10-1-2007

Is Airline Passenger Profiling Necessary?

Timothy M. Ravich

Follow this and additional works at: http://repository.law.miami.edu/umlr

Part of the Law Commons

Recommended Citation
Available at: http://repository.law.miami.edu/umlr/vol62/iss1/2

This Article is brought to you for free and open access by Institutional Repository. It has been accepted for inclusion in University of Miami Law Review by an authorized administrator of Institutional Repository. For more information, please contact library@law.miami.edu.
I. **INTRODUCTION**

On August 10, 2006 British intelligence prevented a terrorist plot to blow up ten airplanes by detonating common liquids. In response, the Transportation Security Administration ("TSA") banned certain carry-on items. In May 2007 TSA unveiled "FIDO," a hand-held scanner capa-
ble of detecting liquid explosives inside sealed bottles. Although providing an important layer of security, carry-on restrictions and explosives detecting equipment exemplify why profiling is necessary to safeguard commercial aviation. Reaction-based national aviation security policy focused myopically on objects instead of people is backward looking and flawed, "the equivalent of fighting the last war."  

Profiling airline passengers should be a vital part of commercial aviation security because screening for bad people is at least as important as screening for bad things. This article explores the theoretical underpinnings of government- and private-sector profiling systems like "CAPPS," "CAPPS II," and "Secure Flight," along with the "Registered Traveler" program, and examines whether such systems represent effective anti-terrorism measures designed to manage the risk against future airline terrorism. In doing so, this article does not accept the ongoing development of profiling systems uncritically.

---


5. One source identifies three classes of profiling: biometric, psychometric, and sociometric. Biometric, Psychometric, and Sociometric Profiling, IBPONLINE, Oct. 24, 2003, http://security.pr.crau.edu/read.php?kind=html&article_volume=15&article_issue=8&article_title=Biometric%2C%20Psychometric%2C%20and%20Sociometric%20Profiling. “In biometric profiling, the information leading to behavioral prediction comprises human physical characteristics . . . [like] the iris, finger pads, structural and kinesic elements of the face, and partially overlapping physiological phenomena that can be detected remotely. Sweating, pulse rate, and respiration are examples of common psychophysiological phenomena.” Id. Psychometric profiling involves “inferred traits as to human cognition, emotion, motivation, and behavioral tendencies, as well as a plethora of observed traits further describing certain behaviors such as speaking and walking.” Id. Finally, “[i]n sociometric profiling, the information leading to behavioral prediction comprises interpersonal, intragroup, intraorganizational, and intracultural aspects of an individual’s biological, psychological, and social functioning—e.g., academic and work history, criminal record, degree and type of cooperation and competition with other individuals, participation in informal networks, and ethnic identification.” Id.
As a threshold matter, whether profiling systems can reliably predict who is or is likely to become a terrorist is questionable. Terrorists come from every background, and age, sex, ethnicity, education, and economic status are becoming irrelevant considerations for profiling purposes. For example, three of the suspects arrested in the August 2006 liquid-bomb plot were religious converts from London’s affluent suburbs, including one man who was the son of an English Conservative Party activist and who loved the movie *Team America.* Practically, then, identifying terrorists through profiling may be impossible, not merely counterintuitive.

Legally, too, airline passenger profiling raises important constitutional considerations that should not be dismissed simply because more security is needed at the nation’s airports. Liberty and privacy are chief among these considerations. Liberty, like life and the pursuit of happiness, is one of the specific unalienable rights expressed in the Declaration of Independence. Liberty, in turn, involves privacy or the “right ‘to be let alone.’” Liberty and privacy are abstractions, encompassing many definitions and evading certain meaning simultaneously.

---

6. See MARC SAGEMAN, UNDERSTANDING TERROR NETWORKS 99 (2004); see also Richard W. Bloom, Commentary on the Motivational Psychology of Terrorism Against Transportation Systems: Implications for Airline Safety and Transportation Law, 25 TRANSP. L.J. 175, 179 (1998) (“[M]ost profilers analyze external features, such as physical characteristics, behaviors, or demographics. However, intrapsychic processes may be more robust correlates of terrorist behavior, but are more difficult to identify. Yet, some psychologists even believe that these correlates either do not exist or are irrelevant in analyzing human behavior.”); Craig Whitlock, *Terrorists Proving Harder To Profile: European Officials Say Traits of Suspected Islamic Extremists Are Constantly Shifting,* WASH. POST, Mar. 12, 2007, at A1 (“With new plots surfacing every month, police across Europe are arresting significant numbers of women, teenagers, white-skinned suspects and people baptized as Christians—groups that in the past were considered among the least likely to embrace Islamic radicalism.”).

7. Whitlock, *supra* note 6, at A1. That no reliable profile of a terrorist may exist was further illustrated by the fact that investigators of the August 2006 liquid-bomb plot suspected that a husband and wife planned to smuggle liquid explosives aboard airplanes using their infant daughter’s bottle. *Id.* Another more recent example of terrorism by people considered to be caregivers occurred on June 30, 2007 when several physicians put into action a plot to drive a suicide car bomb into the arrival terminal at the airport in Glasgow, Scotland. See Olga Craig, *The People Who Cure You Will Kill You,* SUNDAY TELEGRAPH (London), July 8, 2007, at 20; Aditi Khanna et al., *Doctors of Terror,* INDIA TODAY, July 16, 2007, at 40.

8. THE DECLARATION OF INDEPENDENCE para. 2 (U.S. 1776).


10. The definition of terrorism is complicated and evolving. See, e.g., CONOR GEARTY, THE FUTURE OF TERRORISM (1997); BRUCE HOFFMAN, INSIDE TERRORISM 1 (rev. & expanded ed.
theless, Americans demand certainty after September 11, 2001, especially in regard to commercial aviation security. Historically, though, abstractions such as civil liberties have suffered in times of indefiniteness and national security crises and, presently, the invitation for aviation security policy makers to restrict liberty and privacy in reaction to terrorist threats is attractive.11 Designing and implementing effective airline passenger profiling systems need not present liberty and privacy, on one hand, and national security, on the other hand, as mutually exclusive policy choices.12

Privacy, liberty, and security proponents are equally blameworthy in presenting their arguments for or against airline passenger profiling


systems in absolute terms. The starting point for many libertarians and privacy advocates is Benjamin Franklin's uncompromising statement in 1759, that "[t]hose who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety." Oppositely, one well-known airline CEO gives this ultimatum: "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."

Rejecting the notion that security is possible only at the expense of liberty and privacy, this article recommends an aviation security policy in which profiling plays an integral and lawful role. After detailing specific government- and private-sector profiling initiatives, this article assesses airline passenger profiling in terms of three broad questions: Who is the enemy that aviation security policy intends to identify? Is profiling rational or racist? And do airline passenger profiling systems necessarily require a policy choice favoring national security over liberty and privacy rights? Concluding with an overview of international airline security measures by and between the European Union and the United States, this article ultimately submits that airline passenger profiling, with its focus on bad people and not just bad things, should be a centerpiece of national aviation security policy after September 11.

II. PROFILING INITIATIVES

Terrorism has always shadowed commercial airline travel. The first documented airline hijacking occurred as early as 1931, when Peruvian revolutionaries overtook a domestic flight to distribute propaganda. Hijackers have since seized commercial airplanes to bargain for the exchange of political prisoners or to escape to a particular destination like Cuba. In contrast, the objective of the September 11
hijackers was to kill Americans and to destroy national icons of American economic, military, and political might.\textsuperscript{18}

The September 11 hijackers—ten of nineteen were identified for further security screening by a computer passenger profiling system\textsuperscript{19}—caused a cascade of damage emanating from their hijacking. Their weapons were not guns and certainly were not the box cutters they used to gain cockpit access. Rather, in hijacking at least four airplanes, the September 11 terrorists commandeered the entire U.S. commercial aviation system and existing infrastructure. In doing so, the September 11 terrorists exposed erroneous assumptions on which national aviation security policy operated for decades. Thus,

\[\text{[t]he biggest challenge to preventing the civil aircraft from becoming a weapon of destruction is forty years of accumulated preconceptions that now need to be overcome. First and foremost, and emotionally toughest, is the recognition that 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. Preventing terrorists from taking over the flight controls, and thus preventing them from turning the plane into a weapon of further destruction, takes precedence no matter what the danger to the plane.}\textsuperscript{20}

On the surface, September 11 represented a departure from historical conceptions of airline terrorism. At the same time, September 11 also represented a failure of aviation security policy makers to appreciate the history of aviation terrorism. A former U.S. Department of Transportation ("DOT") Inspector General recounted the following:

There was a plot . . . to take four jetliners, maybe it was five, depending on if you count the plane that escaped. Anyway, there was a plot to take four jetliners. They hijacked them in a jihad to protest America's role in Israel. In this jihad, they would take the planes and crash them into something to do maximum harm to a nation and gov-

\[\text{At that time hijackers wanted to trade passengers and crew for large sums of money, release of political prisoners and escape to a safe haven. . . . Groups of hijackers willing to commit suicide were deemed highly unlikely . . . .}]; see also \text{JAMES A. AREY, THE SKY PIRATES} (1972); \text{RODNEY A. SNYDER, NEGOTIATING WITH TERRORISTS: TWA FLIGHT 847} (1994); \text{Stanley B. Rosenfield, Air Piracy: Is It Time To Relax Our Security?, 9 NEW ENG. L. REV. 81, 88 (1973–1974)}; \text{Mark. W. Levine, Note, Cuban Hijackers and the United States: The Need for a Modified Aut Dedere Aut Judicature Rule, 32 COLUM. J. TRANSNAT'L L. 133, 134 (1994).}\]

\text{18. See Moussaoui Trial: A Foiled Hijacker Rejoices over 9/11, MIAMI HERALD, Mar. 28, 2006, at A1 ("'You rejoiced in the fact that Americans were killed?' the prosecutor asked. 'That is correct,' [Zacarias Moussaoui, an al Qaeda conspirator who was part of the 9/11 plot] said, matter-of-factly. 'You called the collapse of the twin towers "gorgeous?" 'Indeed.'").}\n
ernment at which they were very displeased... Sorry, but they would have casualties. They would not even give them a second thought... You think I am talking about September Eleventh, don’t you? I am not.

I happen to be talking about September Twelfth, September 12, 1970. The same thing happened. The four planes were taken to the Middle East and blown up. In that case, they allowed the passengers—a very bizarre way that they did it, but they allowed the passengers to scramble to get off the plane.21

Whatever the novelty or precedence of the tactics of September 11, the terrorist threat confronting today’s airlines is conceptually different from national security concerns that previously confronted aviation security policy makers. Whereas the Soviet Union created “things” during the Cold War that could be observed and countered, terrorism is an indefinite threat, as “the terrorists create only transactions that can be sifted from the noise of everyday activity only with great difficulty.”22 In this new context, airline profiling systems may offer aviation security officials a preemptive and forward-looking mechanism to identify terrorists.23

But profiling airline passengers is controversial. Critics of airline passenger profiling systems voice four main concerns. First, privacy advocates and civil libertarians contend that profiling systems as security measures are too extreme. According to those critics, would-be terrorists with September 11-like intentions constitute a discrete minority of the traveling population. Consequently, profiling systems are not the least intrusive security alternative because they intrude into the privacy of the overwhelming majority of airline passengers who pose no threat to aviation security.24

21. Mary Schiavo, Flying Right: What It Takes To Make Aviation Safer and More Secure After 2001, 14 DEPAUL BUS. L.J. 279, 295 (2002). One author suggests “[t]he first attempt to convert a hijacked aircraft into a flying bomb targeted on a symbol of international salience, and the only known prequel to September 11, was the Christmas Eve 1994 hijacking of a French Airbus by a four-man team from the Algerian terrorist movement GIA, who wanted to crash the plane into the Eiffel Tower.” Karber, supra note 20, at 789.

22. Paul Rosenzweig, Civil Liberty and the Response to Terrorism, 42 DUQ. L. REV. 663, 679 (2004). An extensive unclassified database of terrorism attacks, called the Global Terrorism Database, is available online at http://www.start.umd.edu/data/gtd. “The database was developed by Start, the National Consortium for the Study of Terrorism and Responses to Terrorism, based at the University of Maryland, with funding from the U.S. Homeland Security Department. It includes 80,000 terror incidents from 1970–2004. Start plans to update the database through 2007 within the next twelve months.” The Global Terrorism Database, AVIATION WK. & SPACE TECH., May 28, 2007, at 23.


24. See infra Part III.
Second, profiling critics wonder about the source and ownership of information in passenger dossiers. Arguably, profiling systems deprive travelers of control over their personal information. The federal government refuses to disclose precisely what information it will rely on to compile a passenger profile and threat assessment. The government alone knows the source of profiling data. Some profiling system critics argue that the source of the government's profiling data is untrustworthy commercial databases that have nothing to do with airline travel.25

Third, profiling systems are operationally ineffective, producing "false positives" and "false negatives." Anecdotal evidence of existing profiling systems identifying law-abiding passengers for heightened screening or unnecessary interrogations or both is discouraging. For example, TSA, FBI, and the Secret Service have stopped an airline passenger from Kentucky twenty-two different times because his name is similar to that of an apparent financier of al Qaeda.26 Meanwhile, existing screening systems failed to notice anything remarkable when the name of America's most-wanted fugitive, Osama Bin Ladin, was tested.27 These infrequent but not unique experiences, aggravated by the evolving danger of identity theft, illustrate a serious defect of an aviation security regime dependent on machines to make threat assessments.28

Finally, while airline passengers may pose unequal security risks as a matter of fact, profiling systems treat passengers unequally and discriminatorily as a matter of law. Critics of airline passenger profiling specifically contend that computerized screening is internally biased against passengers with connections to areas of the world whose behavior or policies conflict with the interests of the United States—namely the Middle East. As such, critics believe that profiling would promote an unconstitutional categorization of travelers by ethnicity, race, religion, or a combination of all three.29 And although the federal govern-

25. See infra Part II.B–C.
29. In considering whether the incidence of stopping minorities at an airport was disproportionate to that for whites when compared with the total number of travelers, a federal
ment has rejected the notion that profiling operates on this basis, many critics of airline passenger profiling systems maintain that the government cannot be trusted to design egalitarian machinery that ignores the shared ethnic, geo-cultural, or religious backgrounds of the September 11 terrorists. Profiling system proponents counter this concern with an appeal to common sense: We should use what we know about past terrorists. While this may be true in a practical sense, profiling raises more nuanced legal issues. This section presents the major private and government profiling initiatives since September 11 and addresses the practical and legal benefits of both, as well as their drawbacks.

