

# University of Miami Law Review

---

Volume 62  
Number 1 *Volume 62 Number 1 (October 2007)*

Article 2

---

10-1-2007

## Is Airline Passenger Profiling Necessary?

Timothy M. Ravich

Follow this and additional works at: <https://repository.law.miami.edu/umlr>



Part of the [Law Commons](#)

---

### Recommended Citation

Timothy M. Ravich, *Is Airline Passenger Profiling Necessary?*, 62 U. Miami L. Rev. 1 (2007)  
Available at: <https://repository.law.miami.edu/umlr/vol62/iss1/2>

This Article is brought to you for free and open access by the Journals at University of Miami School of Law Institutional Repository. It has been accepted for inclusion in University of Miami Law Review by an authorized editor of University of Miami School of Law Institutional Repository. For more information, please contact [library@law.miami.edu](mailto:library@law.miami.edu).

## ARTICLES

### Is Airline Passenger Profiling Necessary?

TIMOTHY M. RAVICH\*

|   |    |
|---|----|
| I. INTRODUCTION .....   | 1  |
| II. PROFILING INITIATIVES .....   | 5  |
| A. <i>Computer Assisted Passenger Prescreening System (CAPPS)</i> ..... | 9  |
| B. <i>CAPPS II</i> .....  | 16 |
| C. <i>Secure Flight</i> .....   | 19 |
| D. <i>Biometrics and the Registered Traveler Program</i> .....          | 25 |
| III. DISCUSSION .....   | 29 |
| A. <i>Identifying the Enemy</i> .....                                   | 31 |
| B. <i>Is Airline Passenger Profiling Rational or Racist?</i> .....      | 37 |
| C. <i>Security or Privacy: A False Choice?</i> .....                    | 45 |
| D. <i>An International Perspective: E.U.-U.S.</i> .....                 | 48 |
| IV. CONCLUSION .....  | 53 |

#### I. INTRODUCTION

On August 10, 2006 British intelligence prevented a terrorist plot to blow up ten airplanes by detonating common liquids.<sup>1</sup> In response, the Transportation Security Administration (“TSA”) banned certain carry-on items.<sup>2</sup> In May 2007 TSA unveiled “FIDO,” a hand-held scanner capa-

---

\* Adjunct Professor of Law, University of Miami School of Law. The author presented aspects of this article at the 46th Annual Transportation Research Forum at George Washington University as chair of a panel featuring representatives of the Transportation Security Administration, Heritage Foundation, Electronic Privacy Information Center, and American Civil Liberties Union. Thanks to Dr. Richard W. Bloom, Dean, College of Arts and Sciences and Director, Terrorism, Intelligence, and Security Studies, and Gregory A. Popp, Director, Center for Professional Education & Legal Affairs, both of Embry-Riddle Aeronautical University, for their invaluable comments on earlier versions of this article. The views expressed herein are solely those of the author, who welcomes comments at [ravicht@bellsouth.net](mailto:ravicht@bellsouth.net).

1. *Agent Infiltrated Terror Cell, U.S. Says*, CNN.COM, Aug. 11, 2006, <http://www.cnn.com/2006/US/08/10/US.security/index.html>.

2. See John M. Doyle, *Bomb Plot Fallout*, AVIATION WK. & SPACE TECH., Oct. 2, 2006, at

ble of detecting liquid explosives inside sealed bottles.<sup>3</sup> 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.”<sup>4</sup>

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.<sup>5</sup> In doing so, this article does not accept the ongoing development of profiling systems uncritically.

---

98 (“[As of August 10, 2006] passengers can now carry on small containers—3-oz. or less—of shampoo, toothpaste, skin creams, and similar items—if they all fit into a zippered, one-quart, clear plastic bag . . .”). For a detailed list of permitted and prohibited carry-on items, see TRANSP. SEC. ADMIN., PREPARE FOR TAKEOFF: PERMITTED AND PROHIBITED ITEMS, available at [http://www.tsa.gov/assets/pdf/Prohibited%20and%20Permitted%20Items\\_printerfriendly\\_3-16-07.pdf](http://www.tsa.gov/assets/pdf/Prohibited%20and%20Permitted%20Items_printerfriendly_3-16-07.pdf).

3. See Peter J. Howe, *Logan Tests Device That Sniffs Out Explosive Liquids: Scanners Won't End Need for Carry-on Rules but Will Make Skies Safer*, TSA SAYS, BOSTON GLOBE, May 25, 2007, at 1C. In 1987 and 1994, terrorists detonated liquids, including nitroglycerin in contact lens solution bottles, on international airplanes. See Jessica Ruvinsky & Kyla Dunn, *The Truth About Liquid Bombs: Promising New Technologies Could Sniff Out Liquid Bombs. But Can Their Limitations Be Overcome?*, DISCOVER, Nov. 1, 2006, at 50.

4. Shaun Waterman & Jessica Taylor, *Analysis: TSA Liquid Ban To Continue*, UNITED PRESS INT'L., Aug. 14, 2006, [http://www.upi.com/Security\\_Terrorism/Analysis/2006/08/14/analysis\\_tsa\\_liquid\\_ban\\_to\\_continue/5694](http://www.upi.com/Security_Terrorism/Analysis/2006/08/14/analysis_tsa_liquid_ban_to_continue/5694) (discussing the need for developments in screening technology that go beyond merely scanning for metal objects); see also *How Did Hijackers Get Past Airport Security?*, L.A. TIMES, Sept. 23, 2001, at A1 (“For three decades, [aviation security] has been preoccupied with looking for guns and explosives rather than for dangerous people. . . . U.S. Security efforts aim to catch the bomb; El Al’s is to catch the bomber.”) (internal quotation marks omitted).

5. One source identifies three classes of profiling: biometric, psychometric, and sociometric. *Biometric, Psychometric, and Sociometric Profiling*, IBPPONLINE, Oct. 24, 2003, [http://security.pr.erau.edu/read.php?kind=html&article\\_volume=15&article\\_issue=8&article\\_title=Biometric%2C%20Psychometric%2C%20and%20Sociometric%20Profiling](http://security.pr.erau.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.<sup>6</sup> 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*.<sup>7</sup> 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.<sup>8</sup> Liberty, in turn, involves privacy or the "right 'to be let alone.'"<sup>9</sup> Liberty and privacy are abstractions, encompassing many definitions and evading certain meaning simultaneously.<sup>10</sup> None-

---

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).

9. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 *HARV. L. REV.* 193, 195 (1890) (quoting THOMAS M. COOLEY, *A TREATISE ON THE LAW OF TORTS* 29 (2d ed. 1888)); see also *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (referring to privacy as "the most comprehensive of rights and the right most valued by civilized men"), *overruled by Berger v. New York*, 388 U.S. 41 (1967), and *Katz v. United States*, 389 U.S. 347 (1967); Ayn Rand, *The Soul of an Individualist*, in *THE FOUNTAINHEAD* (1943), reprinted in *FOR THE NEW INTELLECTUAL: THE PHILOSOPHY OF AYN RAND*, at 98 (Random House 1961) ("Civilization is the progress toward a society of privacy.").

