



Transportation Research Forum

Industry Issue Paper: Airline Passenger Profiling Systems after 9/11: Personal Privacy versus National Security

Author(s): Timothy M. Ravich

Source: *Journal of the Transportation Research Forum*, Vol. 44, No. 2 (Summer 2005), pp. 127-141

Published by: Transportation Research Forum

Stable URL: <http://www.trforum.org/journal>

The Transportation Research Forum, founded in 1958, is an independent, nonprofit organization of transportation professionals who conduct, use, and benefit from research. Its purpose is to provide an impartial meeting ground for carriers, shippers, government officials, consultants, university researchers, suppliers, and others seeking exchange of information and ideas related to both passenger and freight transportation. More information on the Transportation Research Forum can be found on the Web at www.trforum.org.

AIRLINE PASSENGER PROFILING SYSTEMS AFTER 9/11: PERSONAL PRIVACY VERSUS NATIONAL SECURITY

This paper reviews the Transportation Security Administration's forthcoming computerized profiling system called "Secure Flight." Secure Flight is the latest generation of so-called "computer assisted passenger pre-screening systems." Such systems invite considerable privacy and civil liberty concerns, evoking references to an Orwellian society. This article confronts the central legal, political, and social tension borne of profiling systems such as Secure Flight, namely the conflict between the ideal of a "right to be let alone" (Warren and Brandeis 1890) relative to the post-Sept. 11 ultimatum of former American Airlines Chairman and CEO Robert L. Crandall (2002): "You want to travel on the airline system? You give up your privacy. You don't want to give up your privacy? Don't fly. Your privacy isn't equal to the safety of the rest of us."

by **Timothy M. Ravich**

INTRODUCTION

As the U.S. Supreme Court confirmed, the "freedom to travel throughout the United States has long been recognized as a basic right under the Constitution."¹ Not only is the freedom to travel a basic right of American law, but the "[c]onstitutional right to interstate travel is virtually unqualified."² A recent and sustained marketing campaign by low-cost carrier Southwest Airlines — "You are now free to move about the country" — underscores the liberty to air travel that Americans enjoy. Wealthier Americans were the primary passengers of early airlines. Modern deregulated air travel is more democratic and accessible. Today, anybody, from anywhere, can fly commercially. This freedom has been complicated by the national trauma caused by the events of Sept. 11, 2001, however.

Sept. 11 changed the paradigm of commercial airline security. As stated by a former strategy advisor to the Secretary of Defense and the Chairman of the Joint Chiefs of Staff (Karber, 2001-2002), "the survival of the plane and its occupants is no longer the ultimate objective in a situation involving assailants attempting to seize control of the aircraft." Whatever the novelty

of the tactics of Sept. 11, the societal *effects* of Sept. 11 are anything but novel. The legacy of Sept. 11 is a campaign to determine and isolate "them" from "us." Ironically, in the course of rooting out the proverbial enemy among us, the federal government's investigative energies are directed internally to "us."

Any efforts by the federal government to bolster national security presents a fundamental tension in American society between the practical need for security and the societal promise of liberty (AuBuchon, 1999; Dowley, 2002; Haas, 2004). Some Americans receive anti-terrorism measures as necessary to protect not just their freedoms, but their very lives. Other Americans resist well-intentioned federal efforts to promote security at the expense of personal freedoms. These Americans charge that hard-won constitutional protections must not be dismissed too easily as abstractions or legal niceties even, or especially, in the face of tangible threats by anti-democracy regimes. As a result of Sept. 11, the modern forum of this historic debate is the national commercial aviation system.

Specifically, on August 26, 2004, the Transportation Security Administration (TSA) introduced its plan for a comprehensive

computerized profiling system called “Secure Flight.” Scheduled to launch in the summer of 2005, Secure Flight will empower the federal government to assess the security risk(s) of domestic (not international) airline passengers. Under Secure Flight, airlines are obligated to furnish the TSA with passenger name records (PNR) for each of their respective customers. PNRs may include basic information such as a traveler’s itinerary, reservation history, and credit card data along with service-related information such as whether a traveler requested a special meal (*e.g.*, kosher) and/or whether the traveler is traveling alone or with any companion(s). The TSA will compare PNR data with other governmental watch lists, including a “no-fly” list, to develop a passenger profile.³ A remarkable profile will prompt the TSA to identify a traveler as a “selectee” for secondary security screening. Profiling of this nature invites debate of constitutional proportion.

Profiling system critics voice three principal concerns about Secure Flight. First, privacy advocates and civil libertarians contend that profiling systems such as Secure Flight are extreme. Would-be terrorists with grandiose Sept. 11-like intentions constitute a discrete minority of the traveling population. Accordingly, Secure Flight will not be the least intrusive security alternative because it will intrude into the privacy of the overwhelming majority of airline passengers, namely benign millions of law-abiding citizens who pose no aviation security threat. Second, profiling systems arguably deprive travelers of control over their personal information. In constructing a passenger profile and threat assessment, the federal government refuses to disclose precisely what information it will rely upon. Only the government knows the source of profiling data, which some profiling system critics argue may include information contained in untrustworthy commercial databases having nothing to do with airline travel. Further, it is unclear how the TSA will avoid and/or remedy profiling errors caused by mistaken identity, identity theft, fraud, or otherwise. Finally, intentionally or not, profiling systems may promote an unconstitutional categorization of travelers into ethnic, racial, and/or religious groupings. Instead of accepting the presumption that everyone is an

equal security risk, airline passenger profiling systems may cater to a post-Sept. 11 prejudice against certain types of travelers, in particular passengers from the Middle East (von Rochow-Leuschner, 2004). For many profiling system critics, the government cannot be trusted to design egalitarian machinery that is so disciplined as to be blind to the fact that all of the Sept. 11 terrorists were of a related and distinct ethnic, geo-cultural, and/or religious background (Baker, 2002; Banks, 2004; Chandrasekhar, 2003; Derbyshire, 2001; McDonald, 2002).