A. Computer Assisted Passenger Prescreening System (CAPPS)

The Federal Aviation Administration ("FAA") mandated passenger profiling in the 1960s in response to increased airliner hijackings during that period.\(^{30}\) Federal security officials believed they could identify potential hijackers based on a profile—a mosaic of personal attributes hijackers typically possessed.\(^{31}\) Specifically, FAA’s "Anti-Air Hijack Profile" established approximately twenty-five characteristics empirically linked with hijackers historically.\(^{32}\) If a passenger fit a "profile,"

---


\(^{31}\) Computer-based profiling generally involves two different types of data: pattern based and subject based. James X. Dempsey & Lara M. Flint, Commercial Data and National Security, 72 GEO. WASH. L. REV. 1459, 1464 (2004). Pattern-based searches commonly occur in the consumer sector in tracking customer purchases and preventing credit card fraud. See id. at 1463. Whereas "'pattern-based' searches . . . refer to searches of large databases when the query does not name a specific individual, address, identification number, or other personally identifiable data element, but instead seeks information that matches or departs from a pattern . . . , 'subject-based' queries are data searches that seek information about a particular subject already under suspicion based on information derived from traditional investigative means, whether that subject is represented by a name, a telephone number, or a bank account number." Id. at 1464. For a discussion of the usefulness of data mining for homeland security, including a review of private and public initiatives such as the Terrorism Information Awareness project ("TIA"), CAPPs II, Multi-State Anti-Terrorism Information Exchange ("MATRIX"), and the Able Danger program, see Jeffrey W. Seifert, CONG. RESEARCH SERV., DATA MINING AND HOMELAND SECURITY: AN OVERVIEW 4-20 (2007), http://www.fas.org/sgp/crs/intel/RL31798.pdf.

\(^{32}\) In United States v. Slocum, a federal appellate court considered the Federal Aviation Administration's Anti-Air Hijack Profile and 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
security officials X-rayed the passenger’s carry-on luggage or investigated the passenger through other search procedures. But FAA abandoned profiling in 1972, finding it ineffective. Instead, FAA created global security checkpoints to X-ray all carry-on luggage.

The perceived need for airline passenger screening was renewed after July 17, 1996 when a Boeing 747, TWA Flight 800 flying from New York to Paris, exploded soon after it took off. Although a defective fuel tank caused the tragedy, government officials initially believed that terrorists had destroyed TWA Flight 800. Consequently, on August 22, 1996 President Bill Clinton announced the creation of the “White House Commission on Aviation Safety and Security.”

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.


34. See, e.g., Santiago v. State, 435 A.2d 499, 500–02 (Md. Ct. Spec. App. 1981); Gregory T. Nojeim, Aviation Security Profiling and Passengers’ Civil Liberties, AIR & SPACE LAW., Summer 1998, at 3, 6 (“Profiling did not work to stop hijacking. In 1972, the last year (1972) the United States used profiles to determine whose carry-on luggage would be X-rayed to stop hijacking, there were 28 hijackings of U.S. passenger aircraft. Hijacking dropped off when profiling was abandoned and every passenger’s carry-on luggage was X-rayed.”).


36. Id.

37. Id.

body, which also was known as 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." The Gore Commission issued its final report in February 1997, making several security recommendations including the revitalization and reformulation of passenger profiling from the 1960s:

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.

FAA developed a computer assisted passenger screening program using this blueprint.

The first-generation computer airline passenger profiling system was developed by Northwest Airlines in 1996 under a grant from FAA. After testing a prototype, Northwest Airlines released the profiling software to other airlines through the FAA in 1997. The profiling

40. WHITE HOUSE COMM'N FINAL REPORT, supra note 38, § 3.19. The airlines themselves protested the Gore Commission's final report, citing implementation costs and decrying government overreach. See Pastemak, supra note 35, at 1. Vice President Al Gore wrote a letter to the president of the Air Transport Association of America, stating, "I want to make it very clear that it is not the intent of this administration or of the commission to create a hardship for the air transportation industry." The O'Reilly Factor: Did Al Gore Increase or Jeopardize Airline Security? (Fox television broadcast Sept. 27, 2001). At least one commentator saw an unnatural relationship between this letter and donations that were subsequently made to the Democratic National Convention in the closing weeks of the 1996 presidential election: $265,000 from American Airlines, $120,000 from Delta Airlines, $115,000 from United Airlines, and $87,000 from Northwest Airlines. Id; see also Walter V. Robinson & Glen Johnson, Airlines Fought Security Changes Despite Warning, Companies Wanted To Avoid Delays, BOSTON GLOBE, Sept. 20, 2001, at A1 (discussing the Gore Commission and airline security standards in the wake of September 11).
41. See Bill Dedman, FAA Looking To Expand System, BOSTON GLOBE, Oct. 12, 2001, at A27 ("CAPS was born in February 1995 in a hotel room in Washington. The host for the small group of government security specialists—which included the FBI, Secret Service and US Customs Service—was Jay Dombrowski, the security chief for Northwest Airlines. CAPS is his creation. 'I wrote it,' he says, 'but they set the profile.'").
42. Id.
software operated through the internal computer reservation system of each airline and was known as the “Computer Assisted Passenger Prescreening System” ("CAPPS").\textsuperscript{43} The government presented this initial device not as a profiling system, but as a “management tool”; its goal was “not to pick a needle out of the haystack, . . . but to make the haystack smaller.”\textsuperscript{44}

CAPPS collects approximately thirty-nine pieces of pre-boarding data on random and ordered bases.\textsuperscript{45} The data that CAPPS collects helps to identify travelers who should be subjected to heightened security procedures. To the distress of privacy advocates, CAPPS profiles are confidential.\textsuperscript{46} As one commentator noted, “[m]aking profiles public is necessary to make them legal, however, doing so would also destroy their usefulness.”\textsuperscript{47} Indeed, the government will not disclose any criterion on which a CAPPS profile is compiled, but some airline security observers discern that CAPPS focuses on specific features such as the method of payment for an airline ticket (i.e., cash or credit);\textsuperscript{48} the timing of a purchase (i.e., immediately before departure or much earlier);\textsuperscript{49} the identity of travelers,\textsuperscript{50} 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 from the flight on which the traveler is aboard; and whether the flight is round trip or one-way.\textsuperscript{51} A traveler identified by CAPPS as a “selectee” is subject to sec-

\textsuperscript{43} See id.; Billie H. Vincent, Letter to the Editor, Or Keep CAPPS On?, SECURITY MGMT., Aug. 2004, at 8, 8. For political reasons, the Federal Aviation Administration ostensibly changed the initial name of CAPPS from “Computer Assisted Passenger Profile System” to “Computer Assisted Passenger Pre-Screening System.” See id. (emphasis added).

\textsuperscript{44} Dedman, supra note 41, at A27 (internal quotation marks omitted).

\textsuperscript{45} Ian Kilroy, Flying in the Face of Privacy, IRISH TIMES, Nov. 5, 2003, at 15.

\textsuperscript{46} See Nojeim, supra note 34, at 5.

\textsuperscript{47} Jamie L. Rhee, Comment, Rational and Constitutional Approaches to Airline Safety in the Face of Terrorist Threats, 49 DEPAUL L. REV. 847, 865 (2000).

\textsuperscript{48} See Richard Lowry, Profiles in Cowardice: How To Deal with the Terrorist Threat—And How Not To, NAT’L REV., Jan. 28, 2002, at 32, 34 (citing a report that the September 11 hijackers of American Airlines Flight 77 “reserved their tickets by credit card, but paid in cash”).

\textsuperscript{49} Morning Edition: Status of Airport Security in America (National Public Radio broadcast Sept. 19, 2001) (reporting that “five of the [September 11] hijackers who later crashed United Airlines Flight 175 into the south tower of the World Trade Center, purchased very expensive one-way tickets; $14,000 for five tickets. The tickets were purchased at the last minute.”).

\textsuperscript{50} See Wave of Security Changes Are Coming After Terrorist Hijacking in U.S., WORLD AIRPORT WK., Sept. 18, 2001, at 2001 WLNR 399475 (“The FAA’s Computer-Assisted Passenger Prescreening System (CAPPS) did not work. . . . Most of these terrorists had been in the country for some time, leading middle-income lifestyles with a good education, good-paying jobs and families.”). For more discussion on the background of would-be terrorists, see sources cited infra note 163.

\textsuperscript{51} Morning Edition, supra note 49.
IS AIRLINE PASSENGER PROFILING NECESSARY?

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).

CAPPS critics asserted that profiling would not work. They noted that profiling outside of the aviation arena had been unsuccessful; for instance, the U.S. Customs Service has not stopped the drug trade using profiling. Profiling system critics also argued that CAPPS would not have prevented even the first documented bombing of a commercial airplane in the United States. That event occurred in 1955 when a passenger’s son covertly packed a bomb in his mother’s luggage to collect insurance policy proceeds. The unsuspecting passenger boarded her fateful flight without drawing any additional security screening. Profiling would likely have been ineffective in this circumstance, where an innocent passenger was manipulated for a sinister purpose. Today, too, the risk of “false negatives,” where crucial people or events are missed, is real.

Accordingly, critics of airline passenger profiling systems dismiss both the theory and operation of CAPPS and related programs as over-inclusive, flagging up to half of all passengers yet missing


53. Nojeim, supra note 34, at 6.

54. See Schiavo, supra note 21, at 295; see also Ted Rohrlich, Response to Terror Aviation Security, L.A. TIMES, Nov. 5, 2001, at A1 (“How long does it take the United States to counter a threat to commercial aviation? In the case of a bomb stowed in luggage in the belly of an airliner, the answer is nearly half a century. And counting. Since a man placed a bomb in his mother’s suitcase in 1955 and blew up a United Airlines flight over Colorado, more than two dozen fatal explosions have been recorded on aircraft around the world.”).

55. Greg Nojeim, legislative counsel at the American Civil Liberties Union and member of the Gore advisory panel, said, “This is not going to make all passengers safer. It only tells the terrorists that they should plant the bomb on someone who doesn’t fit the profile.” Tiffany Danitz, Snooping on Passengers Under FAA’s Watchful Eye, INSIGHT, Mar. 31, 1997, at 22, 23.

Airline passenger profiling critics also have voiced concern about the potential, if not actual use, of race to identify travelers for heightened scrutiny. The DOT represented that CAPPS variables "are not based on the race, ethnicity, religion or gender of passengers." Additionally, the Gore Commission officially recommended the use of safeguards against race-based profiling, stating that profiles should not include information of a constitutionally suspect nature such as race, religion, or national origin. Those safeguards emphasized using verifiable profile factors that are based on data proven to predict risk, setting up strict limits on dissemination of profile records, creating an independent panel to monitor the system and to ensure that civil liberties are not abridged, and continuing profiling only until effective Explosive Detection Systems are developed. The Gore Commission elaborated that

Factors 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.

In 1997, the U.S. Department of Justice ("DOJ") reviewed the selection criteria used by CAPPS and opined that CAPPS did not discriminate unlawfully against passengers or include passenger traits, such as names or mode of dress, that may directly be associated with race, ethnicity, or religion. The DOJ concluded that CAPPS "will not have...

57. See Rosenzweig, supra note 22, at 712.
59. WHITE HOUSE COMM'N FINAL REPORT, supra note 38, § 3.19.
60. Id.
61. Id.
62. DEP'T OF JUSTICE, CIVIL RIGHTS REVIEW, supra note 52 ("The Department of Justice's principal finding is that the FAA's proposed Computer Assisted Screening system ('CAPS') will not discriminate on the basis of race, color, national or ethnic origin, religion, or gender.") (emphasis in original); see also Justice Department Says Proposed Passenger Profiling System Non-Discriminatory, AIR SAFETY WK., Oct. 20, 1997, at 6 (stating that the DOJ reviewed the proposed passenger system and issued recommendations to ensure that CAPS would not discriminate against passengers). See generally Graeme Browning, Big Brother May Get His Big Chance, NAT'L J., Sept. 21, 1996, at 2037 (discussing the use of technology in the computer-generated profiling system).
any unjustified disparate impact on any group of passengers." Profiling system opponents nevertheless found the Gore Commission's stated goals specious, and the DOJ's conclusions unbelievable.

Finally, some CAPPS critics questioned the source, integrity, and potential for misuse of information ostensibly used for airline passenger profiling. Some CAPPS opponents specifically cautioned against the dissemination of CAPPS profiles to other governmental agencies for purposes unrelated to terrorism or aviation security. The American Civil Liberties Union ("ACLU"), in particular, argued that the profiling system raised concerns about personal privacy:

By its very nature, the computerized profiling system runs afoul of a central principle of privacy: Information given for one purpose ought not 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 portions of 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.