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.<sup>11</sup> 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.<sup>12</sup>

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

---

2006); JAY M. SHAFRITZ ET AL., *ALMANAC OF MODERN TERRORISM* 263–65 (1991); R.I.R. Abeyaratne, *The Effects of Unlawful Interference with Civil Aviation on World Peace and the Social Order*, 22 *TRANSP. L.J.* 449, 451–56 (1995); R.R. Baxter, *A Skeptical Look at the Concept of Terrorism*, 7 *AKRON L. REV.* 380, 380 (1974); Christopher L. Blakesley, *Ruminations on Terrorism & Anti-Terrorism Law & Literature*, 57 *U. MIAMI L. REV.* 1041, 1042–62 (2003); John Dugard, *International Terrorism: Problems of Definition*, 50 *INT'L AFF.* 67, 67 (1974); Thomas M. Franck & Scott C. Senecal, *Porfiry's Proposition: Legitimacy and Terrorism*, 20 *VAND. J. TRANSNAT'L L.* 195, 202 (1987); Geoffrey Levitt, *Is "Terrorism" Worth Defining?*, 13 *OHIO N.U. L. REV.* 97, 97 (1986); Michael P. Scharf, *Defining Terrorism as the Peace Time Equivalent of War Crimes: A Case of Too Much Convergence Between International Humanitarian Law and International Criminal Law?*, 7 *ILSA J. INT'L & COMP. L.* 391, 391 (2001); *see also* Stethem v. Islamic Republic of Iran, 201 F. Supp. 2d 78, 89 (D.D.C. 2002) ("All acts of terrorism are by their very definition extreme and outrageous and intended to cause the highest degree of emotional distress, literally, terror, in their targeted audience: The more extreme and outrageous, the greater the resulting distress.").

11. *See, e.g.*, WILLIAM H. REHNQUIST, *ALL THE LAWS BUT ONE: CIVIL LIBERTIES IN WARTIME* (1998); *THE WAR ON OUR FREEDOMS: CIVIL LIBERTIES IN AN AGE OF TERRORISM* (Richard C. Leone & Greg Anrig, Jr. eds., 2003); Joseph Kubler, *U.S. Citizens as Enemy Combatants: Indication of a Roll-back of Civil Liberties or a Sign of Our Jurisprudential Evolution?*, 18 *ST. JOHN'S J. LEGAL COMMENT.* 631, 674 (2004); Eric A. Posner & Adrian Vermeule, *Accommodating Emergencies*, 56 *STAN. L. REV.* 605, 605–06 (2003); Geoffrey R. Stone, *Civil Liberties in Wartime*, 28 *J. SUP. CT. HIST.* 215, 215 (2003); Daniel W. Sutherland, *Homeland Security and Civil Liberties: Protecting America's Way of Life*, 19 *NOTRE DAME J.L. ETHICS & PUB. POL'Y* 289, 302 (2005); Diane P. Wood, *The Rule of Law in Times of Stress*, 70 *U. CHI. L. REV.* 455, 455 (2003); John Yoo, *Essay, The Terrorist Surveillance Program and the Constitution*, 14 *GEO. MASON L. REV.* 565 (2007); Richard A. Posner, *Security Versus Civil Liberties*, *ATLANTIC MONTHLY*, Dec. 2001, at 46, 46; *see also* Frank Cerabino, *Hard-Won Freedoms Easily Lost, Groups Say*, *PALM BEACH POST*, Sept. 30, 2001, at 1A ("The fear and uncertainty of living among terrorists has made many Americans think that maybe Big Brother should be bigger—not smaller—and that hard-fought constitutional rights are negotiable in tough times.").

12. Compare K. A. Taipale, *Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd*, 7 *YALE J.L. & TECH.* 123, 127 (2004–2005) ("Security and privacy are not a balancing act but rather dual obligations of a liberal democracy that present a wicked problem for policy makers.") (emphasis in original), with Darren W. Davis & Brian D. Silver, *Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America*, 48 *AM. J. POL. SCI.* 28, 29 (2004) ("America's response to the terrorist attacks [of September 11, 2001] reveals a 'contestability of rights' in which the commitment to civil liberties collides with other cherished values. . . . [O]ne cannot support both liberty and order at the same time. More precisely, as support for civil liberties increases, support for order and security decreases, and vice versa.") (citation omitted).

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."<sup>13</sup> 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."<sup>14</sup>

Rejecting the notion that security is possible only at the expense of liberty and privacy,<sup>15</sup> 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.<sup>16</sup> Hijackers have since seized commercial airplanes to bargain for the exchange of political prisoners or to escape to a particular destination like Cuba.<sup>17</sup> In contrast, the objective of the September 11

---

13. 6 THE PAPERS OF BENJAMIN FRANKLIN 242 (Leonard W. Labaree et al. eds., Yale Univ. Press 1963); see also Thomas F. Powers, *Can We Be Secure and Free?*, 151 PUB. INT. 3, 5 (2003) ("In a liberal republic, liberty presupposes security; the point of security is liberty.").

14. Robert Crandall, *Security for the Future: Let's Get Our Airlines Flying*, Address at the Freedom Versus Fear: The Future of Air Travel Conference (Oct. 29, 2001), in 67 J. AIR L. & COM. 7, 19 (2002).

15. See Taipale, *supra* note 12, at 126 ("The current public debate that pits security and privacy as dichotomous rivals to be traded one for another in a zero-sum game is based on a general misunderstanding and apprehension of technology on the one hand and a mythology of privacy that conflates secrecy with autonomy on the other.").

16. See Humphrey G. Dawson, *Civil Aviation, Hijacking and International Terrorism: An Historical and Legal Review*, 15 INT'L BUS. LAW. 57, 58 (1987).

17. See *Special Report on Airport Security—Part I: Government, Industry Face Logistics Nightmare in Meeting Screening Deadline*, AIRPORT SEC. REP., Apr. 10, 2002 ("The hijackers' success on Sept. 11 relied heavily on their exploitation of the U.S. government's aviation security policy developed in response to 1970s hijackings of aircraft to Cuba and other destinations. . . .

hijackers was to kill Americans and to destroy national icons of American economic, military, and political might.<sup>18</sup>

The September 11 hijackers—ten of nineteen were identified for further security screening by a computer passenger profiling system<sup>19</sup>—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,

[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.<sup>20</sup>

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-

---

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 JAMES A. AREY, *THE SKY PIRATES* (1972); RODNEY A. SNYDER, *NEGOTIATING WITH TERRORISTS: TWA FLIGHT 847* (1994); Stanley B. Rosenfield, *Air Piracy: Is It Time To Relax Our Security?*, 9 NEW ENG. L. REV. 81, 88 (1973–1974); Mark. W. Levine, Note, *Cuban Hijackers and the United States: The Need for a Modified Aut Dedere Aut Judicare Rule*, 32 COLUM. J. TRANSNAT’L L. 133, 134 (1994).

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.’”).

19. NAT’L COMM’N ON TERRORIST ATTACKS UPON THE U.S., *THE 9/11 COMMISSION REPORT* 1 n.2 (2004) [hereinafter 9/11 REPORT].

20. Phillip A. Karber, *Re-Constructing Global Aviation in an Era of the Civil Aircraft as a Weapon of Destruction*, 25 HARV. J.L. & PUB. POL’Y 781, 793 (2002) (discussing the innovation of the September 11 terrorists to create “second-order effects”).

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.<sup>21</sup>

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."<sup>22</sup> In this new context, airline profiling systems may offer aviation security officials a preemptive and forward-looking mechanism to identify terrorists.<sup>23</sup>

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.<sup>24</sup>

---

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.

23. See U.S. DEP'T OF JUSTICE, FACT SHEET: SHIFTING FROM PROSECUTION TO PREVENTION, REDESIGNING THE JUSTICE DEPARTMENT TO PREVENT FUTURE ACTS OF TERRORISM (2002), <http://www.fas.org/irp/news/2002/05/fbireorganizationfactsheet.pdf>.