In the final analysis, the Secure Flight initiative supposes that the events of Sept. 11 could have been prevented or at least contested. This article accepts that premise and supports the federal effort to pre-screen airline passengers more thoroughly. In doing so, this article surveys and does not dismiss important countervailing constitutional and practical considerations to profiling. Last, this article offers some recommendations on how TSA policy should evolve to account for these concerns while advancing efforts to preempt terrorist plots involving the United States commercial airline system.

WHO IS THE ENEMY?

The initial questions borne of Sept. 11 were “what happened?” and “who did this?” These questions are resolved (National Commission on Terrorist Attacks upon the United States 2004). The secondary inquiry of what, if anything, can be done to identify and preempt future perpetrators remains open. To answer this question, federal aviation security policy makers assume that terrorists have identifiable characteristics or behavioral patterns that are different from other airline passengers. Profiling systems are sensible in this context because they distinguish “them” from “us” and “good” from “bad,” collecting as much information as possible about terrorists who maneuver among otherwise law-abiding airline passengers. Profiling systems such as Secure Flight, however, generate serious and divergent commentary challenging why “good” Americans themselves must be investigated as if they are a part of a terrorist threat.

The effectiveness of a profiling system intended to secure Americans and their rights

may require some contradictory impingement of the Constitution itself. The end of secure commercial airplane flight may necessitate undesirable means, particularly the abridgment of certain rights if only in the short term. It is not unreasonable or unwise to extrapolate from what is known. Future terrorists may be similar to those involved on Sept. 11. Therefore, profiling in terms of ethnicity, political agenda, race and/or religious affiliation has utility (Derbyshire, 2001; McDonald, 2002). Any federal systematic consideration of these attributes to enforce domestic airline security, however, is anathema to the Constitution and its corresponding freedom to travel (Baker, 2002; Banks, 2004; Chandrasekhar, 2003; Reser, 1998). Aviation security policy makers also must imagine threats from so-far unrevealed sources. The TSA must forecast that future terrorists are outside the Sept. 11 terrorist profile. Consequently, every airline passenger poses potential danger. The practice of the federal government targeting a substantial subset of its population (*i.e.*, airline passengers), however, also is antithetical to the ideals of both the Constitution and the Bill of Rights. Thus, the paramount questions about profiling systems are whether and how it is possible for the federal government to balance airline security measures with constitutional privacy considerations. The answers are as polarized as these questions suggest.

Profiling systems such as Secure Flight promote a zero-tolerance philosophy that the government should do whatever is necessary to prevent a Sept. 11-like event from occurring. The U.S. Constitution requires more balance and moderation. Secure Flight must be a proportional reaction to the terrorism of Sept. 11 and must perform within the confines of the Constitution.

One way to assess whether a profiling system is constitutionally acceptable is to examine the magnitude of operational errors that invariably may occur. The anecdotal evidence of unnecessary interrogations triggered by existing profiling systems is discouraging in this context. For example, an airline passenger from Kentucky was stopped 22 different times by the TSA, FBI, and Secret Service because his name is the same as that of an apparent financier of Al Qaeda. This experience, compounded by

the evolving danger of identity theft, emphasizes actual perils of computerized profiling systems. Errors occur, but are not always remedied effectively. The U.S. General Accounting Office specifically determined that the TSA failed to address issues of database accuracy, operational safeguards to protect system abuse, security measures to protect unauthorized system access, and passenger redress (U.S. General Accounting Office, 2004). Standing alone, these issues are important. These issues do not exist in a vacuum, however, but instead are relative to and tempered by the fact that the predecessor screening system to Secure Flight successfully identified nine of the 19 Sept. 11 terrorists. It is another matter that the only consequence of identification was detention of the terrorists' baggage until the terrorists themselves boarded the doomed airplanes. The developing story of Secure Flight, therefore, is about a struggle to determine an acceptable level of personal and societal costs brought by new security regimes (AuBuchon, 1999; Daniel, 2002; Kite, 2004; Miller, 2003; Rhee, 2000; Rosenzweig, 2004; Spencer, 2002).

HISTORY OF AIRLINE PASSENGER PROFILING

The degree to which federal aviation policies reasonably interfere with personal rights, if at all, is measured against the Constitution. The Fourth Amendment of the United States Constitution specifically is the interface of the competing, but similarly esteemed, ideals of national security and personal privacy. The Fourth Amendment provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.⁴

There is little practicality in obtaining a search warrant for every airline passenger who passes through an airport terminal. Consequently, Fourth Amendment jurisprudence finds curious application in the context of airline and airport

security. For example, boarding gate searches via metal detectors called magnetometers are court-sanctioned procedures that proportionally and defensibly intrude on personal liberty in favor of public safety and welfare. As one U.S. Court of Appeals reasoned:

. . . the search for the sole purpose of discovering weapons and preventing air piracy, and not for the purpose of discovering weapons and precriminal events, fully justified the minimal invasion of personal privacy by magnetometer. The use of the device, unlike frisking, cannot possibly be “an annoying, frightening, and perhaps humiliating experience, . . .”⁵

Searching airline passengers by profiling may be different, however, and so has received different treatment. Unlike magnetometers, airline passenger profiling intends to discover indicia of precriminal events that would expose selected travelers to further examination. Whatever its legality, airline passenger profiling is not new, finding precedent in earlier federal security measures designed to prevent air piracy.