To protect airline passenger privacy without a corresponding decline in aviation security, the ACLU imagined security measures other than 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

63. Dep't of Justice, Civil Rights Review, supra note 52.
64. Nojeim, supra note 34, at 7; see also id. at 5 ("Other security measures, which could well be applied to passengers selected by the computerized profiling system . . . include: asking passengers personal questions about their travel; having their luggage sniffed by trained dogs; removing the contents of . . . luggage and examining each item in front of other passengers; escorting the passenger through the airport 'for security reasons' in full view of other passengers; or using sophisticated 'cameras' to peer under their clothing and project a detailed image of their bodies, naked, in a search for contraband, explosives, or weapons."). But see Taipale, supra note 12, at 140-41 ('[I]t is the fetish for absolute secrecy promulgated by the privacy lobby that precludes or delays the development of appropriate technologies to improve security while also protecting civil liberties, and leaves us with little security and brittle privacy protection.' ")
on probable cause of criminality. After September 11, however, aviation security policy makers moved to enhance CAPPS capabilities.

B. **CAPPS II**

Senior government officials described the proposed successor profiling system to CAPPS I as the single most important component of the nation’s aviation security infrastructure. “CAPPS II” was designed to authenticate the identity of commercial airline passengers by comparing each traveler’s passenger name record (“PNR”), including full name, home address, telephone number and date of birth, against governmental databases for security assessment. The aim of CAPPS II was to bridge law enforcement and intelligence databases. “CAPPS II also would have notified law enforcement officials whenever the screening process turned up passengers with outstanding warrants against them, even for non-travel-related incidents.” Controversially, then, CAPPS II exploited commercial databases for counterterrorism purposes.

Opponents argued that CAPPS II would interfere with an airline passenger’s constitutional rights by using commercial databases for purposes unrelated to airline travel. For example, an airline passenger who has filed for bankruptcy or is late in paying credit card bills may be a bad credit risk, but is not necessarily a terrorist threat because of financial delinquency. Nonetheless, a profiling system might equate economic disadvantage with “shiftiness.” In this context, many CAPPS II critics viewed the use of commercial databases to safeguard airline travel as an unacceptably high cost to passenger privacy rights.

To defeat CAPPS II, civil liberty and privacy proponents publicized several embarrassing operational failures of CAPPS I. In September

66. Robert O'Harrow, Jr., Airport Screening System Touted as Improvement, WASH. POST, Aug. 27, 2004, at E03 (“People close to the program said recently that Bush administration officials made it clear this summer that they were worried that the privacy questions sparked by the system could have a political impact during the presidential campaign. Security officials have postponed both testing and implementation of the system until after the election.”). See generally Deborah von Rochow-Leuschner, CAPPS II and the Fourth Amendment: Does It Fly?, 69 J. AIR L. & COM. 139, 146 (2004); Michael J. DeGrave, Note, Airline Passenger Profiling and the Fourth Amendment: Will CAPPS II Be Cleared for Takeoff?, 10 B.U. J. SCI. & TECH. L. 125, 151 (2004).
2004 British pop star Cat Stevens (who became a Muslim in the 1970s and is known today as Yusuf Islam) was removed from an international flight bound for the United States. Stevens’s 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. CAPPS II opponents used these examples to contend that airline passenger profiling systems would not lawfully or reliably make airline travel safer, but rather would produce unintended and negative consequences for airline passengers.

In all, the chief concern surrounding CAPPS II was “mission creep,” whereby information intended for one purpose might be exploited for unintended purposes. CAPPS II critics argued that the information comprising an airline passenger profile might unacceptably slip, bit-by-bit, into the hands of non-TSA governmental actors for uses outside of aviation security. In this way, airline passenger profiling systems are unique for their invasiveness.

For example, if you do not buy the book Amazon.com recommended to you based on other customers’ buying patterns, the negative conse-


71. Id.; see also Today (NBC television broadcast Sept. 23, 2004). Matt Lauer asked Asa Hutchinson, Homeland Security Undersecretary, regarding the placement of Cat Stevens on a terror watch list: “Mr. Secretary, this is a high profile example. How often do you think this really happens?” “Very infrequently,” Hutchinson replied. Id. No-Fly and selectee lists are administered by the Transportation Security Intelligence Service as “security directives” issued by the Under Secretary of the TSA. See 49 U.S.C.A. § 114(l)(2)(A) (West 2007). Security directives are issued without notice or opportunity for public comment. Id.


75. See Angela Kim, ACLU Skeptical of TSA’s New Passenger Screening System, AVIATION DAILY, Aug. 30, 2004, at 1. David Stanley, Communications Director of ACLU’s Technology and Liberty Program, stated, “Identity-based security systems are never going to be effective. The focus should be on physical screening, good intelligence, [and] good police footwork to chase down leads.” Id. Independent of aviation profiling programs, the Federal Bureau of Investigation is currently developing a computer profiling system—the System to Assess Risk (“STAR”)—to identify emergent foreign threats in order to assign risk scores to possible suspects such as credit bureaus assign rating to consumers based on spending behavior and debt. See Ellen Nakashima, FBI Plans Initiative To Profile Terrorists; Potential Targets Get Risk Rating, WASH. POST, July 11, 2007, at A08.
quences 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.\footnote{76. Dempsey & Flint, supra note 31, at 1471.}

These criticisms eventually reached TSA, which offered to make several modifications to the proposed CAPPS II program.\footnote{77. See Interim Final Privacy Notice, 68 Fed. Reg. 45,265 (Aug. 1, 2003); Privacy Notice Act, 68 Fed. Reg. 2101 (Jan. 15, 2003).}

TSA suggested three significant amendments to the CAPPS II design.\footnote{78. Interim Final Privacy Notice, 68 Fed. Reg. at 45,267.} First, TSA agreed to erase most passenger information in the CAPPS II system within seven days after passengers completed their scheduled travel.\footnote{79. Id. at 45,269.} TSA also proposed appellate mechanisms for passengers erroneously targeted for heightened, secondary security screening.\footnote{80. Id. at 45,267.} Most important, TSA proposed limiting the use of private commercial data to compose a traveler's security profile.\footnote{81. Id. at 45,266.} In particular, TSA proposed transmitting PNR information to commercial data providers solely for the purpose of authenticating a passenger's identity.\footnote{82. Id.} Commercial data miners, in turn, would evaluate whether a passenger is who he represented he was when reserving a flight.\footnote{83. Id.} On completion of this authentication process, the CAPPS II system would review a passenger's commercial identity against intelligence and law enforcement databases.\footnote{84. Id.} Passengers positively identified without any corresponding matches with intelligence or law enforcement data would proceed to their flights.\footnote{85. Id.} Those passengers with more remarkable profiles would be subjected to further search or law enforcement action or both.\footnote{CAPPS II opponents viewed these measures as insufficient and CAPPS II never materialized.}

Apart from external criticism and its substantive problems, CAPPS II was defeated because it was a marketing disaster. By developing the system without notice or opportunity for meaningful public comment, TSA did precisely what privacy advocates cautioned CAPPS II would
do—deny citizens due process of the law. The fact that CAPPS II was developed behind the closed doors fueled civil libertarian charges that the federal government was overrunning the Constitution.

Opposition to the CAPPS II program peaked when the nation learned that some airlines voluntarily provided TSA with lists of their respective passengers for testing in the CAPPS II system. JetBlue Airways, for instance, was sued for providing a data-mining government contractor with millions of passenger records (including names, addresses, and phone numbers). A consumer research company evaluated these records, which included information about each passenger's demographics, including occupation, income, gender, home- and car-ownership history, and household composition. This information was collected and transmitted without the knowledge or consent of the passengers whose identity was disclosed. Several other airlines were sued as their collaboration with the federal government to develop CAPPS II emboldened profiling system opponents. Ultimately, CAPPS II was defeated by the concern of marrying PNR data with commercial and law enforcement databases. TSA abandoned CAPPS II on July 13, 2004, after the U.S. General Accounting Office reported that “[u]ntil TSA finalizes its privacy plans for CAPPS II and addresses such concerns, we lack assurance that the system will fully comply with the Privacy Act.”

C. Secure Flight

TSA followed its aborted CAPPS II program with “Secure Flight,” in August 2004. Secure Flight was a product of the “Intelligence Reform and Terrorism Act of 2004” through which Congress required

---


90. AVIATION SECURITY: COMPUTER-ASSISTED PASSENGER PRESCREENING SYSTEM FACES SIGNIFICANT IMPLEMENTATION CHALLENGES, supra note 74, at 42.
TSA to "commence testing of an advanced passenger prescreening system that will allow the Department of Homeland Security ("DHS") to assume the performance of comparing passenger information . . . to the automatic selectee and no fly lists." Secure Flight was designed to improve government "No-Fly" and "automatic selectee" lists. It was designed to reduce the number of domestic airline passengers pulled aside for more rigorous screening while increasing the chance of catching known or suspected terrorists. Secure Flight would be built on the technology platform of its controversial predecessor, CAPPS II. The technical similarity between CAPPS II and Secure Flight encouraged the contention that Secure Flight was a euphemism, nothing more than "a stripped-down version of the old CAPPS II system with a more consumer-friendly name."

Similar to CAPPS II, Secure Flight represented ongoing efforts by the executive branch of the federal government to involve itself directly with aviation security after September 11. For example, Secure Flight would shift passenger prescreening responsibilities from the privatized airlines to the federal government. Airlines currently compare passenger names with government provided terrorist watch lists, which are based on recommendations and information received from federal agencies, including intelligence and law enforcement agencies. Certain sen-

94. Bill Scannell, TSA Cannot Be Trusted, USA TODAY, Sept. 28, 2004, at 12A.
sitive government watch list information, however, is not available to airlines. To close this intelligence gap, Secure Flight would have unified 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 a Terrorist Screening Database ("TSDB").

TSA promoted Secure Flight as a system different from CAPPS II. Secure Flight would access commercial databases only to confirm the actual identity of a traveler and to compute a risk score only for purposes related to commercial aviation security. Additionally, TSA proposed that Secure Flight would be augmented by an appellate process for travelers mistakenly or inequitably selected for secondary screening. Finally, TSA proposed employing a passenger advocate to whom passengers could turn if they were unfairly flagged for heightened security treatment. After providing public notice and entering into a multimillion-dollar contract with IBM, TSA began testing Secure Flight by collecting historical passenger information and comparing that information with commercial data. This comparison was an attempt to resolve false positive matches against TSDB records.

To test Secure Flight, TSA ordered more than seventy domestic airlines to submit PNRs for the month of June 2004. The data that TSA requested "varie[d] from airline to airline. . . . It may also [have] include[d] 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." Thus, where CAPPS II . . . required the airlines to turn over only passenger names, dates of birth, home addresses and home telephone numbers[,] Secure

---


97. David Hughes, ‘Secure Flight’ Draws Fire: Privacy Advocates Fear the U.S. Security Bureaucracy Will Trample Individual Rights, AVIATION WK. & SPACE TECH., Nov. 1, 2004, at 54 (quoting Justin Oberman, Director of TSA’s Office of National Risk Assessment, in connection with a "very robust redress policy" that will give the public the ability to come in and appeal to the passenger advocate).


Flight mandate[d] 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.100 This prompted privacy advocates to contend Secure Flight was more invasive than CAPPS II.101

In fact, Secure Flight generated the type of constitutionally based opposition that defeated the CAPPS II program.102 Citizens themselves expressed mixed opinions about Secure Flight, including whether and how it would avoid or remedy circumstances of identity theft.103 Meanwhile, 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 TSA produce documents explaining how or if the FBI intended to protect the privacy of travelers

100. Jon Hilkevitch, Privacy Fears Dog Terror Screen; Foes: New System Is More Intrusive, CHI. TRIB., Sept. 22, 2004, at 13; see also Leslie Miller, Feds Criticized for Ordering Airlines To Provide Traveler Data, STAR-LEDGER (Newark, N.J.), Nov. 14, 2004, at 23 ("The lists are ‘a hodgepodge of information, accurate and inaccurate,’ [an ACLU lawyer] said. ‘They’re the basement of the program, and the floor is rotten.’"); USA To Test Screening Programme, FLIGHT INT’L (London), Aug. 31, 2004, at 8 ("[A]ccording to [a] TSA administrator, ‘Secure Flight differs from earlier proposed systems by focusing efforts on looking for known or suspected terrorists, rather than using it for other law-enforcement purposes.’").

101. Scannell, supra note 94, at 12A ("The TSA wants these 54 million records—which include everything from credit card numbers to whether a kosher meal was requested—to test Secure Flight, a revised version of a discredited proposal for a passenger profiling system, known as CAPPS II. The TSA does not deserve our trust.").


103. See All for It—And Completely Opposed, AIR SAFETY Wk., Oct. 11, 2004; see also Jennifer Babson, False Alarm Diverts Delta Flight, MIAMI HERALD, Dec. 27, 2004, at 1B (reporting diversion of 132-passenger flight from Colombia to Atlanta after the name of a passenger who was the victim of identity theft was mistakenly thought to be someone on a federal security watch list); Editorial, No-Fly List Belongs in the Wastebasket, ST. PETERSBURG TIMES, Nov. 11, 2007, at 2P ("A list that can’t distinguish between the real Robert Johnson and all the others isn’t worth much. What makes these lists even more questionable is that some of the most dangerous terrorist suspects are not on them because intelligence agencies don’t want to reveal their names."); Unsecureflight.com, http://www.unsecureflight.com (last visited Oct. 31, 2007). Consider also this exchange on National Public Radio between a private citizen (referred to in the following dialogue as "Caller") and Mark Hatfield, TSA Director of Communications and Public Information (referred to in the following dialogue as "TSA"):

[CALLER]: . . . I have been stopped 22 different times by the TSA, the FBI and the Secret Service. My name is similar to that of another person in Chicago, Illinois, who is apparently a financier for al-Qaeda. I have done everything possible to keep this from happening, and wanted to know if there’s any advice you might be able to give me to get my name or my comparison name off this list.
in the course of maintaining records in terrorist screening databases. EPIC's specific critique was that profiling systems such as Secure Flight would deny airline passengers any judicially enforceable rights:

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

---

[CORRECTION]

[TSA]: ... have you contacted the TSA Contact Center and gone through the process of submitting your name and filling out the form so that we can take a look at why that might be happening? I can't address what's causing your experiences with the FBI or the Secret Service, but as far as the airport security experience, if you're getting selected for secondary screening or being delayed before you're allowed to board, we're—we've got the system set up ...