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.<sup>25</sup>

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.<sup>26</sup> Meanwhile, existing screening systems failed to notice anything remarkable when the name of America's most-wanted fugitive, Osama Bin Ladin, was tested.<sup>27</sup> 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.<sup>28</sup>

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.<sup>29</sup> And although the federal govern-

---

25. See *infra* Part II.B–C.

26. *Talk of the Nation: Flight Passenger Screening* (National Public Radio broadcast, Sept. 22, 2004) [hereinafter *Talk of the Nation*]; see also *infra* note 103 and accompanying text.

27. Timothy W. Maier, *Cracks in System Open to Terrorists*, INSIGHT, Mar. 15, 2004, at 26.

28. See Addie S. Ries, Comment, *America's Anti-Hijacking Campaign—Will It Conform to Our Constitution?*, 3 N.C. J.L. & TECH. 123, 150 (2001) ("[T]echnologies presently used to search passengers are sufficient if operated in a competent manner. [But] too much reliance on technology diverts attention from the human components necessary for an effective security program."). Using mathematical models and computer simulation, students at Massachusetts Institute of Technology wrote a paper showing "how a terrorist cell can increase thier chances of mounting a successful attack under the CAPS system as opposed to a security system that uses only random searches." Samidh Chakrabarti & Aaron Strauss, *Carnival Booth: An Algorithm for Defeating the Computer-Assisted Passenger Screening System*, FIRST MONDAY, Oct. 2002, [http://www.firstmonday.org/issues/issue7\\_10/chakrabarti](http://www.firstmonday.org/issues/issue7_10/chakrabarti).

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.<sup>30</sup> Federal security officials believed they could identify potential hijackers based on a profile—a mosaic of personal attributes hijackers typically possessed.<sup>31</sup> Specifically, FAA's "Anti-Air Hijack Profile" established approximately twenty-five characteristics empirically linked with hijackers historically.<sup>32</sup> If a passenger fit a "profile,"

---

district court noted that the racial and ethnic division of all airline travelers nationally was 88% white, 5% African American, 1% Asian, 1% Hispanic, and 4% "other." *United States v. Travis*, 837 F. Supp. 1386, 1390 (E.D. Ky. 1993).

30. The first hijacking of a commercial airplane in the United States occurred in 1961 and involved the diversion of a flight originating from Key West, Florida to Cuba. See Jack H. Daniel III, Comment, *Reform in Airport Security: Panic or Precaution?*, 53 *MERCER L. REV.* 1623, 1625 (2002). From 1961 to 1973, approximately 343 hijackings took place. *Deterring Airport Terrorist Attacks and Compensating the Victims*, 125 *U. PA. L. REV.* 1134, 1134 n.3 (1977).

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.<sup>33</sup> But FAA abandoned profiling in 1972, finding it ineffective. Instead, FAA created global security checkpoints to X-ray all carry-on luggage.<sup>34</sup>

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.<sup>35</sup> Although a defective fuel tank caused the tragedy,<sup>36</sup> government officials initially believed that terrorists had destroyed TWA Flight 800.<sup>37</sup> Consequently, on August 22, 1996 President Bill Clinton announced the creation of the "White House Commission on Aviation Safety and Security."<sup>38</sup> This

---

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.

464 F.2d 1180, 1183 (3d Cir. 1972); see also Abraham Abramovsky, *The Constitutionality of the Anti-Hijacking Security System*, 22 BUFF. L. REV. 123, 131 (1973); Alona E. Evans, *Aircraft Hijacking, What Is Being Done*, 67 AM. J. INT'L L. 641, 648-63 (1973); Gary N. Horlick, *The Developing Law of Air Hijacking*, 12 HARV. INT'L L.J. 33 (1971). See generally James L. Buchwalter, *Validity of Airport Security Measures*, 125 A.L.R. 5th 281 (2005).

33. E.g., Stephen P. Halbrook, *Firearms, The Fourth Amendment, and Air Carrier Security*, 52 J. AIR L. & COM. 585, 640 (1987).

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.").

35. Judy Pasternak, *Response to Terror Air Security*, L.A. TIMES, Oct. 6, 2001, at 1.

36. *Id.*

37. *Id.*

38. WHITE HOUSE COMM'N ON AVIATION SAFETY & SEC., FINAL REPORT TO PRESIDENT CLINTON 3 n.5 (1997) [hereinafter WHITE HOUSE COMM'N FINAL REPORT], available at <http://www.fas.org/irp/threat/212fin-1.html>; see Robert W. Hahn, *The Economics of Airline Safety and Security: An Analysis of the White House Commission's Recommendations*, 20 HARV. J.L. & PUB. POL'Y 791, 792 (1997). Also in 1996, Congress revised section 307 of the Federal Aviation Reauthorization Act of 1996, Pub. L. No. 104-264, 110 Stat. 3253, and directed the Federal Aviation Administration to assist airlines in developing a computer assisted passenger profiling system in conjunction with other security measures and technologies. In the same year, Congress amended the Foreign Sovereign Immunities Act of 1976, Pub. L. No. 94-583, 90 Stat. 2891 (codified as amended at 28 U.S.C. §§ 1330, 1602-1611 (2000)), enacting the Anti-Terrorism and Effective Death Penalty Act of 1996 to eliminate immunity that foreign states enjoyed from the jurisdiction of U.S. courts in cases involving torture, extrajudicial killing, aircraft sabotage, hostage taking, and other acts undertaken by an officials, employees, or agents of foreign states. Pub. L. No. 104-132, § 221, 110 Stat. 1214 (codified as amended at 28 U.S.C. § 1605); see also *Alejandro v. Republic of Cuba*, 996 F. Supp. 1239, 1247-48 (S.D. Fla. 1997) (explaining how the Anti-Terrorism and Effective Death Penalty Act altered the Foreign Sovereign Immunities Act).

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.”<sup>39</sup> 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.<sup>40</sup>

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.<sup>41</sup> After testing a prototype, Northwest Airlines released the profiling software to other airlines through the FAA in 1997.<sup>42</sup> The profiling

---

39. Exec. Order No. 13,015, 61 Fed. Reg. 43,937 (Aug. 22, 1996).

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 Pasternak, *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").<sup>43</sup> 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."<sup>44</sup>

CAPPS collects approximately thirty-nine pieces of pre-boarding data on random and ordered bases.<sup>45</sup> 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.<sup>46</sup> As one commentator noted, "[m]aking profiles public is necessary to make them legal, however, doing so would also destroy their usefulness."<sup>47</sup> 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);<sup>48</sup> the timing of a purchase (i.e., immediately before departure or much earlier);<sup>49</sup> the identity of travelers,<sup>50</sup> 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.<sup>51</sup> A traveler identified by CAPPS as a "selectee" is subject to sec-

---

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).

44. Dedman, *supra* note 41, at A27 (internal quotation marks omitted).

45. Ian Kilroy, *Flying in the Face of Privacy*, IRISH TIMES, Nov. 5, 2003, at 15.

46. See Nojeim, *supra* note 34, at 5.

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).

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").

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.").

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.