Terrorism has tempered the freedom to travel throughout the history of commercial aviation (Reser, 1998). For example, the Federal Aviation Administration (FAA) has long regulated passenger profiling. The FAA mandated passenger profiling as a fundamental part of airline security in the 1960s, an active period of commercial aircraft hijackings. The FAA’s “Anti-Air Hijack Profile” established approximately 25 characteristics empirically linked with those of past hijackers.⁶ The purpose of this passenger screening system was to identify personal attributes that, if possessed by a traveler, would entitle security operators to examine that traveler’s carry-on luggage by X-ray or otherwise. The FAA ultimately abandoned hijacker-related profiling in 1972 in favor of global security checkpoints and X-rays of all carry-on luggage. The threat of hijackings and terror, however, did not abate and the need for profiling systems regenerated years later.

On July 17, 1996, the need for passenger screening reemerged, catalyzed by the disaster of TWA Flight 800. A trans-Atlantic Boeing 747, TWA Flight 800 exploded while

climbing over the coast of New York. The disaster occurred because of a defective fuel tank. Survivors suspected terrorism as the cause-in-fact. On this mistaken suspicion, on August 22, 1996, President Bill Clinton directed the development of the “White House Commission on Aviation Safety and Security” (Gore Commission). The Gore Commission was charged with “develop[ing] and recommend[ing] to the President a strategy designed to improve aviation safety and security, both domestically and internationally.”⁷ On Feb. 17, 1997, the Gore Commission issued its final report, making several security-related recommendations among which was the reintroduction of passenger profiling (Hahn 1997). The Gore Commission identified three ways in which to improve and promote 1960s-era passenger profiling:

First, FBI, CIA, and [Bureau of Alcohol, Tobacco, and Firearms] should evaluate and expand the research into known terrorists, hijackers, and bombers needed to develop the best possible profiling system. They should keep in mind that such a profile would be most useful to the airlines if it could be matched against automated passenger information which the airlines maintain. Second, the FBI and CIA should develop a system that would allow important intelligence information on known or suspected terrorists to be used in passenger profiling without compromising the integrity of the intelligence or its sources. Third, the Commission will establish an advisory board on civil liberties questions that arise from the development and use of profiling systems (White House Commission, 1997).

From this, the FAA advanced its efforts to develop a computer-assisted passenger screening program, the precursor to Secure Flight.

CAPPS I

The first-generation computer airline passenger profiling system was developed by Northwest Airlines in 1996 under a grant from the FAA. After testing a prototype, Northwest Airlines

released the profiling software to other airlines through the FAA in December, 1997. The profiling software operated through the internal computer reservation system of each airline. Known as the “Computer-Assisted Passenger Prescreening System” (CAPPS), this initial system effected the concept that data collection is power (Nehf, 2003; Solove, 2002). CAPPS collects approximately 39 pieces of pre-boarding data that, both on a random and an intentional basis, identify travelers who should be subjected to heightened security procedures. Significantly, to the distress of privacy advocates, CAPPS profiles are confidential (Nojeim, 1998; Rosenzweig, 2004; Smith, 1998). The confidentiality of CAPPS profiling criteria underscores the ever-present tension between national security pressures and constitutional guarantees (AuBuchon, 1999; Crandall, 2002; Kearns, 1999; Smith, 1998). As one commentator (Rhee, 2000) noted, “[m]aking profiles public is necessary to make them legal, however, doing so would also destroy their usefulness.”

While the government will not disclose any criterion upon which a CAPPS profile is constructed, certain elements of the system are known with some confidence. Some observers of airline security (Nojeim, 1998) believe that CAPPS tracks several aspects of passenger conduct:

- method of payment for an airline ticket (*i.e.*, cash or credit);
- the timing of a purchase (*i.e.*, immediately before departure or in advance);
- the identity of travelers, including with whom, if anybody, the passenger is traveling;
- the activity at the destination, including whether the passenger intends to rent a car;
- the flight itinerary, including where the flight originates and its ultimate destination;
- the passenger’s specific travel plans, including ultimate destination when different than the flight upon which the traveler is aboard; and
- whether the flight is round trip or one-way.

A traveler identified by CAPPS as a “selectee” is subject to secondary screening:

Depending on the destination of the passenger (domestic or foreign) and the availability of advanced technology at particular airports, the additional security measure applied to selectees typically will involve one of the following: bag matching (the requirement that checked luggage be flown only if it is determined that the passenger who checked the luggage has boarded the airplane); examination by a certified explosive detection system (EDS); or examination using other advanced technology (such as explosive detection device or a trace detector) (U.S. Department of Justice 1997).

Curiously, this security regime likely would not have prevented the first documented bombing of a commercial airliner in the United States. That event occurred in 1955 when a passenger’s son covertly packed a bomb in the passenger’s luggage to collect insurance policy proceeds (Daniel, 2002; Smith, 1998). The unsuspecting passenger boarded the fateful flight without drawing any additional security screening. The effectiveness of profiling systems in the possible circumstance that innocent passengers are manipulated for sinister purposes is dubious.

Therefore, profiling invites significant criticism along operational grounds. CAPPS critics contend that the methodology used to profile airline passengers for further screening is over-inclusive, flagging up to half of all passengers yet missing vital targets (Rosenzweig, 2004). Profiling system opponents also contend that such systems simply do not work. For example, profiling by the U.S. Customs Service has not stopped the drug trade (Nojeim, 1998). In 1999, the FAA responded to this and other criticism by limiting the use of CAPPS profiles to baggage screening, abandoning the practice of subjecting selectees to personal searches and questioning. Concerns remained, however, about whose baggage was searched and why.

The U.S. Department of Transportation (DOT) (2001) stated affirmatively that CAPPS variables “are not based on the race, ethnicity, religion or gender of passengers.” In an earlier assessment, the Gore Commission enumerated

several safeguards to ensure such objectivity of airline passenger profiling systems:

- Profiles should not include information of a constitutionally suspect nature such as race, religion, or national origin;
- Factors should be verifiable data that are proven to predict risk;
- Strict limits should be set on dissemination of profile records, and a system should be established for passengers to challenge the accuracy of personally identifiable information;
- An independent panel should be set up to monitor the system and make sure no civil liberties are abridged; and
- Profiling should be continued only until effective explosive-detection systems are developed (White House Commission, 1997).