[CALLER]: It's beyond secondary screening. ... I've been pulled off to the tarmac in Denver and questioned by two Secret Service agents; a very embarrassing issue. And, yes, I have been in contact with the TSA and I've really had no recourse other than to get every frequent-flier card I can and, again, to go one-on-one with a TSA agent as I'm getting ready to the board the plane.

[TSA]: ... Secure Flight is a very clean-focused, well-defined program, and I think some of the references in that last exchange you had were to the predecessor, which was CAPPS II, which never really got off the ground and, in fact, it did grow beyond its original intent as a passenger prescreening system focused solely on aviation, and I think that was part of its demise. It just—it started getting attachments and extra features. It got too heavy to take off ....

*Talk of the Nation, supra* note 26. In Green v. Transportation Security Administration, airline passengers sued TSA on the ground that TSA's "maintenance, management, and dissemination of the No-Fly List was unconstitutional." 351 F. Supp. 2d 1119, 1122 (W.D. Wash. 2005); see also Matthew L. Wald & John Schwartz, *Airport Screening Program's Expansion Led to Its Demise*, SUN-SENTINEL (Ft. Lauderdale), Sept. 20, 2004, at 3A (discussing privacy concerns with the Secure Flight system).

protections are available, nor [is] information about how long TSA will keep the PNR [passenger name record] data that it collects for Secure Flight, even though the agency intends to launch the program early next year.105

Despite this criticism, federal efforts to develop Secure Flight proceeded for four years at an expense in excess of $200 million. On September 19, 2005 however, Secure Flight was dealt a serious setback as the Aviation Security Advisory Committee forwarded a report of a nine-member panel of security and privacy experts—the Secure Flight Working Group ("SFWG")—to TSA without recommendation:

The SFWG found that TSA has failed to answer certain key questions about Secure Flight: First and foremost, TSA has not articulated what the specific goals of Secure Flight are. Based on the limited test results presented to us, we cannot assess whether even the general goal of evaluating passengers for the risk they represent to aviation security is a realistic or feasible one or how TSA proposes to achieve it.106

These and other unresolved concerns about the purpose and architecture of Secure Flight doomed the program in 2006.107 Nonetheless, DHS contends that it is working to "reduce mistakes, protect privacy rights and achieve . . . reliability" in order to release a revamped form of Secure Flight sometime between 2008 and 2010.108

105. Reactions to Secure Flight, AIR SAFETY WK., Oct. 4, 2004, at 1, available at 2004 WLNR 825677 (quoting a September 28, 2004 EPIC statement); see also Michael J. Sniffen, Agency Admits It Broke Law, MIAMI HERALD, Dec. 23, 2006, at 9A ("The Homeland Security Department admitted . . . it violated the Privacy Act two years ago by obtaining more commercial data about U.S. airline passengers than it had announced it would. . . . But the privacy office still couldn't bring itself to use the word 'violate.' Instead, the privacy office said, 'TSA announced one testing program, but conducted an entirely different one.'").


D. Biometrics and the Registered Traveler Program

Part of the controversy surrounding security programs like CAPPS, CAPPS II, and Secure Flight centered on their involuntary nature. But privatized efforts are also underway to develop profiling systems that operate on a voluntary basis, following a Congressional directive to develop advanced biometric technology applications for aviation security.109 The product of this mandate is the “Registered Traveler” program.110

The Registered Traveler program is a federal credentialing effort that invites passengers to consent to profiling by volunteering their biographical and biometric data for essentially low level federal security clearance. Initially tested at five airports,111 Registered Traveler offers an exchange with airline passengers: a biometric-encoded pass card or “smart card” for biographical information, fingerprints, iris images, and a membership fee.112 After also undergoing a security threat assess-


111. The Registered Traveler Program was tested for fourteen months at airports in Washington, D.C., Boston, Houston, Los Angeles, and Minneapolis. Greenemeier, supra note 68, at 1; see also British Airways Has Agreed, AVIATION WK. & SPACE TECH., Sept. 4, 2006, at 18 (noting that British Airways was the first airline to join the Registered Traveler Program). That different airports may facilitate Registered Traveler programs has led to the creation of a coalition of ten to twenty airports throughout the United States whose goal is a national, interoperable system to allow for compatibility among private providers of the Registered Traveler program. See U.S. DEP’T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE REGISTERED TRAVELER INTEROPERABILITY PILOT 2 (2006), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_rt.pdf.

Registered Traveler is chiefly a private undertaking. TSA performs a limited, inherently governmental and facilitating role such as providing security threat assessment for adjudication and program oversight, as well as conducting physical screening at TSA checkpoints. Meanwhile, private service providers at sponsoring airports administer Registered Traveler. Verified Identity Pass, a New York company led by the founder of CourtTV, is one of four private service providers for Registered Traveler through a program called “Clear.” Available through the Internet or in person at temporary cubicles in selected airports, “Clear” allows passengers to obtain a “clear card” by filling out an application, paying a membership fee (of which $28 is a TSA enrollment fee), and providing credentialing information, e.g., driver’s license number, previous home address, and social security number. In an open

113. See Stephen Majors, Passengers Skip Line—For a Price, MIAMI HERALD, Jan. 6, 2007, at 1C.
115. See id.
116. See Edward Hasbrouck, Mr. Brill Builds His Own Airline Screening Service, PRIVACY J., Oct. 2005, at 1; see also Paul Hoversten, TSA Sets June 20 as Launch Date for Nationwide Registered Traveler Program, HOMELAND SECURITY & DEF., Nov. 9, 2005, at 1 (“It is hard to imagine that the government could offer the efficiency, customer service, incentives for continual innovation, and privacy protections that a robustly competitive private sector industry could provide,’ [Steven Brill] said.”). There are three other TSA-approved service providers in addition to Verified Identity Pass: Unisys Corporation of Reston, Virginia, Verant Identification Systems, Inc. of Rochester, New York, and Vigilant Solutions of Jacksonville, Florida.
117. Carol Pucci, Travelers Weigh Benefits of New Security Program, SEATTLE TIMES, Jan. 29, 2006, at J1; see also Thomas Frank, TSA: Program May Use Fliers’ Financial Data, USA TODAY, Jan. 23, 2006, at 3A (reporting that Verified Identity Pass experimented with giving applicants quizzes generated by commercial data to authenticate their identity, but some questions were either too difficult, such as the year someone received their social security number, or so easy that ‘‘[a] terrorist . . . could pass the quiz on behalf of any person’’”). DHS requires sponsoring entities and service providers of the Registered Traveler program to furnish Registered Traveler applicants with a written “TSA Privacy Statement” at the time of application, stating in part:

Routine Uses. The information will be used by and disclosed to TSA personnel and contractors or other agents who need the information to assist in the operation of the Registered Traveler program. Additionally, TSA may share this information with airports and airlines to the extent necessary to ensure proper identification, ticketing, security screening and boarding of Registered Travelers. TSA may disclose information to appropriate law enforcement or other government agencies as necessary to identify and respond to outstanding criminal warrants or potential threats to transportation security.

letter, the CEO of Verified Identity Pass introduced “Clear” by acknowledging the tension between national security and personal privacy with which even voluntary profiling systems contend:

In the post 9-11 era we have to take new measures to protect ourselves yet not destroy our way of life by strangling the free flow of people and commerce. Somehow, we have to find common sense solutions that don’t make everyone a suspect and create security bottlenecks everywhere we go. To be blunt, that means we need a fair, sensible way not to treat everyone the same when it comes to terrorism protection.

[W]e think we have a special responsibility to protect your privacy. Yes, we are using biometric identifiers such as fingerprints and iris images. Yes, your enrollment application will be submitted to the government for a basic security threat assessment before we can issue you a Clear card. But we do not believe the process and the questions stop there. We know that this kind of new idea and new process is bound to make many people uneasy about what we are doing with their personal information, especially at a time when every day seems to bring new headlines about identity theft. . . . [W]e’ve made ourselves strictly and publicly accountable for keeping them.”

Though consumer-friendly and relatively transparent when compared to CAPPS, CAPPS II, and Secure Flight, the Registered Traveler program has been criticized as involving an unwarranted invasion of privacy. Specifically, the ACLU has argued that the supposed benefits of Registered Traveler do not justify the important privacy rights that airline passengers must forgo merely to obtain the status of “Trusted Traveler.” Additionally, critics of the Registered Traveler program note that it creates two classes of airline passengers, those who can afford the label of “Trusted Traveler” and those who cannot: “[T]he system would give special treatment to people based on their ability to pay [and while] some travelers buy extra services, . . . the issue here is security, not extra leg room or an in-flight meal.”

119. See Jeffrey Leib, “What Happened to the Benefits?” Says Travel Group, DENVER POST, Jan. 22, 2006, at C-01; see also Leslie Miller, TSA Toughens Registered Traveler Rules, WASH. POST, Jan. 21, 2006, at A11 (reporting that companies selling Registered Traveler cards must demonstrate whether “applicants are members of terrorist sleeper cells by plowing through bank records, insurance data and other personal information available commercially—or by some other method”).
the Registered Traveler program may destabilize existing anti-terrorism programs by enabling terrorist leaders to find out if their operatives are on the terrorist watch lists against which Registered Travelers are compared.121 As one critic contended, "[m]embers of a terrorist sleeper cell could obtain false identification and become registered travelers, using the lessened security screening to evade detection and commit a terrorist act."122

Aside from operation concerns, Registered Traveler is attractive to business interests. Business travelers have embraced Registered Traveler for making airline travel less burdensome. Private vendors like Verified Identity Pass, too, have profited by partnering with airports to receive a cut of the annual fee collected from Trusted Travelers. Airports, in turn, see marketing and customer service opportunities in Registered Traveler. Airport authorities at Logan International Airport in Boston, Massachusetts, for example, have stimulated interest in the Registered Traveler program by giving "Trusted Travelers" discounts on airport parking and dining.123 Such business opportunities have raised the question whether Registered Traveler is more of a revenue scheme than an anti-terrorism device.

TSA had planned to roll out Registered Traveler nationally in 2007, with approximately twenty airports participating in the program by 2008. By mid-2007, however, the future of the Registered Traveler pro-

---

121. Dirty Socks? Enplane in the Fast Lane; Program in Works Will Let Frequent Fliers Pay for a Card That's a Bit like E-ZPass, MORNING CALL (Allentown, Pa.), Jan. 21, 2006, at A1 ("[The] chief technology officer of Computerpane Internet Security, Inc. said [that the Registered Traveler Program was] an easy way to test if your potential mission-goers have themselves on the list. . . ."); see also Paul Hudson, Aviation Security Headed in Wrong Direction, AIR & SPACE LAW., Summer 2002, at 6, 7 ("A smart card issued to certain frequent flyers is reverse or positive profiling, and profiling has generally been a failure in aviation security, particularly when used for antihijacking security."); Traci Watson, U.S. Looks at Which Tech Proposals Will Fly, USA TODAY, Nov. 26, 2001, at 4A ("Seventeen of the nineteen Sept. 11 terrorists were ordinary, law-abiding citizens until after they were on the planes," says James Wayman, director of the National Biometrics Test Center at San Jose State University. 'They had Social Security cards and frequent-flier numbers. How could any biometric device have stopped them?'").

122. Jay Boehmer, Trusted Traveler To Fly, BUS. TRAVEL NEWS, Nov. 14, 2005, at 1, 32 ("When asked to make sure that nobody in the Registered Traveler program is a terrorist, [Tom Ridge, the first secretary of DHS], said, 'Candidly, there is no guarantee. But as you manage that risk, you also have to realize that, in a post-9/11 world, it is very unlikely a group of people can take over an airplane and turn it into a missile.'").

gram was uncertain. In August 2007 Senator Mel Martinez (R-Fla.) successfully proposed to authorize DHS to follow the lead of Canada, Israel, Japan, the Netherlands, and the United Kingdom by creating an international registered traveler program. At the same time, however, TSA Administrator Kip Hawley insisted that the Registered Traveler program "was not a security program" and that, "[a]fter prioritizing our security initiatives based on risk, TSA decided that taxpayers' resources are best applied to more critical needs."  

III. DISCUSSION

As the fifth anniversary of September 11 approached, Americans considered whether commercial airline security had improved since 2001. The unsuccessful August 10, 2006 terrorist plot to detonate liquid explosives aboard international airplanes bound for the United States offered a somber perspective. The two week period following that attempt was discouraging also. During that period, approximately twenty-five "security incidents" occurred at airports and nine commercial airplanes were diverted from their intended destinations. Some jetliners were escorted to the ground by fighter planes. These "incidents" suggested that crises had become a regular feature of worldwide commercial airline travel after September 11.