51. *Morning Edition*, *supra* note 49.

ondary screening:

Depending on the destination of the passenger (domestic or foreign) and the availability of advanced technology at particular airports, the additional security measure applied to selectees typically will involve one of the following: bag matching (the requirement that checked luggage be flown only if it is determined that the passenger who checked the luggage has boarded the airplane); examination by a certified explosive detection system (EDS); or examination using other advanced technology (such as explosive detection device or a trace detector).<sup>52</sup>

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.<sup>53</sup> 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.<sup>54</sup> 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.<sup>55</sup> Today, too, the risk of "false negatives," where crucial people or events are missed, is real.<sup>56</sup> 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

---

52. U.S. DEP'T OF JUSTICE, REPORT BY THE DEPARTMENT OF JUSTICE TO THE DEPARTMENT OF TRANSPORTATION ON THE DEPARTMENT'S CIVIL RIGHTS REVIEW OF THE FEDERAL AVIATION ADMINISTRATION'S PROPOSED AUTOMATED PASSENGER SCREENING SYSTEM (1997) [hereinafter DEP'T OF JUSTICE, CIVIL RIGHTS REVIEW], available at <http://www.usccr.gov/pubs/sac/mi0501/app.htm>.

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.

56. See Anita Ramasastry, *Lost in Translation? Data Mining, National Security and the "Adverse Inference" Problem*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 757, 761 (2006); see also Stephen W. Dummer, *False Positives and Secure Flight Using Dataveillance When Viewed Through the Ever Increasing Likelihood of Identity Theft*, 11 J. TECH. L. & POL'Y 259 (2006); Michael O. Finkelstein & Bruce Levin, *On the Probative Value of Evidence from a Screening Search*, 43 JURIMETRICS 265 (2003).

vital targets.<sup>57</sup>

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.”<sup>58</sup> 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.<sup>59</sup> 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.<sup>60</sup> The Gore Commission elaborated that

[f]actors to be considered for elements of the profile should be based on measurable, verifiable data indicating that the factors chosen are reasonable predictors of risk, not stereotypes or generalizations. A relationship must be demonstrated between the factors chosen and the risk of illegal activity.

. . . .

Procedures for searching the person or luggage of, or for questioning, a person who is selected by the automated profiling system should be premised on insuring respectful, non-stigmatizing, and efficient treatment of all passengers.<sup>61</sup>

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.<sup>62</sup> The DOJ concluded that CAPPS “will not have

---

57. See Rosenzweig, *supra* note 22, at 712.

58. Press Release, U.S. Dep’t of Transp., DOT Investigates Passenger Security Screening’s Impact on Minorities (June 4, 2001) (internal quotation marks omitted), available at <http://www.dot.gov/affairs/dot5501.htm>.

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.”<sup>63</sup> 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.<sup>64</sup>

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.<sup>65</sup> 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.<sup>66</sup> "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.<sup>67</sup> 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."<sup>68</sup> 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."<sup>69</sup> 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

---

65. Nojeim, *supra* note 34, at 9.

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).

67. See Yousri Omar, Note, *Plane Harassment: The Transportation Security Administration's Indifference to the Constitution in Administering the Government's Watch Lists*, 12 WASH. & LEE J. C.R. & SOC. JUST. 259, 271-72 (2006).

68. Larry Greenemeier, *TSA Extends Registered Traveler Program to Reagan National*, TECHWEBNEWS, Sept. 3, 2004, available at 2004 WLNR 4752237.

69. Ramasastry, *supra* note 56, at 777. See generally Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595 (2004) (discussing the use of personal commercial data for the purpose of law enforcement).

2004 British pop star Cat Stevens (who became a Muslim in the 1970s and is known today as Yusuf Islam)<sup>70</sup> was removed from an international flight bound for the United States. Stevens's name was on the government's "No-Fly" list.<sup>71</sup> CAPPS I also identified U.S. Senator Edward M. Kennedy (D-Mass.) and U.S. Representative Don Young (R-Alaska) for extra security scrutiny.<sup>72</sup> 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.<sup>73</sup> 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.<sup>74</sup> In this way, airline passenger profiling systems are unique for their invasiveness:<sup>75</sup>

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

---

70. Airline "Safeguards" Intrusive, and They Don't Work, FORT WAYNE J. GAZETTE (Indiana), Sept. 24, 2004, available at 2004 WL 15166654.

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.*

72. Rachel L. Swarns, *Senator? Terrorist? A Watch List Stops Kennedy at Airport*, N.Y. TIMES, Aug. 20, 2004, at A1; Sara Kehaulani Goo, *Faulty "No-Fly" System Detailed*, WASH. POST, Oct. 9, 2004, at A01.

73. See JEFFREY W. SEIFERT, CONG. RESEARCH SERV., DATA MINING AND HOMELAND SECURITY: AN OVERVIEW 22-23 (2007), <http://www.fas.org/sgp/crs/intel/RL31798.pdf>; see also Ramasastry, *supra* note 56, at 762; DANIEL J. WEITZNER ET AL., MIT COMPUTER SCI. AND ARTIFICIAL INTELLIGENCE LAB., TRANSPARENT ACCOUNTABLE DATA MINING: NEW STRATEGIES FOR PRIVACY PROTECTION 3 (2006), <http://www.w3.org/2006/01/tami-privacy-strategies-aaai.pdf>.

74. See U.S. GEN. ACCOUNTING OFFICE, AVIATION SECURITY: COMPUTER-ASSISTED PASSENGER PRESCREENING SYSTEM FACES SIGNIFICANT IMPLEMENTATION CHALLENGES 42 (2004), available at <http://www.gao.gov/new.items/d04385.pdf>.

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.<sup>76</sup>

These criticisms eventually reached TSA, which offered to make several modifications to the proposed CAPPS II program.

TSA suggested three significant amendments to the CAPPS II design.<sup>77</sup> First, TSA agreed to erase most passenger information in the CAPPS II system within seven days after passengers completed their scheduled travel.<sup>78</sup> TSA also proposed appellate mechanisms for passengers erroneously targeted for heightened, secondary security screening.<sup>79</sup> Most important, TSA proposed limiting the use of private commercial data to compose a traveler's security profile.<sup>80</sup> In particular, TSA proposed transmitting PNR information to commercial data providers solely for the purpose of authenticating a passenger's identity.<sup>81</sup> Commercial data miners, in turn, would evaluate whether a passenger is who he represented he was when reserving a flight.<sup>82</sup> On completion of this authentication process, the CAPPS II system would review a passenger's commercial identity against intelligence and law enforcement databases.<sup>83</sup> Passengers positively identified without any corresponding matches with intelligence or law enforcement data would proceed to their flights.<sup>84</sup> Those passengers with more remarkable profiles would be subjected to further search or law enforcement action or both.<sup>85</sup> 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

---

76. Dempsey & Flint, *supra* note 31, at 1471.

77. See Interim Final Privacy Notice, 68 Fed. Reg. 45,265 (Aug. 1, 2003); Privacy Notice Act, 68 Fed. Reg. 2101 (Jan. 15, 2003).

78. Interim Final Privacy Notice, 68 Fed. Reg. at 45,267.

79. *Id.* at 45,269.

80. *Id.* at 45,267.

81. *Id.* at 45,266.

82. *Id.*

83. *Id.*

84. *Id.*

85. *Id.*

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).<sup>86</sup> 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.<sup>87</sup> This information was collected and transmitted without the knowledge or consent of the passengers whose identity was disclosed.<sup>88</sup> Several other airlines were sued as their collaboration with the federal government to develop CAPPS II emboldened profiling system opponents.<sup>89</sup> 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."<sup>90</sup>

### 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

---

86. Philip Shenon, *Airline Gave Up Passenger Data: Private Information on Customers Was Given to Defense Contractor To Assess Terrorism Risks*, PITTSBURGH POST-GAZETTE, Sept. 20, 2003, at A5.

87. See TORCH CONCEPTS, INC., HOMELAND SECURITY—AIRLINE PASSENGER RISK ASSESSMENT (2003), [http://www.abditum.com/~rabbi/S3B3\\_Roark.pdf](http://www.abditum.com/~rabbi/S3B3_Roark.pdf).