The Gore Commission elaborated that:

[f]actors to be considered for elements of the profile should be based on measurable, verifiable data indicating that the factors chosen are reasonable predictors of risk, not stereotypes or generalizations. A relationship must be demonstrated between the factors chosen and the risk of illegal activity . . . Procedures for searching the person or luggage of, or for questioning, a person who is selected by the automated profiling system should be premised on insuring respectful, non-stigmatizing, and efficient treatment of all passengers (*Ibid.*).

In 1997, the U.S. Department of Justice (DOJ) reviewed the selection criteria in CAPPs and opined that CAPPs did not “discriminate unlawfully against passengers” or include passenger traits such as names or mode of dress that might be directly associated with race, ethnicity, or religion (U.S. Department of Justice 1997). The DOJ concluded that CAPPs would not have a “disparate impact on any group of passengers” (*Ibid.*). Profiling system opponents, however, found the Gore Commission’s stated goals specious and the DOJ’s conclusions unbelievable.

The chief criticism of CAPPs — a criticism leveled with equal force against forthcoming profiling systems — relates to the confidentiality of the data relied upon to construct passenger

profiles. Profiling system critics protest the lack of transparency of CAPPs data as well as the source, integrity, and potential for misuse of such information. Some CAPPs opponents specifically warn about the dissemination of CAPPs profiles to other governmental agencies for purposes unrelated to terrorism or aviation security. The American Civil Liberties Union (ACLU) argues:

By its very nature, the computerized profiling system runs afoul of a central principle of privacy: Information given for one purpose ought not to be used for other purposes without the consent of the person to whom it pertains. People book a flight, or enroll in a frequent flyer program, not because they want to yield up data about themselves for a massive profiling system, but because they want to travel, and occasionally, travel for free.

The computerized profiling system relies on the wealth of data airlines collect about passengers for reasons other than profiling. Information airlines collect about their passengers includes name, address, the destinations to which a passenger flies with a particular airline, how the passenger paid for their tickets and who may have purchased the tickets for the passenger, the people with whom the passenger has traveled, whether the passenger booked onward travel such as a car or hotel, and other information. This personal data needs to be protected (Nojeim, 1998).

To protect airline passenger privacy without a corresponding decline in aviation security, the ACLU imagines security measures alternative to profiling, including training security personnel to identify tangible evidence of suspected criminal activity on reasonable, articulable bases other than stereotypes; screening airline personnel and employees of air security vendors (within constitutional means); adding measures to enforce security standards at foreign airports; and limiting FBI and law-enforcement access to passenger records except pursuant to a court order based on probable cause of criminality (*Ibid.*). After Sept. 11, however, aviation

security policy makers moved to enhance CAPPS capabilities.

CAPPS II

Described by senior government officials as the single most important component of the nation's aviation security infrastructure (O'Harrow, *Washington Post*, August 27, 2004), CAPPS II was a post-Sept. 11 proposal to update CAPPS I. CAPPS II intended to authenticate the identity of commercial airline passengers by checking each traveler's PNR, including full name, home address, telephone number and date of birth, against governmental databases for security assessment. CAPPS II would bridge airline passenger profiling systems to law enforcement and intelligence databases. As one publication reports (*CMP TechWeb*, Sept. 3, 2004), "CAPPS II would have notified law-enforcement officials whenever the screening process turned up passengers with outstanding warrants against them, even for non-travel-related incidents." As important, CAPPS II would use *commercial* databases for counterterrorism purposes. The use of commercial databases would enable aviation security analysts to create a mosaic of information derived from a variety of sources (Kearns, 1999). These aggressive features, if implemented, would make more potent the federal government's anti-terrorism efforts, which failed on Sept. 11. CAPPS II advocates understood the proposed system to be both a necessary overhaul of existing aviation security measures and an appropriately calibrated defensive measure. This rationale, however, met spirited opposition (DeGrave, 2004; von Rochow-Leuschner, 2004).

CAPPS II critics protested forcefully that, even acknowledging the magnitude of the terrorism of Sept. 11, CAPPS II would blunt Constitutional privacy rights to an intolerable degree. In an article on the expansiveness of CAPPS II (Wald and Schwartz, *South Florida Sun-Sentinel*, Sept. 20, 2004), several reporters relate a concern about "mission creep," whereby information comprising an airline passenger profile would unacceptably slip bit-by-bit into the hands of non-TSA governmental actors for uses unrelated to aviation security. Additionally, CAPPS II critics repeated their criticism of

CAPPS I that the constitutional costs to liberty and privacy rights outweighed imagined or actual benefits of profiling systems. CAPPS II opponents also publicized several embarrassing failures of CAPPS I. In September, 2004, British pop star Cat Stevens, who became a Muslim in the 1970s and today is known as Yusuf Islam, was evicted from an international flight bound for the United States. Stevens' name was on the government's "no-fly" list. CAPPS I also identified U.S. Senator Edward M. Kennedy (D-Mass.) and U.S. Representative Don Young (R-Alaska) for extra security scrutiny. The deepest criticism respecting CAPPS II related to the system's proposed use of commercial data for law-enforcement purposes. As two commentators noted:

For example, if you do not buy the book Amazon.com recommended to you based on other customers' buying patterns, the negative consequences are slight. If your credit card company puts a hold on the use of your card because it noticed an odd usage pattern and suspected someone might have stolen your card, you can explain and continue to use your card. But the consequences of using data for counterterrorism purposes can be much more serious. They can include arrest, deportation, loss of a job, greater scrutiny at various screening gates, investigation or surveillance, or being added to a watch list (Dempsey and Flint, 2004).