On August 25, 2006 alone, seven commercial flights were reported disrupted. A Continental Airlines flight from Buenos Aires, Argentina was delayed at its planned stopover in Houston, Texas when a college student aboard the airplane was detained for packing dynamite in his checked luggage. An American Airlines flight from Manchester,
England to Chicago, Illinois was forced to land in Bangor, Maine at a former military base because of an unspecified threat. A U.S. Airways jet destined for Charlotte, North Carolina from Phoenix, Arizona made an emergency landing in Oklahoma City, Oklahoma after federal air marshals tackled and subdued a disruptive passenger who had pushed a flight attendant. A Corpus Christi, Texas to Bakersfield, California Continental Airlines flight was held at its scheduled stop in El Paso, Texas after a missing lavatory panel was discovered. A utility knife was discovered on an empty passenger seat of a Pennsylvania to Connecticut U.S. Airways flight. An Aer Lingus flight originating in New York was evacuated during a scheduled stopover in western Ireland following an unfounded bomb threat. Finally, a United Airlines flight bound for LaGuardia Airport in New York from Chicago, Illinois was evacuated and delayed when a ten-year-old boy falsely announced that he had a bomb strapped to his leg.

These scares were caused by people with bad intentions or bad judgment, not merely by objects like bombs and knives. That a ten-year-old boy could cause an evacuation of an airplane of a hundred or more passengers aptly illustrates the challenge confronting aviation security officials. Aesop's fable of a boy who falsely cried wolf so often that he lost credibility within his community has little application to the commercial aviation industry. Authorities responsible for aviation security must assume the worst and entertain both credible and incredible threats at any time, every time. Terrorism is asymmetrical

132. Id.; see also NBC Nightly News with Brian Williams, supra note 128.
133. FBI: Dynamite Found in Luggage, supra note 131.
134. Id.
135. Id.
136. Id.
137. NBC Nightly News with Brian Williams, supra note 128.
138. The government's own credibility is at stake in its creation and enforcement of aviation security policy. For example, TSA publicizes that "[a]irlines can and should automatically de-select any 8-year-olds out there that appear to be on a watch list. Whether you're eight or 80, the most common occurrence is name confusion and individuals are told they are on the no fly list when in fact, they are not." Myth Busters: The "No Fly" List Includes an 8-Year Old Boy, http://www.tsa.gov/approach/mythbusters/8yo_noflylist.shtm (last visited Oct. 13, 2007). Yet, stories of children on watch lists persist. See, e.g., Ken Kaye, Coral Springs Boy, 7, on No-Fly List Has Been Delayed at Airport Three Times, S. FLA. SUN-SENTINEL, July 24, 2007, at IA (reporting that 7-year-old Michael Martin had been denied boarding on multiple occasions since September 11, 2001 presumably because he shares the name of an Irish terrorist who was convicted in an Arizona smuggling ring that attempted to ship bomb detonators to the Irish Republican Army); see also supra notes 26 and 103 and accompanying text.
139. See, e.g., CNN Newsroom: National Intelligence Report on Terrorist Threat Released (CNN television broadcast July 17, 2007) ("We cannot know the enemy's calculation, nor when it will shift. We prepare for and anticipate both, with the realization that the enemy only has to be
in this respect, and the fact terrorists need to be successful only once to achieve disaster has become a central tenet of the doctrine of preemption that dominates U.S. foreign policy under President George W. Bush and Vice President Dick Cheney. Profiling airline passengers may help to right this acute imbalance. As detailed below, however, whether certain civil liberties should be negotiated or trumped in the name of national security and airline safety is debatable, particularly as government surveillance, domestic wiretapping, and eavesdropping programs are a source of contemporary public concern.

A. Identifying the Enemy

The initial questions borne of September 11 were "What happened?" and "Who did this?" These questions are resolved. The more difficult questions of who is a terrorist and what, if anything, can be done to identify and preempt future perpetrators remain unanswered. To resolve these questions, federal aviation security policy makers who favor profiling airline passengers assume 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 move secretly among law-abiding airline passengers. Ironically, in the course of rooting out the proverbial enemy among us, the federal government’s investigative energies are directed internally to "us" and thus threaten the bundle of travel rights that exist in the United States enjoy.


142. See 9/11 Report, supra note 19, at 1–14; see also Brian M. Jenkins, The Organization Men: Anatomy of a Terrorist Attack, in How Did This Happen? Terrorism and the New War 1–14 (James F. Hoge, Jr. & Gideon Rose eds., 2001).

143. In Kent v. Dulles, 357 U.S. 116, 125–26 (1958), the U.S. Supreme Court recognized that [the right to travel is a part of the “liberty” of which the citizen cannot be deprived...
That CAPPS identified a majority of the September 11 terrorists may justify profiling and a corresponding infringement of some existing travel and privacy rights. After all, CAPPS effectively identified "them." That is, ten of the nineteen hijackers were identified by then operational profiling systems. That the consequence of being identified was minimal for the terrorists is another matter. The terrorists' baggage was detained until the terrorists themselves boarded the doomed airplanes. This represents a defect in enforcement, not profiling. By concentrating on bombs instead of people, security officials failed to use profiling systems effectively. But, within a week after September 11, government officials began to talk more about observation of passengers as an important layer of aviation security. As a result, a corps of "behavior detection officers" has evolved among TSA's approximately 43,000 screeners in a program called "Screening Passengers by Observation Technique" ("SPOT"). Success of this program is critical if commercial aviation security policy is to get beyond "the culture of contraband."

For years Israeli aviation security officials have focused on airline

without due process of law under the Fifth Amendment. . . . [D]eeply engrained in our history [is] this freedom of movement . . . [a]cross frontiers in either direction, and inside frontiers. . . . Freedom of movement is basic in our scheme of values. The modern right to travel may have originated in clause 42 of the Magna Carta:

It shall be lawful in future for anyone, without prejudicing the allegiance due to us, to leave our kingdom and return safely and securely by land and water, save, in the public interest, for a short period in time of war—except for those imprisoned or outlawed in accordance with the law of the kingdom and natives of a land that is at war with us and merchants (who shall be treated as aforesaid).

Magna Carta, cl. 42 (1215), reprinted in RALPH V. TURNER, MAGNA CARTA: THROUGH THE AGES 231–32 (2003); see also Heather E. Reser, Comment, Airline Terrorism: The Effect of Tightened Security on the Right To Travel, 63 J. AIR L. & COM. 819, 821 (1998) (arguing that increased security and travel restrictions interfere with the right to travel). Contra Tracey Maclin, The Decline of the Right of Locomotion: The Fourth Amendment on the Streets, 75 CORNELL L. REV. 1258 (1990). Although "Americans have enjoyed the freedom to walk the streets and move about the country free from unreasonable government intrusion for many years[,]" id. at 1260, "not all Americans have been able to move freely about the country. In many parts of colonial America, both North and South, Negroes were required to carry 'passes.'" Id. at 1260 n.4 (emphasis in original).


passengers themselves. They screen passengers individually and personally in a process taking hours per person.\textsuperscript{147} The United States has not had to cope with the pervasive terrorism that threatens Israel, and intentionally time-consuming airline passenger profiling is neither a standard nor a welcomed feature in the United States. But it appears to be effective.\textsuperscript{148} In 1986, for example, a pregnant woman on a London-to-Tel Aviv flight was pulled aside by El Al for further screening. Security officials were suspicious of a pregnant woman traveling alone. In fact, unbeknownst to the passenger, her Jordanian boyfriend had planted a bomb in her carry-on luggage that would have killed the 375 people on her flight.\textsuperscript{149} As a result of security processes like these, no successful hijackings have ever occurred out of an Israeli airport.\textsuperscript{150}

Behavioral profiling has flaws, though. "Learning to defeat poorly trained screeners is a lot easier than learning to fly a jumbo jet[,]"\textsuperscript{151} and the occurrence of "false positives" may be higher where human beings are responsible for profiling. Indeed, where a computer might generate a false positive because it is insensitive to details outside of its protocol, observation-based profiling involves a subjective, perhaps discriminatory determination that may confuse quirky passengers for terrorists. Naturally, not every passenger who is anxious about flying, with sweaty palms and nervous movements, is a terrorist.\textsuperscript{152}


\textsuperscript{148} Cf. id. ("I sort of got the feeling at certain airports that [improper treatment of Arab or gentile passengers] wasn't frowned upon, that what was important was that the planes left on time and didn't blow up," [said a former Israeli airport security screener who supports airline passenger profiling].")

\textsuperscript{149} See Daniel Brook, Profiling’s Gender Gap: If a Woman Can Do Anything a Man Can Do, Doesn’t That Include Terrorism?, LEGAL AFF., Sept.–Oct. 2003, at 44 (describing the DOJ’s post-September 11, 2001 National Security Entry Exit Registration System that was designed to require visa holders from 24 Muslim countries (and North Korea) to register with the U.S. Bureau of Citizenship and Immigration Services; it applied only to men); Lowry, supra note 48, at 32 ("It is inarguable that sensitivity about profiling in the U.S. made the September 11 hijackers’ job easier. Their plot would have simply been a non-starter in Israel. There, passengers are divided into three categories: Israelis and foreign Jews, non-Jewish foreigners, and anyone with an Arab name. Those in third category get lots of special attention . . . .")

\textsuperscript{150} Bernard E. Harcourt, Search and Defend, N.Y. TIMES, Aug. 25, 2006, at A21 ("Israelis . . . recruit their officers mostly from the military, subject them to stringent tests . . . and give them nine weeks of training in behavior recognition. This is a far cry from the T.S.A.’s program: recruits are routine screeners, required only to have a high school degree and a criminal background check; they are given four days of classroom training in observation and questioning techniques, three days of field practice, then sent out on the job.").

\textsuperscript{151} Id.

\textsuperscript{152} See, e.g., Sedigh v. Delta Airlines, Inc., 850 F. Supp. 197, 198–99 (E.D.N.Y. 1994); see also Editorial, Clerics’ Lawsuit Threatens Security of All Passengers, USA TODAY, Mar. 27, 2007, at 19A ("Six Muslim clerics, returning from a religious conference in Minneapolis, were removed from a US Airways flight after passengers and crew raised alarms. . . . The six say they are innocent victims of ethnic profiling for merely praying quietly in Arabic at the terminal. . . . Suing passengers who merely report such behavior threatens everyone’s ability to travel
Scholarship suggests that behavioral profiling may be impossible, not simply error-prone like computer programs. Profiling is based on the presumption that individuals who become involved in global terrorism share features. Terrorists may have common social backgrounds or common psychological make-up. Additionally, individuals drawn to terrorism may have been recruited because of common situations. A January 2007 study by Professor Edwin Bakker of the Netherlands Clingendael Institute of International Relations showed that most of 242 Islamic radicals who were convicted or accused of planning terrorist attacks in Europe from 2001 to 2006 were men of Arab descent who had been born and raised in Europe and came from lower or middle-class backgrounds. They ranged from sixteen to fifty-nine years of age at the time of arrest (the average was twenty-seven years old) and about one in four had a criminal record. Still, identifying terrorists beyond these demographics proves problematic.

More attention should be devoted to understanding the personal experiences that motivate people to become radicals. For example, Dutch researchers claim that one reason why more young women are becoming involved in radical networks in the Netherlands is that they come under the influence of “Moroccan lover boys,” “charismatic Romeos who manipulate emotionally needy women into committing criminal acts.” Meanwhile, the social background of the Salafi mujahedin, for example—their geographical origins, socioeconomic status, education, faith as youth, and occupation—debunk common stereotypes of terrorists. Often, members of the Salafi mujahedin enjoyed a modern education, became devout before joining the jihad, and were not hardened criminals.
Profiling—whether by computer or person—is further complicated because theories for identifying terrorists often suffer from a lack of specificity and corroborative data. In psychological terms, the “personal pathology thesis” that terrorists suffer from mental illnesses finds little support. The convenient and comforting theory that terrorists are sociopaths and psychopaths or fanatics with overvalued ideas, obsessed like anorexic people with body dysmorphic disorder, appears to be unsupported. The thesis that terrorists suffer from pathological narcissism, paranoia, or an authoritarian personality have found little empirical support, too. Of a sample of sixty-one “terrorists” about whom some childhood data existed, only four had evidence of antisocial personality disorder. Two of those individuals were Christian converts, i.e., Jose Padilla and Richard Reid. Even the fact that terrorist tactics involve suicide is explicable in a cultural context of martyrdom rather than insanity. The social circumstances that have led individuals to sample of sixty-nine mujahedin described their childhoods in positive or neutral terms—“shy, introverted, serious, quiet, bright, excellent student, loner, pleasant, easy-going, happy, [and] gentle.” Id. at 85; see also Donald G. McNeil, Jr., Assets of a Bombing Suspect: Keen Wit, Religious Soul, Angry Temper, N.Y. TIMES, Oct. 6, 1998, at A6 (describing the life and character of a suspected terrorist).


163. Sageman, supra note 6, at 81.

164. Id.


166. E.g., Sageman, supra note 6, at 82–83 (“Like the Japanese kamikaze . . . the Salafi shahada . . . legitimizes and encourages the nobility of martyrdom. . . . Even the Christian Bible
join jihad, including age, place of recruitment, faith, employment, and relative deprivation, are multivariable. Consequently, profiling may be impracticable because, "[i]n terms of generating a common profile of the global Salafi mujahed[, for example], there are as many profiles as there are clusters of mujahedin." 