88. See *In re Jetblue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299 (E.D.N.Y. 2005).

89. See, e.g., *In re American Airlines, Inc., Privacy Litig.*, 370 F. Supp. 2d 552 (N.D. Tex. 2005); *Elec. Privacy Info. Ctr. v. Dep't of Homeland Sec.*, 384 F. Supp. 2d 100, 104 (D.D.C. 2005); *Dyer v. Northwest Airlines Corps.*, 334 F. Supp. 2d 1196 (D.N.D. 2004); *In re Northwest Airlines Privacy Litig.*, No. 04-126, 2004 WL 1278459 (D. Minn. June 6, 2004); *Turrett v. JetBlue Airways*, No. 03-6785, 2003 WL 22843134 (C.D. Cal. Nov. 25, 2003). See generally Richard Sobel & John A. Fennel, *Troubles with Hiibel: How the Court Inverted the Relationship Between Citizens and the State*, 48 S. TEX. L. REV. 613 (2007); Drew Shenkman, Comment, *Flying the Not-So-Private Skies: How Passengers' Personal Information Privacy Stopped at the Airplane Door, and What (If Anything) May Be Done To Get It Back*, 17 ALB. L.J. SCI. & TECH. 667 (2007). For a discussion of the doctrine of standing in lawsuits involving data-mining and surveillance see Eugene Kontorovich, *What Standing Is Good For*, VA. L. REV. 1663, 1687–88 (2007).

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.”<sup>91</sup> Secure Flight was designed to improve government “No-Fly” and “automatic selectee” lists.<sup>92</sup> 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.<sup>93</sup> 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.”<sup>94</sup>

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.<sup>95</sup> 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-

---

91. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 102, 118 Stat. 3638, 3715.

92. See generally *Gilmore v. Gonzales*, 435 F.3d 1125, 1140 (9th Cir. 2006), cert. denied, 127 S. Ct. 929 (2007) (rejecting an airline passenger’s claim that the government’s identification policy, including CAPPS, CAPPS II, and No-Fly and Selectee lists, were an unconstitutional “scheme”); *Pub. Citizen, Inc. v. Fed. Aviation Admin.*, 988 F.2d 186, 197–98 (D.C. Cir. 1993) (upholding aviation security rules adopted by the Federal Aviation Administration in response to the Aviation Security Improvement Act of 1990); *Ibrahim v. Dep’t of Homeland Sec.*, No. C06-00545 WHA, 2006 WL 2374645 at \*1 (N.D. Cal. Aug. 16, 2006) (finding that the court lacked subject matter jurisdiction to consider the constitutionality of a No-Fly List); Garrett Hodes, Comment, *Terrorist Threats: The Friendly Skies Aren’t Too Friendly About Notification*, 46 U. KAN. L. REV. 365, 368 (1998) (discussing the Aviation Security Improvement Act of 1990 and public notifications of terrorist threats to civil aviation); Peter M. Shane, *The Bureaucratic Due Process of Government Watch Lists*, 75 GEO. WASH. L. REV. 804 (2007).

93. See Daniel J. Steinbock, *Designating the Dangerous: From Blacklists to Watch Lists*, 30 SEATTLE U. L. REV. 65, 77–89 (2006); Ricardo Alonso-Zaldivar, *New Passenger Profiling System To Be Tested*, L.A. TIMES, Aug. 27, 2004, at A12; Angela Kim, *TSA Directs Airlines To Hand over PNR in 40 Days*, AVIATION DAILY, Sept. 22, 2004, at 1.

94. Bill Scannell, *TSA Cannot Be Trusted*, USA TODAY, Sept. 28, 2004, at 12A.

95. Congress federalized the aviation security system after September 11, 2001. In addition to creating DHS (of which TSA is a part) in November, 2001, the government also assumed responsibility for screening passengers, a task historically managed by private airlines through independent contractors. As a result, all airport screeners are federal employees. See Aviation and Transportation Security Act, Pub. L. No. 107-71, 115 Stat. 597 (2001) (to be codified in scattered sections of 49 U.S.C.). See generally Andrew Hessick, *The Federalization of Airport Security: Privacy Implications*, 24 WHITTIER L. REV. 43 (2002).

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").<sup>96</sup>

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.<sup>97</sup> 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 multi-million-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.<sup>98</sup>

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."<sup>99</sup> Thus, where

CAPPS II . . . required the airlines to turn over only passenger names, dates of birth, home addresses and home telephone numbers[,] Secure

---

96. See U.S. DEP'T OF JUSTICE, REVIEW OF THE TERRORIST SCREENING CENTER'S EFFORTS TO SUPPORT THE SECURE FLIGHT PROGRAM i-ix (2005), <http://www.usdoj.gov/oig/reports/FBI/a0534/final.pdf>.

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).

98. See Leslie Miller, *Multimillion-dollar Anti-Terror Identity Checks Failing Tests*, DAILY BREEZE (Torrance, Cal.), Oct. 26, 2006, at A11.

99. Matthew L. Wald, *U.S. Airlines Forced To Give Data on Travelers; For Antiterror Screen, Government Wants Name, Numbers, Meals*, INT'L HERALD TRIB., Sept. 23, 2004, at 1. Secure Flight was not designed to apply to foreign airlines, yet the names of European passengers who flew on U.S. airlines probably were among those tested. In its testing phase, therefore, Secure Flight may have violated European privacy laws. See Steve Boggan, *Privacy: The New Security Alert*, TIMES (London), Oct. 14, 2003, at 6; Leslie Miller, *Flier ID Test Stirs Privacy Fears: Security Check Exercise Requires Passenger Records*, HOUS. CHRON., Nov. 20, 2004, at A25; see also *infra* Part III.D.

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.<sup>100</sup>

This prompted privacy advocates to contend Secure Flight was more invasive than CAPPS II.<sup>101</sup>

In fact, Secure Flight generated the type of constitutionally based opposition that defeated the CAPPS II program.<sup>102</sup> Citizens themselves expressed mixed opinions about Secure Flight, including whether and how it would avoid or remedy circumstances of identity theft.<sup>103</sup> 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.").

102. See, e.g., Leigh A. Kite, Note, *Red Flagging Civil Liberties and Due Process Rights in Airline Passengers: Will a Redesigned CAPPS II System Meet the Constitutional Challenge?*, 61 WASH. & LEE L. REV. 1385, 1392 (2004). For more information on the changes between CAPPS II and Secure Flight, see Stephen W. Dummer, Comment, *Secure Flight and Data Veillance, a New Type of Civil Liberties Erosion: Stripping Your Rights When You Don't Even Know It*, 75 MISS. L.J. 583, 590 (2006).

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.<sup>104</sup> 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

---

[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).

104. Elec. Privacy Info. Ctr. v. Transp. Sec. Admin., No. Civ.A. 03-1846 CKK, 2006 WL 626925, at \*1 (D.D.C. Dec. 11, 2002); Sarah Lai Stirland, *Public-Interest Group Challenges FBI over Terrorist Screening*, TECH. DAILY, Oct. 18, 2004, available at <http://www.govexec.com/dailyfed/1004/101804tdpm1.htm>; *see also* JAYASHRI SRIKANTIAH, ACLU OF N. CAL., THE PUBLIC STILL LACKS BASIC INFORMATION ABOUT THE "NO FLY" LIST: AN ANALYSIS OF TSA'S FOIA RESPONSE 1 (2003), <http://www.aclu.org/FilesPDFs/072103-noflysummary.pdf> (discussing the TSA's response to requests made by the ACLU and two activists whose names were on the No-Fly list for information about the list).