Eventually the crescendo of criticism by CAPPS II opponents reached the TSA, which offered to make several system modifications.

The TSA suggested three significant amendments to the CAPPS II design. First, the TSA agreed to erase most passenger information in the CAPPS II system within a certain amount of days after passengers completed their scheduled travel. The TSA also proposed appellate mechanisms for passengers erroneously targeted for heightened, secondary security screening. Most important, the TSA proposed limiting the use of private commercial data to compose a traveler's security profile. In particular, the TSA proposed transmitting PNR information to commercial data providers solely for the purpose of authenticating a passenger's

identity. Commercial data-miners, in turn, would evaluate whether a passenger is, in fact, who s/he represented when reserving a flight. Upon completion of this authentication process, the CAPPS II system would review a passenger's commercial identity against intelligence and law enforcement databases. Passengers positively identified without any corresponding matches with intelligence or law enforcement data would proceed to their flights. Those passengers with more remarkable profiles would be subjected to further search and/or law enforcement action. CAPPS II opponents viewed these measures as insufficient and CAPPS II never materialized.

CAPPS II was a marketing disaster apart from its substantive controversy. By proceeding without notice or opportunity for meaningful public comment, the TSA did precisely what privacy advocates cautioned CAPPS II would do — deny citizens due process of the law. The private method in which CAPPS II developed aggravated privacy-related concerns that the federal government was undercutting the Constitution. This suspicion evolved into certainty when civil libertarians learned that some airlines assisted the government to develop CAPPS II. JetBlue Airways and Northwest Airlines voluntarily provided the TSA with lists of their respective passengers for testing in the CAPPS II system, hoping to secure the very airplane travel they sell. JetBlue Airways, for instance, provided a data-mining government contractor with approximately a million passenger records (including names, addresses, and phone numbers). A consumer-research company ultimately evaluated these records, which included information about each passenger's demographics, including occupation, income, gender, home-ownership and car-ownership history, and household composition. This transfer of information was effected without the knowledge or consent of the passengers whose identity was disclosed. The airlines were sued as a result.⁸ The industry-government collaboration of the CAPPS II program highlighted the depth of information available by marrying PNR data with commercial and law-enforcement databases. The industry-government collaboration of the CAPPS II program also emboldened profiling system opponents. Ultimately, the TSA abandoned

CAPPS II on July 13, 2004, after the U.S. General Accounting Office reported that the TSA failed to meet related privacy concerns (U.S. General Accounting Office 2004).

SECURE FLIGHT

In August, 2004, the TSA introduced "Secure Flight," a next-generation CAPPS. Secure Flight is designed to implement the recommendation that government "no-fly" and "automatic selectee" lists be improved through a terrorist screening database (National Commission on Terrorist Attacks upon the United States, 2004). As one airline industry observer noted (Alonso-Zaldivar, *Los Angeles Times*, August 27, 2004), "[a]bout 15% of the nearly two million domestic air travelers each day are now pulled aside for more intrusive searches." "One of the goals of Secure Flight will be to bring down the rate of passengers selected for secondary screening . . . while effectively catching known or suspected terrorists" (Kim, *Aviation Daily*, Sept. 22, 2004). Secure Flight will be built upon the technology platform of its controversial predecessor, CAPPS II. The technical similarity between CAPPS II and Secure Flight encourages the contention that Secure Flight is, as one privacy advocate suggests (Scannell, *USA Today*, September 28, 2004), nothing other than "a stripped-down version of the old CAPPS II system with a more consumer-friendly name."

The TSA promotes Secure Flight as different from predecessor profiling systems, however. Secure Flight purportedly will access commercial databases only to confirm the actual identity of a traveler and not to compute a risk score for purposes divorced from commercial aviation security. Additionally, the TSA proposes that Secure Flight will maintain an appellate process for travelers mistakenly or inequitably selected for secondary screening. Finally, the TSA proposes employing a passenger advocate to whom passengers could turn if they are unfairly flagged for heightened security treatment. Whether these features alleviate the concerns of privacy advocates and civil libertarians is still at issue (Kite, 2004).

Like CAPPS II, Secure Flight represents ongoing efforts by the executive branch of the federal government to involve itself

directly with aviation security after Sept. 11 (Hessick 2002-2003). Secure Flight will shift passenger prescreening responsibilities from the privatized airlines to the federal government.⁹ Currently, airlines compare passenger names with government-provided terrorist watch lists. Certain sensitive government watch list information, however, is not available to airlines. To close this intelligence gap, Secure Flight will unify the process of comparing passenger identification with government data by having the government alone make this comparison relative to the government's own watch lists, including the Terrorist Screening Center Database (TSCD). In November, 2004, the TSA began testing Secure Flight by collecting historical passenger information and comparing that information with commercial data to determine the accuracy of passenger information and to resolve false positive matches against TSCD records. Therefore, privacy advocates contend that Secure Flight may be more invasive than CAPPS II.

Accordingly, Secure Flight generates the variety of constitutionally-based opposition that defeated the CAPPS II program. Through a request under the Freedom of Information Act, the Electronic Privacy Information Center (EPIC), a Washington, D.C. based public interest group, demanded that the TSA produce documents that explained how or if the FBI intends to protect the privacy of travelers in the course of maintaining records in terrorist-screening databases. EPIC's specific critique is that profiling systems such as Secure Flight deny airline passengers any judicially enforceable rights. EPIC charges that:

Like its [CAPPS] predecessor, Secure Flight has been exempted from crucial provisions of the Privacy Act, which will severely limit the rights individuals typically would have in the personal information the government maintains about them. For instance, Secure Flight may collect and use personal information irrelevant and unnecessary for aviation security. Furthermore, passengers will have no judicially enforceable rights to access and correct the personal

information maintained about them for the program. TSA assures the public, however, that "upon completion of the testing phase, and before Secure Flight is operational, TSA will establish comprehensive passenger redress procedures and personal data and civil liberties protections for the Secure Flight program." No details about these protections are available, nor [is] information about how long TSA will keep the PNR data that it collects for Secure Flight, even though the agency intends to launch the program early next year.¹⁰

Notwithstanding this criticism, efforts to develop Secure Flight are proceeding.