Finally, apart from questions about the underlying psychophysiological aspects of profiling is the overriding question whether profiling systems are scientifically reliable as a matter of law. Profiling systems may be like polygraph machines in that their usefulness to law enforcement, if any, frequently ends at the courthouse steps as an inadmissible technique. Under Daubert v. Merrell Dow Pharmaceuticals, Inc., whether a technique is scientific knowledge is based on several considerations: whether the technique can be and has been tested, whether the technique has been subject to peer review, the known or potential rate of error, and whether the technique used has been generally accepted. As has been noted, the criteria constituting an airline passenger profile are not known publicly and therefore cannot be tested transparently. In fact, the government’s testing of profiling systems in collaboration with the airline industry led to litigation. It is not clear what peers the closed intelligence community has for purposes of evaluating profiling as a technique. Moreover, profiling is neither a generally accepted technique nor a process whose error rate is known or satisfactory. Therefore, even presuming that profiling is necessary to safeguard commercial aviation, no definite set of characteristics constituting an airline passenger profile exists to identify the enemy. As the Supreme Court of Canada stated in the seminal decision R. v. Mohan, personal opinion about the behavior characteristics of an individual is

recognizes the value of such sacrifice: 'Greater love hath no man than this, that a man lay down his life for his friends' (John 16:13).'); see also Ariel Merari, The Readiness To Kill and Die: Suicidal Terrorism in the Middle East, in ORIGINS OF TERRORISM 196–97 (Walter Reich ed., 1990) (discussing the influence of cultural factors on suicidal terrorism); Robert A. Pape, The Strategic Logic of Suicide Terrorism, 97 AM. POL. SCI. REV. 343, 347 (2003) (noting that suicide terrorists justify their actions on the basis of the religious and ideological beliefs of a broader community).

167. SAGEMAN, supra note 6, at 91–96. See generally TED ROBERT GURR, WHY MEN REBEL (1970) (discussing demographic and sociological factors that lead people to join dissident groups).

168. SAGEMAN, supra note 6, at 98.

169. Interview with Richard W. Bloom, Dean, College of Arts and Sciences & Director, Terrorism, Intelligence, and Security Studies, Embry-Riddle Aeronautical University (July 18, 2007) (on file with author).


171. See cases cited supra note 89.

not as valuable as a behavioral profile that is "in common use as a reliable indicator of membership in a distinctive group. Put another way: Has the scientific community developed a standard profile for the offender who commits this type of crime?" To date, neither the scientific nor the intelligence community has created such a reliable indicator of terrorists, and as detailed, it may not be possible to do so.

In all, as Bernard E. Harcourt has argued, society's reliance on predictive or actuarial methods of allocating enforcement and punishment should be abandoned in favor of a return to society's "most central intuition of just punishment: the idea that any person committing a criminal offense should have the same probability of being apprehended as similarly situated offenders." Yet, profiling remains an attractive and important security option. It offers the chance to locate clues where they exist. Of course, this begs the question whether the law permits consideration of some clues but not others, such as race, religion, and ethnicity.

B. Is Airline Passenger Profiling Rational or Racist?

Inarguably, profiling requires discrimination. Both "profiling" and "discrimination" have acquired strong negative connotations. Yet, profiling and discrimination are common, lawful features of economic life in America today because of the commoditization of personal information. Banks and supermarkets have long used profiling as marketing and strategic planning tools. Businesses today segment their

---

173. [1994] 2 S.C.R. 9 ¶ 49 (Can.) (rejecting testimony intended to show that the character traits of a physician accused of sexually assaulting female patients did not fit the psychological profile attributable to any of several groups in which most sex offenders fall).


175. See Ben Winograd, 'Profiling' Not a Dirty Word in Israel; U.S. Studies Airport Security There, RECORD (Bergen County, N.J.), May 10, 2007, at A21; 60 Minutes: That Dirty Little World "Profiling" (CBS television broadcast Aug. 11, 2002) ("[W]hen it comes to identifying criminals and terrorists in our politically correct society, profiling has become a dirty word, and there is a problem drawing the fine line between common sense and bigotry."). Another source notes: In public discourse, profiling is often viewed as constituting one of four narratives. On the one hand, it is something that works but whose work should not be allowed. On the other hand, it is something that should be allowed but may not work. There are also adherents of two other narratives: that profiling works and should be allowed to work and that it doesn't work and shouldn't be allowed even if it did. All four of these narratives may ignore important issues as to the nature, utility, and ethics of profiling.

Biometric, Psychometric, and Sociometric Profiling, supra note 5.


177. See Gram-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (permitting banks and other financial institutions to share customer data with affiliated companies); Steven A.
customers on the basis of buying habits and patterns, where repeat customers earn benefits such as gift cards or giveaways. Airlines certainly profile and categorize their customers through computer reservation and yield management systems, along with frequent flyer reward programs.\textsuperscript{178} In state and federal courts across the nation, lawyers profile potential jurors during voir dire and doing so is an important part of the judicial process. Of course, lawyers may only profile potential jurors on the condition they do not discriminate on the basis of race, color, religion, sex, national origin, or economic status.\textsuperscript{179} In the marketplace and in the courtroom, then, profiling can be rational conduct, and discrimination can entail nothing more than differentiating individuals on permissible grounds for appropriate ends.

Like profiling and discrimination, the connotation and legitimacy of surveillance is context based.\textsuperscript{180} From its founding, the U.S. government has surveilled its own citizens in response to external threats, alternatively justifying its actions as either care or control.\textsuperscript{181} In 1798, for example, Congress passed the Alien Enemies Act, which allowed President John Adams to deport noncitizens identified as threats to the coun-

\begin{flushleft}


180. See DAVID LYON, SURVEILLANCE AFTER SEPTEMBER 11, at 5 (2003) ("Surveillance . . . refers to routine ways in which focused attention is paid to personal details by organizations that want to influence, manage, or control certain persons or populations.").

181. See id. at 11 ("Surveillance is always ambiguous; care and control are always in tension.") (emphasis added); David Cole, The New McCarthyism: Repeating History in the War on Terrorism, 38 HARV. C.R.-C.L. L. REV. 1, 3 (2003); Mark G. Young, Note, What Big Eyes and Ears You Have!: A New Regime for Covert Governmental Surveillance, 70 FORDHAM L. REV. 1017, 1018 (2001).
\end{flushleft}
try without due process of the law. Later, during the Civil War, President Abraham Lincoln suspended the writ of habeas corpus on eight occasions. And in 1875, in Totten v. United States, the U.S. Supreme Court upheld President Lincoln's authority to enter into a contract with a private citizen to spy on Confederate troops. In 1917, during World War I, federal authorities prosecuted opponents to the war under the Espionage Act. Most infamously, on February 19, 1942 President Franklin D. Roosevelt authorized the interment of Japanese Americans to designated military areas, a decision upheld by Korematsu v. United States—a now disgraced decision. The legacy of "us against them" domestic and foreign policy brings into focus the broad question whether legitimate ends, such as national security, are justified by any means, including the deprivation of civil liberties and other rights for particular groups of people. The topic of airline passenger profiling encapsulates this analytic tension, touching on the narrower, disturbing question whether reason and racism are symbionts and not mutually exclusive when it comes to protecting commercial aviation from terrorism.

A federal district judge recently framed the central controversy of airline passenger profiling:

Since the terrorist attacks of September 11, 2001, this country has struggled to meet the stringent demands of national security and, simultaneously, to protect the civil rights of the American people. Some have argued that the practice of racial profiling, wherein law enforcement officials or others single out members of a particular race for heightened investigatory scrutiny, based primarily or exclusively on racial characteristics that allegedly correlate with criminality, represents a conflict between those twin goals. They argue that although members of all races are entitled to be treated equally, racial profiling is a rational and effective security measure. Others argue, much more persuasively, that racial profiling is not a legitimate


183. See Rosenzweig, supra note 22, at 668.

184. 92 U.S. 105, 106 (1875).


security measure, and that at least in the realm of discrimination, liberty and security do not conflict.\textsuperscript{188}

In its most benign form, profiling airline passengers for security purposes helps to distinguish high-risk passengers from low- or no-risk passengers. Profiling after September 11, however, has come to mean something more sinister.

Americans resisted profiling before September 11, but later welcomed it.\textsuperscript{189} Following the thwarted liquid-bomb plot of August 10, 2006 the \textit{Wall Street Journal} appealed to common sense and criticized TSA's refusal to use religious or ethnic factors as even minor factors in screening:

Nobody is suggesting using ethnicity or religion as the only—or even the primary—factors in profiling terrorists. But it also makes no sense to take zero account of the fact that every suicide attack against U.S. aviation to date has been perpetrated by men of Muslim origin. While al Qaeda is no doubt seeking recruits who don't obviously display such characteristics, that doesn't mean we should ignore the likeliest candidates.

The law on this is settled, and in the other direction. On multiple occasions the federal courts have upheld programs that treat groups differently when a "compelling" public interest can be identified: affirmative action, minority set-asides, composition of Congressional districts, and the all-male draft have all met that legal test. Yet the same people who would allocate jobs, federal contracts and college admissions by race or ethnicity object to using them merely as one factor in deciding whom to inconvenience for a few minutes at an airline checkpoint. Surely aviation security is a far more compelling


\textsuperscript{189} See Albert W. Alschuler, \textit{Racial Profiling and the Constitution}, 2002 U. CHI. LEGAL F. 163, 163 (2002) (stating that after September 11, 58\% of Gallup poll respondents favored the screening of Arabs more intensely than other passengers by airlines); David A. Harris, \textit{New Approaches to Ensuring the Legitimacy of Police Conduct: Racial Profiling Redux}, 22 ST. LOUIS U. PUB. L. REV. 73, 74 (2003) ("[A]fter the attacks on the World Trade Center and the Pentagon over fifty percent of Americans . . . said they supported the use of profiling, as long as it was targeted at Middle Easterners and Muslims in airports."); Leti Volpp, \textit{Blaming Culture for Bad Behavior}, 12 YALE J.L. & HUMAN. 89, 95–96 (2000) (noting misdeeds of whites often are perceived as the acts of individuals and not norms associated with race, while the converse perception exists as to other races); Leti Volpp, \textit{The Citizen and the Terrorist}, 49 UCLA L. REV. 1575, 1576–77 (2002) [hereinafter \textit{The Citizen and the Terrorist}] (noting that there is a "public consensus that racial profiling is a good thing, and in fact necessary for survival"); Vikram David Amar, \textit{Opinion, When Racial Profiling Is Appropriate}, L.A. TIMES, Sept. 30, 2001, at M2 ("Fifty-eight percent of Americans favored 'more intensive security checks' for persons (including American citizens) of Arab descent; 49\% favored 'special ID' cards for such people; and 33\% backed special surveillance.").
IS AIRLINE PASSENGER PROFILING NECESSARY?

Stated another way:

[T]he mathematical probability that a randomly chosen Arab passenger might attempt a mass-murder-suicide hijacking—while tiny—is considerably higher than the probability that a randomly chosen white, black, Hispanic, or Asian passenger might do the same. In constitutional-law parlance, while racial profiling may be presumptively unconstitutional, that presumption is overcome in the case of airline passengers, because the government has a compelling interest in preventing mass-murder-suicide hijackings, and because close scrutiny of Arablooking [sic] people is narrowly tailored to protect that interest.

This outlook was formalized when the nation’s sixteen intelligence agencies released the National Intelligence Estimate in July 2007. That document, expressing the intelligence community’s most unified and authoritative written judgments on national security issues, singled out occupants of certain parts of the world—Islamic fundamentalists, particularly the al Qaeda terror network, Lebanese and Iranian-backed Hizballah, Salafi, and smaller non-Muslim ("single issue") groups—as posing a "persistent and evolving terrorist threat" to the United States. Accordingly, profiling may be supportable on grounds more substantial than common sense.

The gut appeal of profiling does not make it any easier to formulate a commercial aviation security policy that profiles lawfully.

190. Editorial, The ‘Profiling’ Debate, WALL ST. J., Aug. 19, 2006, at A10 (arguing that avoiding screening on the basis of ethnic and religious background has resulted in "a policy of random searches that focuses scarce screening resources as much on eight-year-old girls as on 22-year-old men with Pakistani passports."); see also Lowry, supra note 48, at 32 ("Arab-American groups still scream at any suggestion of commonsense security at airports, while the Bush administration still cowers at any association with ‘racial profiling.’ It has become clear in recent weeks that the pieties of American racial politics will remain unchanged—even after contributing to a mass murder."). But see Debra J. Saunders, Editorial, Go Ahead, Search Granny, S.F. CHRON., Aug. 17, 2006, at B7 ("Why . . . search little old white ladies when young Arab and Muslim men were behind the Sept. 11, 2001, attacks and other terrorist plots? The answer is: The feds should avoid racial profiling because it breeds discontent without enhancing security.").


193. See, e.g., Stuart Taylor Jr., The Skies Won’t Be Safe Until We Use Commonsense Profiling, in CIVIL LIBERTIES VS. NATIONAL SECURITY IN A POST-9/11 WORLD 157 (M. Katherine
Constitution is the measure of the reasonableness of any federal aviation policy that interferes with personal rights. The Fourth Amendment of the U.S. Constitution is where the competing ideals of national security, on one hand, and civil liberties and personal privacy, on the other hand, interface. 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.

