. The long term decision is choosing not to participate in order to protect individual privacy from being exploited on to what could become a national identity card. With the program on pace for widespread implementation by 2005 it is up to each individual to make their own decision, whether it be for the short term or the long term.

#### **Works Cited**

- "A Blow Against the Secrecy State" *Las Vegas Review*. Las Vegas, Nev.:Sep 17, 2004. p. 12B: Proquest <<http://www.proquest.com>>
- "Amid Confusion, List of 'No-fly' Passengers Grows." *International Herald Tribune*. Paris Oct 11, 2004. p. 22: Proquest <<http://www.proquest.com>>
- "Overview of the Privacy Act of 1974, 2004 Edition." *United States Department of Justice*. Prepared by Office of Information and Privacy and Office of Management and Budget. Last updated June 18, 2004. Received on Oct 15, 2004 from [http://www.usdoj.gov/04foia/04\\_7\\_1.html](http://www.usdoj.gov/04foia/04_7_1.html).
- "Poll: Fear Of Terror Attack Persists In US" Dow Jones Newswire 2004: *The Wall Street Journal*. <<http://www.wsj.com>>
- Croft, John. "Access Gets Personal". *Air Transport World*. Cleveland: Sep 2003. Vol. 40, Iss. 9, p. A19-A20: : Proquest <<http://www.proquest.com>>
- Colman, Robert and David Fletcher. "For the Public Good" *CMA Management* Hamilton: Oct 2003. Vol. 77, Iss. 6, p. 40-43: : Proquest <<http://www.proquest.com>>
- Hall, Mark. "Feeling Insecure" Mark Hall. *Computerworld*. Framingham: Jul 14, 2003. Vol. 37, Iss. 28, p. 32: Proquest <<http://www.proquest.com>>

- Dean, Lisa S. and Kelly, Naula O'Connor (2004) "Registered Traveler Pilot Privacy Impact Statement." *Transportation Security Administration*, June 24, 2004.
- Greenemeier, Larry. "Secure Flight Program Moves to Test Phase" *Informationweek*. Manhasset: Sep 27, 2004. Iss. 1007, p. 28(1 pp.): Proquest <<http://www.proquest.com>>
- Hirschman, Dave (2001). "Attack Fallout Clouds U.S. Airlines' High-Tech Aim." *Atlanta Journal and Constitution*, Oct. 18, 2001. Knight Ridder/ Tribune Business News, 2001.
- Harrison, Crayton (2004). "EDS, Unisys Hired to Test Registered Traveler Program for Airline Security." *The Dallas Morning News*, June 17, 2004. Knight Ridder/ Tribune Business News, 2004.
- Hoofnagle, Chris and Kshirsagar, Mihir. "In Matter of Privacy Act Notice Concerning Aviation Security Screening Records." *Comments of the Electronic Privacy Information Center*. Last updated February 24, 2003. Received on Nov. 3, 2004 from <http://www.epic.org/privacy/airtravel/tsacomment2.24.2003.html>.
- Kehaulani Goo. Sara. "Secret Rule Requiring ID for Flights at Center of Court Battle." *The Washington Post*. Washington, D.C: Oct 7, 2004. p. A.13. Proquest <<http://www.proquest.com>>
- Lambert, Lane. "9/11 We Remember" *The Patriot Ledger*. Quincy: Sept. 11, 2004. p. 12: Proquest: <<http://www.proquest.com>>
- MacDonald, Heather. "Hijacked by the 'Privocrats'". *The Wall Street Journal*. New York, N.Y.:Aug 5, 2004. p. A.10: Proquest <<http://www.proquest.com>>
- Seidenstat, Paul. "Terrorism, Airport Security, and the Private Sector" *The Review Of Policy Research*. May 2004. Vol. 21, Iss. 3, p. 275-291: Proquest<[www.proquest.com](http://www.proquest.com)>
- Sobel, David L., Holfmann, Marcia, Liskow, Samantha, and Mashayekhi, Dina (2004). "Docket No. TSA-2004-17982. Privacy Act Notice; Registered Traveler Operations Files." *Comments of the Electronic Privacy Information Center*. Department of Homeland Security; Transportation Security Administration.
- US General Accounting Office (2002). "Aviation Security: Registered Traveler Program Policy and Implementation Issues." *Report to the Honorable Kay Bailey Hutchison*, November 2002.
- Walters, Barry D. (2004). "Privacy Act of 1974: Systems of Records; Telecommunications Usage Detail Records; Registered Traveler Operations Files." Department of Homeland Security; Transportation Security Administration, 2004.
- Wilcox, Melynda Dovel and Woods, Lynn (2004). "Scanned and Cleared for Takeoff." *Kiplinger's Personal Finance*. Kiplinger Washington Editors, Inc., 2004.
- Wood-Harper, A.T., Corder, Steve, Wood, J.R.G., and Watson, Heather. "How We Profess: The Ethical Systems Analyst." *Communications of the ACM*. March 1996; Vol. 39, No.3.