On Nov. 12, 2004, after providing public notice and entering into a multi-million dollar contract with IBM Corp. to conduct testing, the TSA ordered more than 70 U.S. airlines to submit PNRs for the month of June, 2004. In an article examining the intrusiveness of profiling systems (Hilkevitch, *Chicago Tribune*, Sept. 22, 2004), one reporter writes that "CAPPS II . . . required the airlines to turn over only passenger names, dates of birth, home addresses and home telephone numbers . . . [whereas] Secure Flight mandates that the airlines provide the security agency with passenger name records for each traveler -- a document that contains 39 fields of information ranging from a passenger's history of selecting pre-reserved seats to the identity of traveling companions." Another source (Wald, *International Herald Tribune*, Sept. 23, 2004) elaborates that the data the TSA requested "varies from airline to airline . . . and may also include the names of others traveling in the same party, meal preference, whether the reservation was changed, the method of payment and comments of all types by airline employees on matters like whether a passenger was drunk or belligerent." With this data, the TSA expects to conclude Secure Flight testing in February, 2005, and, in March, 2005, the Government Accountability Office is expected to report to Congress on the TSA's plan to examine commercial data through Secure Flight.

CONCLUSION

The issue of passenger profiling transcends the narrow topic of aviation security. Secure Flight and its predecessor profiling systems animate a philosophical tension in American society, disrupting the theoretical constitutional fault-line of liberty and order. Americans equate liberty and privacy with a right to avoid the public gaze and to be let alone (Warren and Brandeis 1890). Democratic and utilitarian impulses, meanwhile, encourage individual sacrifice for the greater good, *e.g.*, national security. Whether national security and privacy are equivalent concerns is debatable.

The relative importance of personal liberty and societal security is contextual. While the federal government is stimulated to preempt terrorism, the urgency that motivates Secure Flight dissipates over time as Americans normalize their lives and return to routines after Sept. 11 (Daniel, 2001-2002). Today, increasingly, Americans greet successively intrusive national security measures by the federal government with an “anti-anti-terrorism” sentiment that is based upon concerns about an ever-expanding executive and a “fear of technology” (Rosenzweig, 2004). Some citizens “equate the potential for abuse of Executive Branch authority with the existence of actual abuse,” considering “any expansion of executive authority, notwithstanding the potential for benign and beneficial results, because they judge the potential for the abuse of power to outweigh the benefits gained” (*Ibid*). The TSA’s promise to remedy profiling system mistakes after-the-fact is no promise for many Americans. For privacy advocates and civil libertarians, the idea of federal government access to airline passengers’ personal commercial data is problematic in the first instance. As one DOT official said (Podberesky, 2004), “many on the outside feel that the government cannot monitor its own activities.” The interplay of liberty and order is so delicate and fundamental that, whatever the events of Sept. 11, it is difficult to envision an adaptation of Secure Flight or similar airline passenger profiling system that harmonizes these two ideals.

The events of Sept. 11 mandate better security-related intelligence, however. Intelligence services should gather and share more information to effectuate this end (Kreimer, 2004). Secure Flight is consistent with this objective. Information networking vis-à-vis airline passenger profiling is a clear, limited, context-specific societal objective that, in a post-Sept. 11 environment, legitimately rivals private interests. As one scholar notes (Nehf, 2003), to best protect privacy rights generally, “in the modern digital world, information privacy should be viewed as a societal value justifying a resolution in the public interest, much like environmental policy and other societal concerns, with less emphasis on individual self-policing and market-based mechanisms.” As to Secure Flight specifically, the TSA must do more to publicize the merits of its proposed profiling system so that citizens have confidence in it and their rights relative to it. To date, however, Secure Flight develops at a distance from airline passengers, through technical legal papers, narrow communication channels, and uninviting bureaucracy. The TSA should engage American citizens to participate in national security programs actively.

In place of paternalism, the TSA might create a collaborative approach to national aviation security. This can be done if the TSA provides tangible travel-related benefits in exchange for voluntary sacrifice on the traveler’s part. As part of any aviation security campaign, the federal government might look more closely at the recommendations of private actors in the commercial aviation industry. For example, the Air Transport Association supports expansion of the government’s “Registered Traveler” program, which is being tested at airports in Boston, Houston, Los Angeles, Minneapolis, and Washington, D.C. Registered Traveler invites participants to submit to a background check voluntarily and to provide security agents with their birth date, phone number, address, and a biometric identifier (*e.g.*, fingerprint or iris scan). In return, registered airline passengers may avoid checkpoints and/or extra screening. Passengers who do not want to give up their privacy need not fly commercially (Crandall, 2002).

In the final analysis, the TSA's proposed profiling system divides Americans philosophically. This is evidenced (*Air Safety Week*, October 11, 2004) by the reactions of two American citizens to Secure Flight:

- Matthew Belmonte, Massachusetts Institute of Technology: "TSA's plan to compel United States airlines to produce old passenger name record data would, if implemented, be an unfair invasion of passengers' privacy, since those passengers who chose to fly during the period in question [June 2004] could not have been aware that their personal details would be released in this manner. Passengers expect privacy . . . TSA's continued plan to use information from commercial databases remains worrisome, since most commercial databases offer no easy way for individuals to examine and to correct information pertaining to them."