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.<sup>105</sup>

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.<sup>106</sup>

These and other unresolved concerns about the purpose and architecture of Secure Flight doomed the program in 2006.<sup>107</sup> 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.<sup>108</sup>

---

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.’”).

106. SECURE FLIGHT WORKING GROUP, REPORT OF THE SECURE FLIGHT WORKING GROUP 5 (2005), [http://www.epic.org/privacy/airtravel/sfwg\\_report\\_091905.pdf](http://www.epic.org/privacy/airtravel/sfwg_report_091905.pdf); see also U.S. GOV’T ACCOUNTABILITY OFFICE, AVIATION SECURITY: MEASURES FOR TESTING THE IMPACT OF USING COMMERCIAL DATA FOR THE SECURE FLIGHT PROGRAM, GAO-05-324 (2005), available at <http://www.gao.gov/new.items/d05324.pdf> (reporting results of GAO’s review of measures developed by TSA to assess the effect of using commercial on aviation security); U.S. GOV’T ACCOUNTABILITY OFFICE, AVIATION SECURITY: SECURE FLIGHT DEVELOPMENT AND TESTING UNDER WAY, BUT RISKS SHOULD BE MANAGED AS SYSTEM IS FURTHER DEVELOPED GAO-05-356 (2005), available at <http://www.gao.gov/new.items/d05356.pdf> (addressing the status, effectiveness, and impact on passengers and passenger rights associated with the Secure Flight program).

107. See U.S. GOV’T ACCOUNTABILITY OFFICE, AVIATION SECURITY: SIGNIFICANT MANAGEMENT CHALLENGES MAY ADVERSELY AFFECT IMPLEMENTATION OF THE TRANSPORTATION SECURITY ADMINISTRATION’S SECURE FLIGHT PROGRAM, GAO-06-374T 4–8 (2006), available at <http://www.gao.gov/new.items/d06374t.pdf>.

108. Eric Lipton, *U.S. Official Admits to Big Delay in Revamping No-Fly Program*, N.Y. TIMES, Feb. 21, 2007, at A17; Wait ‘Til Next, Next Year, AVIATION WK. & SPACE TECH., Jan. 22, 2007, at 23.

#### 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.<sup>109</sup> The product of this mandate is the “Registered Traveler” program.<sup>110</sup>

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,<sup>111</sup> 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.<sup>112</sup> After also undergoing a security threat assess-

---

109. See 49 U.S.C.A. § 44903 (West 2007); David Hughes, *New Direction in Screening*, AVIATION WK. & SPACE TECH., Aug. 21, 2006, at 57; see also *The Promise of Registered Traveler Part I and II: Hearing Before the Subcomm. on Economic Security, Infrastructure Protection, and Cybersecurity of the Comm. on Homeland Security House of Representatives*, 109th Cong. 32 (2005) (addressing whether the Registered Traveler Program enhances security and promotes efficiency in airport screening operations); *Implementation of the Aviation and Transportation Security Act with a Focus on the 60-Day Deadline for Screening Checked Baggage: Hearing Before the Subcomm. on Aviation of the H. Comm. on Transp. and Infrastructure*, 107th Cong. (2002) (discussing baggage screening measures).

110. See generally TRANSP. SEC. ADMIN., REGISTERED TRAVELER PROGRAM BUSINESS MODEL (2006), [http://www.tsa.gov/assets/pdf/rt\\_business\\_model.pdf](http://www.tsa.gov/assets/pdf/rt_business_model.pdf); U.S. GEN. ACCOUNTING OFFICE, AVIATION SECURITY: REGISTERED TRAVELER PROGRAM POLICY AND IMPLEMENTATION ISSUES, GAO-03-253, at 1, 29–30 (2002), available at <http://www.gao.gov/new.items/d03253.pdf>; Mardi Ruth Thompson & Kapila Juthani, *Providing Smarter Security and Customer Service: TSA's Secure Flight and Registered Traveler Programs*, 19 AIR & SPACE LAW. 8, 10 (2005) (explaining the purpose and characteristics of both the Secure Flight and Registered Traveler Programs).

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](http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_rt.pdf).

112. See Eric P. Haas, Comment, *Back to the Future? The Use of Biometrics, Its Impact on Airport Security, and How This Technology Should Be Governed*, 69 J. AIR L. & COM. 459, 478 (2004). See generally John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns—Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97 (1997), for a treatment of government use of biometrics, and Greg Star, Comment, *Airport Security Technology: Is the Use of Biometric Identification Technology Valid Under the Fourth Amendment?*, 20 TEMP. ENVTL. L. & TECH. J. 251 (2002), for a discussion of the use of biometrics in accordance with the Aviation and Transportation Security Act and the Fourth Amendment.

ment, registered or "Trusted Travelers" with smart cards are able to cut waiting time by bypassing standard airport screening processes to a special security screening lane.<sup>113</sup>

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.<sup>114</sup> Meanwhile, private service providers at sponsoring airports administer Registered Traveler.<sup>115</sup> 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."<sup>116</sup> 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.<sup>117</sup> In an open

---

113. See Stephen Majors, *Passengers Skip Line—For a Price*, MIAMI HERALD, Jan. 6, 2007, at 1C.

114. See Transp. Sec. Admin., Registered Traveler, [http://www.tsa.gov/what\\_we\\_do/layers/rt/index.shtm](http://www.tsa.gov/what_we_do/layers/rt/index.shtm) (last visited Oct. 13, 2007).

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.

TRANSP. SEC. ADMIN., TSA REGISTERED TRAVELER: SECURITY, PRIVACY AND COMPLIANCE STANDARDS FOR SPONSORING ENTITIES AND SERVICE PROVIDERS § 3.4.5, at 27 (2007), available at [http://www.tsa.gov/assets/pdf/rt\\_standards\\_v3\\_0.pdf](http://www.tsa.gov/assets/pdf/rt_standards_v3_0.pdf).

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.<sup>118</sup>

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.”<sup>119</sup> 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.”<sup>120</sup> Finally, the ACLU has suggested that

---

118. Steven Brill, A Message from Clear's CEO, Steven Brill, <http://www.flyclear.com/clear-ceosmessage.html> (last visited Oct. 13, 2007).

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”).

120. Editorial, *Cutting Corners at Airports; Plans for Speeding Up Security Checks Are Troubling*, SARASOTA HERALD-TRIB., Nov. 12, 2005, at A24. *Contra* Editorial, *How Much Would You Pay To Skip Airport Security Lines?*, PORTLAND PRESS HERALD (Maine), Nov. 8, 2005, at A10 (“[T]he ACLU is off base [because] these registered travelers will be voluntarily submitting

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.<sup>121</sup> 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.”<sup>122</sup>

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.<sup>123</sup> 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-

---

their information and fingerprints. As for the apparent privilege of buying convenience—it’s no different than the longstanding and widely accepted system of offering first-class and coach fares by most airlines.”); Editorial, *Screening Plan Makes Sense*, KANSAS CITY STAR, Nov. 8, 2005 (“[T]he ACLU . . . voiced concerns that participants would have to give too much personal information, and many would be unable to afford the fee. . . . [But w]ithout personal information, no background check can be thorough. And participation is voluntary.”).

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 Computertech 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.’”).