Some of the earliest cases relating the Fourth Amendment to commercial aviation security arose in the context of boarding gate searches via metal detectors and magnetometers. Both metal detectors and magnetometers are court-sanctioned procedures on the basis that there is little practicality in obtaining a search warrant for every airline passenger who passes through an airport terminal. Ample decisional law upholds the type of airport searches conducted by metal detectors and magnetometers as routine and regular aspects of airline travel that proportionally and defensibly intrude on personal liberty interests in favor of public safety and welfare. As the U.S. Court of Appeals for the Fourth Circuit reasoned,

the search for the sole purpose of discovering weapons and prevent-


195. U.S. CONST. amend. IV.

196. See, e.g., United States v. Fern, 484 F.2d 666, 666–69 (7th Cir. 1973); United States v. Cyzewski, 484 F.2d 509, 511 (5th Cir. 1973); United States v. Miner, 484 F.2d 1075, 1077 (9th Cir. 1973); United States v. Doran, 482 F.2d 929, 932 (9th Cir. 1973); United States v. Kroll, 481 F.2d 884, 886 (8th Cir. 1973); United States v. Miller, 480 F.2d 1008, 1010 (5th Cir. 1973); United States v. Legato, 480 F.2d 408, 410–11 (5th Cir. 1973); United States v. Skipwith, 482 F.2d 1272, 1275 (5th Cir. 1973); United States v. Echols, 477 F.2d 37, 39–40 (8th Cir. 1973); United States v. Burton, 475 F.2d 469, 471 (8th Cir. 1973); United States v. Moreno, 475 F.2d 44, 48 (5th Cir. 1973); United States v. Clark, 475 F.2d 240, 242–43 (2d Cir. 1973); United States v. Bell, 464 F.2d 667, 673 (2d Cir. 1972); United States v. Lindsey, 451 F.2d 701, 703 (3d Cir. 1971).
ing 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."\footnote{197}

Profiling proponents discount neither the Constitution generally nor the Fourth Amendment specifically. Rather, they argue that common sense is not inconsistent with the Constitution. Yet, equating Arabs, Middle Easterners, Muslims, or any other group with terrorism is inequitable and contrary to law. Sociologically, too, marginalizing passengers along demographic lines ignores the fact that passengers selected for heightened screening are probably law-abiding citizens posing no threat to any facet of society.\footnote{198} In this respect, some critics of aviation security policy perceive airline passenger profiling to be overtly racist, where "flying while brown" and "flying while Arab\footnote{199} is akin to "driving while black."\footnote{200}

Inflammatory remarks by politicians do not help: a

\footnote{197. United States v. Epperson, 454 F.2d 769, 771 (4th Cir. 1972) ("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 requirement is excused by the exigent national circumstances."); see also United States v. Davis, 482 F.2d 893, 908 (9th Cir. 1973) ("The essential purpose of the scheme is not to detect weapons or explosives or to apprehend those who carry them, but to deter persons carrying such material from seeking to board at all.").}


Louisiana Congressman who favors airline passenger profiling, for example, spat, "a person who has 'a diaper on his head and a fan belt wrapper around the diaper' needs to be singled out for questioning."201 Obviously, there is a better way to make the point that racial profiling may be reasonable, and many proponents of airline passenger profiling have appealed to the logic of profiling on the basis of ethnicity, political agenda, race, or religious affiliation, given the historical demographics of terrorists.202

Aviation security policy makers must identify dangerous people as a practical matter, whatever the legal, psycho-physiological, or scientific validity of profiling systems. Security officials must imagine preceded and unprecedented threats from all passengers, not least of whom are passengers whose background fits with those who have terrorized commercial airline travel historically. The federal government’s systematic targeting of a substantial subset of its population (i.e., airline passengers) no doubt challenges ideals expressed in the Constitution, and particularly in the Bill of Rights. Therefore, the paramount questions for aviation security policy makers are whether and how it is possible to balance—not exchange—airline safety with civil liberties.203 These questions are likely to endure as long as any terrorist threat to commercial aviation persists.

---


C. Security or Privacy: A False Choice?

In a national "Civil Liberties Survey" conducted during the four months following September 11, a sample of American citizens expressed their relative willingness to trade civil liberties for greater personal safety and security.204 A decision to tolerate this exchange is complex, a product of a person's own social and psychological profile, including dogmatism (closed-mindedness), capability for interpersonal trust (faith in people), feelings of national pride and patriotism, along with a person's race and ethnicity, education, age, and community.205 After September 11, Americans appeared to favor civil liberties over security in the abstract, rather than in actual situations.206

Like the concepts of liberty, privacy, and security themselves, society and its citizens are defined and moved by circumstance.207 The national impulse to promote security over privacy and over personal rights has dissipated since September 11.208 Citizens have returned to their September 11 routines as they were before. Today, increasingly, Americans greet successively intrusive national security measures by the federal government with an "anti-anti-terrorism" sentiment that is based on concerns about an ever-expanding executive and a "fear of technology."209 Some citizens "equate the potential for abuse of Executive Branch authority with the existence of actual abuse" and protest "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."210 In this context, TSA's promise to remedy mistakes by profiling systems like CAPPS, CAPPS II, and Secure Flight after the fact is no assurance for many Americans. Similarly, for privacy advocates and civil libertarians, the idea that the federal government or private vendors or both will have access to an airline passenger's personal and biometric data through systems like Registered Traveler is intolerable. Some government officials

204. Davis & Silver, supra note 12, at 28.
205. Id. at 31–32.
206. Id. at 32.
207. Id. at 28 ("Context-specific events provide critical insight into the level of commitment to democratic principles. ... For ordinary citizens during ordinary times, civil liberties issues are likely to be remote from everyday experience; but in certain contexts civil liberties issues have immediate implications for people's sense of freedom and well-being.") (citations omitted).
208. See, e.g., Cerabino, supra note 11, at 1A ("'I knew a lot of people in the World Trade Center, and the next day when I came to work, I couldn't even stand to hear the word 'privacy,'" said ... a senior analyst with Competitive Enterprise Institute, a group that advocates limiting government controls. 'But the cost of being wrong about some of these issues seems appallingly high.").
209. See Rosenzweig, supra note 22, at 663–64.
210. Id. at 664.
even acknowledge the perception that the government cannot monitor its own activities.\textsuperscript{211} Indeed, a willingness to exchange civil liberties for security turns on trust and confidence in government.\textsuperscript{212}

The cynic’s view—that trust is irrelevant, that privacy is impossible in today’s Electronic Information Age, and that there is no meaningful exchange of privacy for security to make—bears at least one mention.\textsuperscript{213} Before September 11, an FAA Director of the Office of Civil Aviation Security wondered whether “virtually all of the data that the U.S. government seeks to collect in CAPPS II is probably already available on each of us through the Internet.\textsuperscript{214}” Such statements serve the misperception that it is hopeless to preserve privacy interests today. As one commentator states:

The availability of information privacy horror stories (in particular, the prevalence of identity theft, spam and hacker stories in the media), and the general mistrust in government agencies to handle personal information appropriately, combined with a general apprehension about technology and how it works, and the natural anxiety relating to disclosure of personal, particularly intimate, information—all spurred on by the privacy lobby—has created a public anxiety about electronic privacy out of proportion to the actual privacy risks and has obscured discussion of the very real threats posed by either failing to provide security or by misallocating security resources.\textsuperscript{215}

The events of September 11 mandate better security related intelligence. Intelligence services should gather and share more information. Airline passenger profiling systems are consistent with this objective. Information networking vis-à-vis profiling is a limited and context-specific societal objective that, in a post-September 11 environment, legitimately challenges without eviscerating privacy interests. Arguably, to best protect privacy rights “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 con-

\begin{itemize}
  \item \textsuperscript{211} Samuel Podberesky, Assistant Gen. Counsel for Aviation Enforcement, Dep’t of Transp., Address at the ABA-TIPS Aviation and Space Law Committee Annual Conference: Practical Views from the Cockpit to the Courtroom (Oct. 22, 2004).
  \item \textsuperscript{212} Davis & Silver, \textit{supra} note 12, at 30.
  \item \textsuperscript{214} Vincent, \textit{supra} note 43, at 8.
  \item \textsuperscript{215} Taipale, \textit{supra} note 12, at 137–38 (footnotes omitted).
\end{itemize}
cerns, with less emphasis on individual self-policing and market-based mechanisms." This perspective is unlikely to take hold in the United States today. While over half of a sample of American citizens supported a trade-off involving the right of privacy by requiring a national identity card after September 11, 82% of those surveyed preferred civil liberties over security when the surveyors framed the right to privacy issue in terms of racial profiling.

Ultimately, the Fourth Amendment, not a sample survey, must balance national security interests and privacy concerns. The Fourth Amendment is designed to protect citizens against unreasonable searches and seizures of their personal belongings. The requirement that the federal government secure a warrant supported by a showing of probable cause, in turn, is predicated on whether a citizen has a "reasonable expectation of privacy." Whether data mining and airline passenger profiling constitutes a search under the Fourth Amendment remains an open question. For now, controversial legislation like the PATRIOT Act and abated or developing profiling systems like

217. Davis & Silver, supra note 12, at 32–33.
218. Ramasastry, supra note 56, at 763.
CAPPS II and Secure Flight are enacted or developed at a distance from citizens through technical legal papers, closed communication channels, and uninviting bureaucracy. The federal government, and TSA specifically, can and should do more to publicize the merits of airline passenger screening systems and to reassure citizens about the status of their traveling rights in the current, insecure environment of commercial aviation.

D. An International Perspective: E.U.–U.S.

Terrorists target international air travel because of aviation’s global reach.\textsuperscript{221} “[A]viation allows the US and its allies to be accessible globally for attack without the need to infiltrate through the home territory of a target—be it government, business, or their representatives.”\textsuperscript{222} The destruction of Pan Am Flight 103 illustrates this principle in action. Pan Am Flight 103 was traveling from London to New York when it was blown up by plastic explosives while flying over Lockerbie, Scotland in December 1988.\textsuperscript{223} While Pan Am was not a state-owned “flag carrier” of the United States, it was iconic of America. By destroying such symbols without also incurring their own casualties, terrorists create “psychopolitical impact—e.g., influence on worldviews, ideologies, policy preferences, preferred lifestyles, and related behaviors of physical and psychological survivors and of other direct and indirect observers of terrorist operations—through their operations so as to ultimately induce

\textsuperscript{221} See supra Part II. See generally S.K. Ghosh, \textit{Aircraft Hijacking and the Developing Law} 13 (1985) (stating that aircraft hijacking is often intended to gain “world-wide publicity”); Nancy Douglas Joyner, \textit{Aerial Hijacking as an International Crime} (1974) (noting that the international community recognizes the existence of threats to global air safety); Edward McWhinney, \textit{Aerial Piracy and International Terrorism} (2d ed. 1987) (discussing the potential for worldwide publicity regarding the disruption and dislocation of international air transportation and the resulting attention for the political cause responsible for such problems).

\textsuperscript{222} Motivation and Aviation as a Terrorism Target, supra note 139.

behavioral change in the world that corresponds to desired political goals.\textsuperscript{224}

The psychopolitical impact of September 11, too, was profound as it involved terrorist activities not overseas, but on domestic airplanes inside the United States. American leaders nevertheless emphasized that the World Trade Center was destroyed on September 11 to make clear that aviation terrorism is a worldwide peril that requires international vigilance. Yet, global solutions to airline safety concerns have been difficult to achieve. Although the United States and the European Union share a common interest in maximizing aviation security, each balances security against civil liberties in culturally discrete and sometimes opposed ways.\textsuperscript{225} These differences are not quaint cultural variations, but significant impediments to securing the airways between sovereign nations in a uniform way.\textsuperscript{226}

Whereas Americans approach privacy as a safeguard of their liberty interests, Europeans conceptualize privacy as a basic human right ensuring personal dignity.\textsuperscript{227} That is,

[w]hen Europeans think about privacy, they are most concerned about personal dignity and the right to control one’s public image, a right threatened primarily by the mass media, the Internet, and commercial data warehouses. By contrast, American conceptions of pri-


privacy are focused on personal liberty and the right to be free from state surveillance, a right threatened primarily by government intrusions into the home.

"Europeans are also far more trusting of government, and willing to allow it to regulate personal choices in ways that Americans would find intolerable . . . ." In this context, airline passenger profiling systems in Europe have evaluated data that not even the CAPPS II and Secure Flight systems proposed to consider. Before September 11, airline passenger profiling systems in Europe used the input of law enforcement agencies such as the international policy agency INTERPOL. Additionally, overseas profiling systems detailed information such as whether a "traveler contribut[ed] to certain suspect charitable organizations." Meanwhile, since 2001 Schiphol Airport in Amsterdam has operated a system called "Privium." Like the Registered Traveler program just being deployed in the United States in 2007, Privium fast-tracks passengers through security checkpoints in exchange for a fee and certain personal and biometric information (e.g., fingerprint or iris scan).

Ironically, what often is

[lost in the partisan uproar in America over the USA Patriot Act is the surprising fact that the expansion of state surveillance authority in Europe after September 11 is arguably more draconian than in the United States . . . .

. . . Europe's greater deference to government authority led countries like Germany and France to adopt surveillance measures after September 11 that in some ways make the Patriot Act seem meek. . . . For example, in 2002 Germany adopted a sweeping law that increased the power of its security agencies. The government was authorized to create a central database with personal information

228. Rosen, supra note 227, at 49.
229. Id. For example, the Belgium, French, and German governments reserve the right to refuse to register objectionable names chosen by parents for their infants. Id.
231. Armstrong & Pereira, supra note 144, at Al.
233. Id. Meanwhile, on June 18, 2007 Canada implemented "Passenger Protect," an online system though which passengers older than twelve must supply a government-issued photo identification before boarding commercial airplanes, and airlines themselves must screen passengers traveling into, out of, or across Canada against a government-issued "No Fly" list of known terrorists or people convicted of crimes against aviation security. Call the Mounties, AVIATION WK. & SPACE TECH., May 21, 2007, at 36, 36; see also Roger Belgrave, Does No-Fly List Violate Privacy?, BRAMPTON GUARDIAN (Canada), July 1, 2007, at 21 (quoting Canadian Member of Parliament as stating, "I think we're asking for a lot of trouble for a lot of innocent people"). See generally Jennifer McClennen & Vadim Schick, "O, Privacy" Canada's Importance in the Development of the International Data Privacy Regime, 38 GEO. J. INT'L L. 669 (2007).
about foreigners, including fingerprints and religious background. The law also authorized the German national identification cards to include biometric data, such as fingerprints. And it explicitly endorsed data mining ... requiring government agencies to turn personal information over to the federal police.234

Existing anti-aviation terrorism security devices employed by the European Union, juxtaposed with developing profiling systems in the United States, suggest that airline passenger screening should be the subject of ready international cooperation. Indeed, "[i]t is now generally accepted that increased information sharing is the best way of preventing terrorism, but information sharing between the public and private sector may be difficult if Americans are focused on the dangers of state surveillance and Europeans are concerned about protecting the dignity of the consumer."235 In fact, U.S. and E.U. aviation security policies today are fractured around the issues of privacy and security.