- Mitchell Stern, SeaGate Travel, Baltimore, Md.: "As a global travel director . . . I am all for Secure Flight. From a privacy aspect, I have no concern that would override the program objective to provide an enhanced, more secure transportation system in America."¹¹

Within this debate, the U.S. government has made a definite choice, allowing national security concerns to overtake privacy interests by some measure. Of course, citizens must not abandon a corresponding right and duty to protect, protest, and effectuate change to the extent constitutional conceptions of privacy and civil liberties are impinged. Airline passenger profiling systems do not purport to be panaceas for security-related vulnerabilities of the commercial airline industry. Instead, they are but one, vital element in a coordinated defense against tangible threats to American lives.

Endnotes

1. *United States v. Guest*, 383 U.S. 757, 758 (1966).
2. *Haig v. Agee*, 453 U.S. 280, 307 (1981). In *Kent v. Dulles*, the United States Supreme Court explained:

The right to travel is a part of the "liberty" of which the citizen cannot be deprived without the due process of law under the Fifth Amendment . . . In Anglo-Saxon law that right was emerging at least as early as the Magna Carta . . . Freedom of movement across frontiers in either direction, and inside frontiers as well, was a part of our heritage. Travel abroad, like travel within the country, may be necessary for a livelihood. It may be as close to the heart of the individual as the choice of what he eats, or wears, or reads. Freedom of movement is basic in our scheme of values. [One author has said,] "Our nation [] has thrived on the principle that, outside areas of plainly harmful conduct, every American is left to shape his own life as he thinks best, do what he pleases, go where he pleases."

357 U.S. 116, 126 (1958). Article 42 of the Magna Carta reads:

It shall be lawful to any person, for the future, to go out of our kingdom, and to return, safely and securely, by land or by water, saving his allegiance to us, unless it be in time of war, for some short space, for the common good of the kingdom: excepting prisoners and outlaws, according to the laws of the land, and of the people of the nation at war against us, and Merchants who shall be treated as it is said above.

3. The government's "no-fly" list identifies known or suspected terrorists while its "watch" list names those identified for tighter pre-boarding scrutiny.

4. U.S. CONST. amend. IV.

5. *United States v. Epperson*, 454 F.2d 769, 771 (4th Cir. 1971) (“To require a search warrant as a prerequisite to the use of a magnetometer would exalt form over substance . . . The danger is so well known, the governmental interest so overwhelming, and the invasion of privacy so minimal, that the warrant is excused by the exigent national circumstances.”).

6. In *United States v. Slocum*, 464 F.2d 1180, 1183 (3d Cir. 1972), a federal appellate court concluded:

The practicalities of commercial air transportation dictate that any attempts to discover potential hijackers among scheduled passengers be carried out with minimum disruption of the boarding procedures. The Profile meets in part this objective by immediately restricting application of the intrusive aspects of the program. Its compilation of easily observable, nondiscriminatory indicia characteristic of the hijacking problem focuses the program on a limited number of persons among each group of boarding passengers. We cannot conclude that solely because the Profile operates on the basis of a statistical comparison of the passengers to past hijackers that, necessarily, it should be considered as an attempt to establish probable cause and, therefore, be subject to scrutiny according to 4th Amendment standards.

7. Executive Order 13,015, 61 Fed. Reg. 43,937 (1996).

8. *Dyer v. Northwest Airlines Corporations*, 2004 WL 2009397 (D.N.D. 2004); *In re Northwest Airlines Privacy Litigation*, 2004 WL 1278459 (D. Minn. 2004); *Turrett v. JetBlue Airways*, 2003 WL 22843134 (C.D. Cal. 2003).

9. The government has federalized the aviation security infrastructure since Sept. 11, 2001. In addition to creating the Department of Homeland Security (of which the Transportation Security Administration is a part), in November, 2001, the federal government assumed responsibility for screening airline passengers, a task historically managed privately by airlines through independent contractors. As a result, today, all airport security screeners are federal employees.

10. *Air Safety Week*, “Reactions to Secure Flight,” Oct. 4, 2004.

11. *Air Safety Week*, “All for It - and Completely Opposed,” Oct. 11, 2004.

References

Alonso-Zaldivar, Ricardo. "New Passenger Profiling System to be Tested." *Los Angeles Times*, Aug. 27, (2004): A12.

AuBuchon, Michael J. "Choosing How Safe is Enough: Increased Antiterrorist Federal Activity and its Effect on the General Public and the Airport/Airline Industry." *Journal of Air Law and Commerce* 64, (1999): 891-911.

Baker, Ellen. "Flying While Arab—Racial Profiling and Air Travel Security." *Journal of Air Law and Commerce* 67, (2002): 1375-1405.

Banks, R. Richard. "Racial Profiling and Antiterrorism Efforts." *Cornell Law Review* 89, (2004): 1201-1217.

Chandrasekhar, Charu A. "Flying while Brown: Federal Civil Rights Remedies to Post-9/11 Airline Racial Profiling of South Asians." *Asian Law Journal* 10, (2003): 215-252.

CMP TechWeb. "TSA Extends Registered Traveler Program to Reagan National." Sept. 3, (2004): 2004 WL 64587874.

Crandall, Robert L. "Security for the Future: Let's Get Our Airlines Flying Again." *Journal of Air Law and Commerce* 67, (2002): 9-27.

Daniel, Jack. H. "Reform in Aviation Security: Panic or Precaution?" *Mercer Law Review* 53, (2002): 1623-1645.

DeGrave, Michael J. "Airline Passenger Profiling and the Fourth Amendment: Will CAPPS II Be Cleared for Takeoff?" *Boston University Journal of Science and Technology Law* 10, (2004): 125-151.

Dempsey, James X. and L. Flint. "Commercial Data and National Security." *George Washington Law Review* 82 (2004): 1459-1502.

Derbyshire, John. "In Defense of Racial Profiling." *National Review* 53, (2001): 38-40.

Dowley, Michael F. "Government Surveillance Powers under the USA Patriot Act: Is It Possible to Protect National Security and Privacy at the Same Time? A Constitutional Tug-of-War." *Suffolk University Law Review* 36, (2002): 165-183.