123. See Peter J. Howe, *Logan To Start Express Security Program This Summer*, BOSTON GLOBE, Jan. 20, 2006, at A1.

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.<sup>124</sup> 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.”<sup>125</sup>

### III. DISCUSSION

As the fifth anniversary of September 11 approached, Americans considered whether commercial airline security had improved since 2001.<sup>126</sup> The unsuccessful August 10, 2006 terrorist plot to detonate liquid explosives aboard international airplanes bound for the United States offered a somber perspective.<sup>127</sup> 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.<sup>128</sup> Some jetliners were escorted to the ground by fighter planes.<sup>129</sup> 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.<sup>130</sup> 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.<sup>131</sup> An American Airlines flight from Manchester,

---

124. *Senate Approves Sen. Martinez Amendment Creating International Registered Traveler Program*, U.S. FED. NEWS, July 27, 2007, available at 2007 WLNR 14485361.

125. Otto Kreisher, *Frustration Raised over Registered Traveler Program Delays*, CONGRESS DAILY, Aug. 1, 2007, available at 2007 WLNR 14694614 (internal quotation marks omitted).

126. See 9/11 REPORT, *supra* note 19, at 383 (“[A]lthough Americans may be safer, they are not safe.”).

127. See Jessica E. Vascellaro, *Air Safety: What Has and Hasn’t Changed*, WALL ST. J., Aug. 19, 2006, at A9 (“‘If last week’s foiled terror plot was not a wake-up call to jump-start our screening technology, then I don’t know what is,’ [Senator Charles Schumer (D-N.Y.) stated].”).

128. See, e.g., *NBC Nightly News with Brian Williams: Nine Flights Grounded amid Security Concerns* (NBC television broadcast Aug. 25, 2006).

129. See *id.* Notwithstanding official statements to the contrary, some Americans believe one of the four airplanes hijacked on September 11, 2001 was shot down by U.S. military fighters. See 9/11 REPORT, *supra* note 19, at 40–46. See generally Kay Hailbronner, *Freedom of the Air and the Convention on the Law of the Sea*, 77 AM. J. INT’L L. 490, 514 (1983) (“[Internationally,] [e]ven if an order to land is deliberately disregarded, a civil unarmed aircraft that intrudes into foreign airspace may not be fired upon.”).

130. See Elizabeth Mehren, *7 Incidents in a Day Show Air Travel Anxiety Is Up*, L.A. TIMES, Aug. 26, 2006, at A1.

131. *FBI: Dynamite Found in Luggage*, CNN.COM, Aug. 25, 2006, <http://www.cnn.com/2006/>

England to Chicago, Illinois was forced to land in Bangor, Maine at a former military base because of an unspecified threat.<sup>132</sup> 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.<sup>133</sup> 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.<sup>134</sup> A utility knife was discovered on an empty passenger seat of a Pennsylvania to Connecticut U.S. Airways flight.<sup>135</sup> An Aer Lingus flight originating in New York was evacuated during a scheduled stopover in western Ireland following an unfounded bomb threat.<sup>136</sup> 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.<sup>137</sup>

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.<sup>138</sup> Authorities responsible for aviation security must assume the worst and entertain both credible and incredible threats at any time, every time.<sup>139</sup> Terrorism is asymmetrical

---

US/08/25/dynamite.plane/index.html ("The passenger said he had been exploring mines in Bolivia and purchased the dynamite as a souvenir . . .").

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](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 1A (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.<sup>140</sup> 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.<sup>141</sup>

### A. *Identifying the Enemy*

The initial questions borne of September 11 were “What happened?” and “Who did this?” These questions are resolved.<sup>142</sup> 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.<sup>143</sup>

---

right once, while we must be right every day, all the time[. . .], stated Fran Townsend, Assistant to the President for Homeland Security and Counterterrorism.”]); *see also* *Motivation and Aviation as a Terrorism Target*, IBPPONLINE, Nov. 5, 2003, [http://security.pr.erau.edu/read.php?kind=html&article\\_volume=15&article\\_issue=10&article\\_title=Motivation%20and%20Aviation%20as%20a%20Terrorism%20Target](http://security.pr.erau.edu/read.php?kind=html&article_volume=15&article_issue=10&article_title=Motivation%20and%20Aviation%20as%20a%20Terrorism%20Target) (“Unfortunately, aviation terrorism is an activity with a huge terrorist advantage—with terrorists picking their spots while security authorities maintain continuous vigilance; with even operationally unsuccessful terrorist operations achieving at least some psychopolitical success through raising anxiety, distrust in leaders, and pressure towards visible and concurrently ineffective programs among population segments who believe that they are or might be under attack.”).

140. *See* RON SUSKIND, *THE ONE PERCENT DOCTRINE: DEEP INSIDE AMERICA’S PURSUIT OF ITS ENEMIES SINCE 9/11*, at 62 (2006).

141. *See* Bob Barr, *Post-9/11 Electronic Surveillance Severely Undermining Freedom*, 41 VAL. U. L. REV. 1383, 1383–85 (2007); Bennie G. Thompson, *The National Counterterrorism Center: Foreign and Domestic Intelligence Fusion and the Potential Threat to Privacy*, 10 PGH. J. TECH. L. & POL’Y 1, 1 (2006).

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 [t]he 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.<sup>144</sup> 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”).<sup>145</sup> Success of this program is critical if commercial aviation security policy is to get beyond “the culture of contraband.”<sup>146</sup>

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).

144. See David Armstrong & Joseph Pereira, *Flight Risks: Nation’s Airlines Adopt Aggressive Measures for Passenger Profiling*, WALL ST. J., Oct. 23, 2001, at A1; Paul Nyhan, *Airlines Will Be Watching for Nervous Passengers*, SEATTLE POST-INTELLIGENCER, Sept. 14, 2001, at A3.

145. See Press Release, Transp. Sec. Admin., TSA Designs and Tests Curriculum To Train Police Officers To Spot Terrorist-Related Activity (Apr. 6, 2006), available at [http://www.tsa.gov/press/releases/2006/press\\_release\\_0655.shtml](http://www.tsa.gov/press/releases/2006/press_release_0655.shtml); Denise Lavoie, *Lawsuit Challenges Profiling at Airports*, ASSOCIATED PRESS, Dec. 3, 2007, WL 12/3/07 APONLINEUS 22:48:54; Eric Lipton, *Faces, Too, Are Searched as U.S. Airports Try To Spot Terrorists*, N.Y. TIMES, Aug. 17, 2006, at A1; Laura Meckler & Daniel Michaels, *Airline Terror Plot: Aircraft-Security Focus Swings to People*, WALL ST. J., Aug. 12, 2006, at A4.

146. Editorial, *Airport Security; Hair Gels, Lipstick and Terrorism*, WASH. POST, Aug. 20, 2006, at B6.

passengers themselves. They screen passengers individually and personally in a process taking hours per person.<sup>147</sup> 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.<sup>148</sup> 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.<sup>149</sup> As a result of security processes like these, no successful hijackings have ever occurred out of an Israeli airport.<sup>150</sup>

Behavioral profiling has flaws, though. "Learning to defeat poorly trained screeners is a lot easier than learning to fly a jumbo jet[.]"<sup>151</sup> 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.<sup>152</sup>

---

147. See Larry Derfner, *Stereotyping Security*, JERUSALEM POST, Mar. 23, 2007, at 14.

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.]").

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 . . .").

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.").

151. *Id.*

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 ("[S]ix 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.<sup>153</sup> Additionally, individuals drawn to terrorism may have been recruited because of common situations.<sup>154</sup> 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.<sup>155</sup> 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.<sup>156</sup> 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.”<sup>157</sup> Meanwhile, the social background of the Salafi mujahedin, for example—their geographical origins,<sup>158</sup> socioeconomic status,<sup>159</sup> 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.<sup>160</sup>

---

securely.”); Libby Sander, *6 Imams Removed from Flight for Behavior Deemed Suspicious*, N.Y. TIMES, Nov. 22, 2006, at A18 (noting that the incident involving the Muslim clerics spurred claims of racial profiling and stereotyping).