Congress enacted the Aviation and Transportation Security Act ("ATSA") in reaction to September 11, requiring airlines flying to and from the United States to provide federal authorities with electronic access to PNR information. Through ATSA, the United States has pressed European security officials specifically for pre-flight information contained in an Advance Passenger Information System.236 However, of the approximately thirty-nine pieces of information that comprise airline passenger profiles in the United States, twenty cannot be disclosed under E.U. privacy laws.237 Consequently, the United States' mandate for PNRs for international flights directly contradicts the E.U. data protection law prohibiting the transfer of personal data to a recipient who would not guarantee its protection. Moreover, airlines with flights to the United States were put into an impossible situation: They could either disclose protected passenger information in violation

234. Rosen, supra note 227, at 52.
235. Id.
of E.U. law or withhold protected passenger information and be denied landing rights in the United States. Not surprisingly, the American position engendered resentment, as when a French citizen opined: "[W]hat right do [American authorities] have to turn the world's airlines into their unpaid informers? Out here, in the real world, that is called blackmail." More officially, Frits Bolkestein, European Commissioner responsible for Internal Market, Taxation and Customs Union issues, noted that "[a]t the heart of this debate lies a fundamental question: To what extent are we prepared to see our civil liberties eroded in the search for greater security? The question becomes even more difficult when different nations come to different answers." To resolve the conflict, the United States agreed to keep passenger data for no more than three-and-a-half years (a concession from an initial request to maintain data for seven years) solely for purposes relating to anti-terrorism.

This agreement has been invalidated, however. On May 30, 2006 the European Court of Justice—the highest court in the European Union, located in Luxembourg—invalidated the agreement to transfer airline passenger records from the European Union to DHS. The Court of Justice acknowledged that the E.U.–U.S. agreement was to promote security and deter terrorism. Nevertheless, it determined that the agreement went outside Article 3(2) of the E.U. Data Protection Directive 95/...
IS AIRLINE PASSENGER PROFILING NECESSARY?

46, which governs processing operations concerning public security, defense, and State security.\textsuperscript{243} In the wake of this decision—and until July 31, 2007—the European Union and the United States operated under an interim accord allowing for the screening of passengers on arrival with information routinely given to airlines, including passengers’ addresses and credit card, passport, and phone numbers.\textsuperscript{244} Had that agreement expired, the European Union and the United States would have been back to a starting point where fundamental political, social, and economic differences exist.\textsuperscript{245}

IV. CONCLUSION

The “freedom to travel throughout the United States has long been recognized as a basic right under the Constitution.”\textsuperscript{246} Airline travel in particular has become such a usual part of life that many Americans simply presume their freedom to it.\textsuperscript{247} In fact, airline service, not airline security was the topic that had the attention of transportation lawmakers throughout the 1990s. Airline passengers—including members of Congress—fumed at airline overbooking practices, delays, and congestion at airports.\textsuperscript{248} September 11 jolted the nation’s focus from service to


\textsuperscript{247} See, e.g., United States v. $124,570 U.S. Currency, 873 F.2d 1240, 1242 (9th Cir. 1989) (“Commercial air travel, once a luxury, has become a staple of modern existence. For many Americans, boarding an airplane to travel across the state or across the country is as ordinary and commonplace an event as boarding a bus or train fifty years ago, or mounting a horse-drawn carriage around the turn of the century.”).

security.  

In the aftermath of September 11, aviation security officials relentlessly hunt for bad things. They continually develop, contract for, and deploy various high- and low-tech anti-terrorism measures, i.e., thermal-neutron analysis to analyze luggage for chemicals used in plastic explosives, computerized tomography to evaluate the quality of a substance, X-ray devices and electromagnetic radiation to search for typical explosives ingredients, trace detectors or "sniffers" to detect for vapor residue of explosives, bomb-sniffing dogs, airline personnel screening, and automated passenger profiling. These layers of security are important, as evidenced in July 2007 when the public learned from an unclassified security bulletin that TSA had been investigating possible "dry-runs" by aviation terrorists to smuggle weapons on airplanes. The argument to

A14. A week later, Denver-bound passengers aboard United Express airplanes were diverted overnight to Cheyenne, Wyoming; passengers were shocked the next day to see the flight crew leaving without them. See Gary Stoller, United Vows Reimbursement: Airline Says It’s Taking Care of Abandoned Fliers, USA TODAY, Apr. 4, 2007, at 5B. Earlier, on December 29, 2006 American Airlines passengers sat on airplanes for hours in Austin, Texas. See Margaret Carlson, Editorial, Bush Wants Airlines To Run on Time, SEATTLE POST-INTELLIGENCER, Oct. 7, 2007, at C4. Not surprisingly, the push for enforceable airline passengers' rights has been renewed. See Airline Passenger Bill of Rights Act of 2007, H.R. 1303, 110th Cong.; Airline Passenger Bill of Rights Act of 2007, S. 678, 110th Cong.

249. Rosenzweig, supra note 22, at 671 ("[A] better view of this history shows that the balance between liberty and security is more like a pendulum that gets pushed off-center by significant events (such as those of September 11th) than a spiral. Over time, after Americans have recovered from the understandable human reaction to catastrophe and after the threat recedes, the pendulum returns to center.").


251. According to a July 20, 2007 report, it appears that federal air marshals and other law enforcement agencies were warned of possible rehearsals of an actual terrorist event over the period of September 2006 through July 2007. TRANSP. SEC. ADMIN., INCIDENTS AT U.S. AIRPORTS MAY SUGGEST POSSIBLE PRE-ATTACK PROBING, TRANSP. INTELLIGENCE GAZETTE (2007), available at http://msnbcmedia.msn.com/i/msnbc/sections/NEWS/pdfs/airport%20warning.pdf (reporting suspicious seizures: (a) in San Diego, California, checked baggage containing two icepacks (filled with clay rather than normal blue gel) covered in duct tape; (b) in Milwaukee, Wisconsin, carry-on baggage containing several items resembling an improvised explosive device ("IED"), such as wire coil, an electrical switch, batteries, three tubes, and two blocks of cheese; (c) checked baggage in Houston, Texas, containing a plastic bag with a 9-volt battery, wires, a block of brown clay-like minerals, and pipes; and (d) in Baltimore, Maryland, checked baggage containing a plastic bag with a block of processed cheese taped to another plastic bag holding a cellular-phone charger); see also Siobhan Gorman, BWI Security the Focus; Officials Play Down Report of Terror 'Dry Run,' BALTIMORE SUN, July 26, 2007, at 1B; Michael
scrutinize airline passenger behavior through profiling or otherwise is not an argument for diminished screening of dangerous objects. However, "the 'magic' attributed to isolated technological fixes must be jettisoned in favor of systems perspectives including the human element." People warrant at least as much attention as putatively dangerous objects. Biometric, psychometric, and sociometric profiling facilitates this objective by focusing on people and their ideas and behaviors, not just their weapons.

This is not to say that airline passengers should exchange their civil liberties for security thoughtlessly or eagerly. Yet, that is what seems to happen. On February 23, 2007 federal aviation security officials tested "SmartCheck" at Sky Harbor International Airport in Phoenix, Arizona. SmartCheck is a $110,000 radiation-emitting, "backscatter" machine that "peeks underneath [airline] passengers' clothing to search for guns, bombs or liquid explosives." While SmartCheck will screen only volunteers initially, the ACLU has objected that it effects a "virtual strip-search." Nevertheless, as one reporter noted, "[i]f passengers . . . who were asked to undergo body scans are an indication, security

---


252. In April 2005, in reaction to Richard Reid's 2001 attempt to detonate explosives hidden in his shoes on a Paris–Miami flight, TSA prohibited passengers from carrying lighters on airplanes. See Joe Sharkey, Lighters Banned on Flights, MIAMI HERALD, Mar. 7, 2005, at 1 ("Each passenger can still carry on up to four books of safety matches. The reasoning there is that lighters can be used like little blowtorches, while matches cannot. Matches and lighters of all kinds remain prohibited from checked bags."). Just over two years later, effective August 4, 2007, the ban on lighters was lifted. See, e.g., Press Release, Transp. Sec. Admin., TSA Announces Procedural Changes at the Checkpoint: Common Lighters No Longer Banned from Carry-ons, Breast Milk Exemption Modified (July 20, 2007), available at http://www.tsa.gov/press/releases/2007/press_release_07202007.shtml. The TSA's relaxation of the prohibition of lighters in the name of efficiency is puzzling. See, e.g., Michael J. Sniffen, TSA Eases Carry-on Rules for Lighters, Breast Milk, ORLANDO SENTINEL, July 21, 2007, at A7 ("Explosives remain the most significant threat to aviation,' TSA administrator Kip Hawley said. 'By enabling our [airport-screening] officers to focus on the greatest threats, we are using our officers' time and energy more effectively and increasing security for passengers.' ") (alteration in original).


254. Paul Giblin & Eric Lipton, New Airport X-rays Scan Bodies, Not Just Bags, N.Y. TIMES, Feb. 24, 2007, at A1 ("Special 'privacy' software intentionally blurs the image, creating an outline of a body that is clear enough to see a collarbone, bellybutton or weapon, but flattens details of revealing contours.").

255. Id.

256. Thomas Frank, Phoenix Test Site for TSA X-ray; ACLU Objects to 'Virtual Strip Search,' USA TODAY, Dec. 1, 2006, at 1A.
trumps privacy." 257 On the first day SmartCheck was deployed, "[m]ost passengers asked to submit to a full-body X-ray at Security Checkpoint B didn’t bat an eyelash. Nine in 10 gamely stepped up to a scanner. . . . ‘Sure, I’d be happy to do it,’ said [a passenger]. . . . ‘Privacy to me isn’t nearly as important as our security, especially if they assure me the X-rays aren’t harmful.’" 258 SmartCheck may well be an important layer of aviation security today or in the near future, but it amplifies a core problem with current aviation security policy and how citizens are informed about it, if at all.

It should not be underestimated that bad people are more dangerous than bad things in the current global aviation marketplace. 259 Correlatively, the search for bad objects should not be over-estimated at the expense of inspecting airline passengers who may pose a threat to civil aviation. 260 Americans wary of an erosion of their privacy rights contend "protections" like CAPPS, CAPPS II, Secure Flight, and the Registered Traveler program represent an Orwellian society realized, the equivalent of "calling on ‘Big Brother’ to protect citizens from ‘Big Brother.’" 261 It is true that such security devices may challenge existing civil liberties. But it is also true that lawful, constitutionally sanctioned surveillance is nothing new in American society. 262 Airline

258. Id.; Crandall, supra note 14, at 19 ("You want to travel on the airline system? You give up your privacy. You don’t want to give it up? Don’t fly. Your privacy isn’t equal to the safety of the rest of us.").
259. Not only are security officials suspicious of passengers, but passengers are wary of security officials and processes. "[M]ore travelers see US government officials as a reason not to visit (70%) compared to the threat of terrorism or crime (54%). Furthermore, two thirds of travelers fear that they will be detained for a simple misstatement and more than half believe that US entry officials are rude." Officials a Bigger Threat Than Terrorists to US Tourism, News@PATA, May 2, 2007, http://www.pata.org/patasite/index.php?id=1684#. 260. See, e.g., Airport Screeners Missed Explosives, Report Says, N.Y. TIMES, Nov. 15, 2007, at A24 (discussing the success of government investigators in learning on the internet how to make an improvised incendiary device with $150 in street-purchased parts, and smuggling liquid, explosives and detonators through airport checkpoints); Nicole Gaouette, Airport Security Fixes Debated, L.A. TIMES, Nov. 16, 2007, at 20 (reporting the call by federal investigators for more physical searches of passengers to reduce the chances that a terrorist can sneak a bomb onto a commercial airplane).
262. See LYON, supra note 180, at 4 ("It must be emphasized that while the events of 9/11 and their aftermath were unprecedented, the idea of ‘everything changed’ on that day is highly misleading. . . . In other words, the establishment of ‘surveillance societies’ that affect the lives of all ordinary people was already well under way long before 9/11.”); see also CHRISTIAN PARENTI, THE SOFT CAGE: SURVEILLANCE IN AMERICA 199–200 (2003) ("Ultimately, 9/11 did not create a technical or legal rupture in the development of everyday superintendence. It did, however, radically accelerate momentum towards the soft cage of a surveillance society, just as it gave the culture of fear a rejuvenating jolt."). See generally SURVEILLANCE AS SOCIAL SORTING (David
passenger profiling represents a necessary policy decision to ensure liberty through security. The central theory underlying modern profiling systems is that September 11 could have been prevented or at least contested. This article accepts that theory as fact and views as necessary efforts to lawfully screen airline passengers more thoroughly than had been done until September 11.