Haas, Eric P. "Back to the Future? The Use of Biometrics, Its Impact on Airport Security, and How this Technology Should be Governed." *Journal of Air Law and Commerce* 69, (2004): 459-489.

Hahn, Robert W. "The Economics of Airline Safety and Security: An Analysis of the White House Commission's Recommendations." *Harvard Journal of Law and Public Policy* 20, (1997): 791-827.

Hessick, Andrew. "The Federalization of Airport Security: Privacy Implications." *Whittier Law Review* 24, (2002-2003): 43-69.

Hilkevitch, Jon. "Privacy Fears Dog Terror Screen; Foes: New System is More Intrusive." *Chicago Tribune*, Sept. 22, (2004): 13.

Karber, Phillip A. "Re-Constructing Global Aviation in an Era of the Civil Aircraft as a Weapon of Destruction." *Harvard Journal of Law and Public Policy* 25, (2002-2003): 781-814.

Kearns, Thomas B. "Technology and the Right to Privacy: The Convergence of Surveillance and Information Privacy Concerns." *William & Mary Bill of Rights Journal* 7, (1999): 975-1011.

Kim, Angela. "TSA Directs Airlines to Handover PNR in 40 Days." *Aviation Daily*, Sept. 22, (2004): 1.

Kite, Leigh A. "Red Flagging Civil Liberties and Due Process Rights of Airline Passengers: Will a Redesigned CAPPS II System Meet the Constitutional Challenge?" *Washington and Lee Law Review* 61, (2004): 1385-1436.

Kreimer, Seth F. "Watching the Watchers: Surveillance, Transparency, and Political Freedom in the War on Terror." *University of Pennsylvania Journal of Constitutional Law* 7, (2004): 133-181.

McDonald, R. Spencer. "Rational Profiling in America's Airports." *Brigham Young University Journal of Public Law* 17, (2002): 113-138.

Miller, Eric J. "The 'Cost' of Securing Domestic Air Travel." *John Marshall Journal of Computer and Information Law* 21, (2003): 405-437.

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. W&W Norton, New York, 2004.

Nehf, James P. "Recognizing the Societal Value in Information Privacy." *Washington Law Review* 78, (2003): 1-91.

Nojeim, Gregory T. "Aviation Security Profiling and Passengers' Civil Liberties." *Air & Space Lawyer* 13, (1998): 3-9.

O'Harrow, Jr., Robert. "Airport Screening System Touted as Improvement." *Washington Post*, Aug. 27, (2004): E03.

Podberesky, Samuel. *Remarks of Assistant General Counsel for Aviation Enforcement, United States Department of Transportation at Practical Views from the Cockpit to the Courtroom, ABA Tort, Trial, and Insurance Practice Forum, Washington, D.C., 2004.*

Reser, Heather. "Airline Terrorism: The Effect of Tightened Security on the Right to Travel." *Journal of Air Law and Commerce* 63, (1998): 819-848.

Rhee, Jamie L. "Rational and Constitutional Approaches to Airline Safety in the Face of Terrorist Threats." *DePaul Law Review* 49, (2000): 847-886.

Rosenzweig, Paul. "Civil Liberty and the Response to Terrorism." *Duquesne Law Review* 42, (2004): 663-723.

Scannell, Bill. "TSA Cannot be Trusted." *USA Today*, Sept. 28, (2004): A12.

Smith, Donna. "Passenger Profiling: A Greater Terror than Terrorism Itself?" *John Marshall Law Review* 32, (1998): 167-195.

Solove, Daniel J. "Digital Dossiers and the Dissipation of Fourth Amendment Privacy." *University of Southern California Law Review* 75, (2002): 1083-1168.

Spencer, Shaun B. "Security vs. Privacy." *Denver University Law Review* 79, (2002): 519-573.

United States Department of Justice. *Report by the Department of Justice to the Department of Transportation on the Civil Rights Review of the Proposed Automated Passenger Screening System, U.S. Dept. of Justice.* 1997. <http://www.usccr.gov/pubs/sac/mi0501/app.htm>

United States Department of Transportation. *DOT Investigates Passenger Security Screening's Impact on Minorities.* 2001. <http://www.dot.gov/affairs/dot5501.htm>

United States General Accounting Office. *Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges, Report to Congressional Committees,* GAO Report No. GAO-04-385, Washington, D.C., 2004.

von Rochow-Leuschner, Deborah. "CAPPS II and the Fourth Amendment: Does it Fly?" *Journal of Air Law and Commerce* 69, (2004): 139-172.

Wald, Matthew L. "U.S. Airlines Forced to Give Data on Travelers for Antiterror Screen." *International Herald Tribune*, Sept. 23, (2004): 1.

Wald, Matthew L. and John Schwartz. "Airport Screening Program's Expansion Led to its Demise." *South Florida Sun-Sentinel*, Sept. 20, (2004): 3A.

Warren, Samuel D. and L. Brandeis. "The Right to Privacy." *Harvard Law Review* 4, (1890): 193-220.

White House Commission on Aviation Safety and Security. *Final Report to President Clinton.* 1997. <http://www.fas.org/irp/threat/212fin~1.html>

Timothy M. Ravich is a trial lawyer in Miami, Florida, having earned his law degree, cum laude, from the University of Miami School of Law where he served as Editor-in-Chief of the University of Miami Business Law Review. Ravich's practice focuses on general and complex commercial contract disputes and business litigation in federal and state courts. A Masters of Business Administration candidate in aviation planning and policy at Embry-Riddle Aeronautical University, Ravich also focuses on aviation law and legislation. He has written extensively on issues relating to commercial airline passengers' rights including "Re-Regulation and Airline Passenger Rights" in the *Journal of Air Law and Commerce* (2002).