153. SAGEMAN, *supra* note 6, at 69.

154. *Id.*

155. Summary of *Jihadi Terrorists in Europe, Their Characteristics and the Circumstances in Which They Joined the Jihad: An Exploratory Study*, <http://www.clingendael.nl/cscp/publications/?publications/?id=6480&&type=summary>; Whitlock, *supra* note 6, at A1.

156. Whitlock, *supra* note 6, at A1.

157. *Id.*

158. SAGEMAN, *supra* note 6, at 70 (“[A]bout two-thirds of the 172 mujahedin in the sample come from Saudi Arabia (31), Egypt (24), France (18), Algeria (15), Morocco (14), and Indonesia (12).”).

159. *Id.* at 73–74 (“[A]bout three-fourths [of 102 people on whom data was gathered] of global Salafi mujahedin were solidly upper or middle class, refuting the argument that terrorism arises from poverty.”).

160. *Id.* at 96 (“Members of the global Salafi jihad were generally middle-class, educated young men from caring and religious families, who grew up with strong positive values of religion, spirituality, and concern for their communities.”). Additionally, the vast majority of a

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.<sup>161</sup> The thesis that terrorists suffer from pathological narcissism, paranoia, or an authoritarian personality have found little empirical support, too.<sup>162</sup> Of a sample of sixty-one “terrorists” about whom some childhood data existed, only four had evidence of antisocial personality disorder.<sup>163</sup> Two of those individuals were Christian converts, i.e., Jose Padilla<sup>164</sup> and Richard Reid.<sup>165</sup> Even the fact that terrorist tactics involve suicide is explicable in a cultural context of martyrdom rather than insanity.<sup>166</sup> 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).

161. See SAGEMAN, *supra* note 6, at 81; see also HERVEY CLECKLEY, *THE MASK OF SANITY: AN ATTEMPT TO REINTERPRET THE SO-CALLED PSYCHOPATHIC PERSONALITY* (1941); MAXWELL TAYLOR, *THE FANATICS: A BEHAVIOURAL APPROACH TO POLITICAL VIOLENCE* (1991). *Contra* Paul R. McHugh, *A Psychiatrist Looks at Terrorism: There's Only One Way To Stop Fanatical Behavior*, WKLY. STANDARD, Dec. 10, 2001, at 21 (stating that both terrorist behavior and anorexia nervosa are associated with a passionate attitude, termed an “overvalued idea”).

162. SAGEMAN, *supra* note 6, at 83–91; see also RICHARD M. PEARLSTEIN, *THE MIND OF THE POLITICAL TERRORIST* 15–32 (1991) (discussing narcissism and the psychology of the political terrorist); Jerrold M. Post, *Terrorist Psycho-Logic: Terrorist Behavior as a Product of Psychological Forces*, in *ORIGINS OF TERRORISM* 25 (Walter Reich ed., 1990) (noting that no major psychopathology was revealed in the study of the psychology of terrorists); ROBERT S. ROBINS & JERROLD M. POST, *POLITICAL PARANOIA: THE PSYCHOPOLITICS OF HATRED* 103 (1997) (“[M]any drawn to the path of terrorism have a paranoid disposition and find the externalizing rhetoric attractive.”); Salman Akhtar, *The Psychodynamic Dimension of Terrorism*, 29 *PSYCHIATRIC ANNALS* 350, 351 (1999) (“[E]vidence does exist that most major players in a terrorist organization are, themselves, deeply traumatized individuals.”); Jerrold M. Post, *Hostilité, Conformité, Fraternité: The Group Dynamics of Terrorist Behavior*, 36 *INT'L J. GROUP PSYCHOTHERAPY* 211–24 (1986) (discussing the existence of a uniformity in terrorist behavior); Jerrold M. Post, *Narcissism and the Charismatic Leader–Follower Relationship*, 7 *POL. PSYCHOL.* 675–88 (1986); Jerrold M. Post, *Notes on a Psychodynamic Theory of Terrorist Behavior*, 7 *TERRORISM: AN INT'L J.*, 241, 241 (1984) (“Because of the diversity of terrorist groups and causes, there is ‘no one terrorist mindset.’”); Andrew Silke, *Cheshire-Cat Logic: The Recurring Theme of Terrorist Abnormality in Psychological Research*, 4 *PSYCHOL., CRIME & L.* 51, 62–68 (1998) (concluding that psychological evidence indicates that “terrorists are normal people”).

163. SAGEMAN, *supra* note 6, at 81.

164. *Id.*

165. Pam Belluck, *Threats and Response: The Bomb Plot; Unrepentant Shoe Bomber Is Given a Life Sentence for Trying To Blow Up Jet*, N.Y. TIMES, Jan. 31, 2003, at A13.

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.<sup>167</sup> 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.”<sup>168</sup>

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.<sup>169</sup> 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.<sup>170</sup> 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.<sup>171</sup> 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.<sup>172</sup> 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).

170. 509 U.S. 579, 593–94 (1993).

171. See cases cited *supra* note 89.

172. See Bernard E. Harcourt, *Rethinking Racial Profiling: A Critique of the Economics, Civil Liberties, and Constitutional Literature, and of Criminal Profiling More Generally*, 71 U. CHI. L. REV. 1275, 1275–76 (2004); Yoram Margalioth & Tomer Blumkin, *Targeting the Majority: Redesigning Racial Profiling*, 24 YALE L. & POL’Y REV. 317, 328 (2006).

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?”<sup>173</sup> 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.”<sup>174</sup> 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.<sup>175</sup> Yet, profiling and discrimination are common, lawful features of economic life in America today because of the commoditization of personal information.<sup>176</sup> Banks and supermarkets have long used profiling as marketing and strategic planning tools.<sup>177</sup> 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).

174. Bernard E. Harcourt, *AGAINST PREDICTION: PROFILING, POLICING, AND PUNISHING IN AN ACTUARIAL AGE* 238 (2007).

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.

176. See, e.g., Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 66–67 (2003); Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1035–42 (1999).

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.<sup>178</sup> 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.<sup>179</sup> 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.<sup>180</sup> 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.<sup>181</sup> In 1798, for example, Congress passed the Alien Enemies Act, which allowed President John Adams to deport noncitizens identified as threats to the coun-

---

Bercu, *Smart Card Technology, Novel Privacy Concerns and the Legal Response*, 7 J. PROPRIETY RTS. 2 (1995); Oliver Ireland & Rachel Howell, *The Fear Factor: Privacy, Fear, and the Changing Hegemony of the American People and the Right to Privacy*, 29 N.C. J. INT'L L. & COM. REG. 671, 673-74 (2004); Janet Dean Gertz, Comment, *The Purloined Personality: Consumer Profiling in Financial Services*, 39 SAN DIEGO L. REV. 943, 960-63 (2002); Allison Kidd, Recent Development, *A Penny Saved, A Lifestyle Learned? The California and Connecticut Approaches to Supermarket Privacy*, 4 N.C. J.L. & TECH. 143, 144-45 (2002) (stating that supermarkets use customer discount cards associated with a customer's Social Security number or driver's license number to record purchases of food, personal hygiene products, tobacco products, alcohol, over-the-counter medicines, and sometimes prescription drugs, and that they share such information with marketers and product manufacturers); Lisa Jane McGuire, Comment, *Banking on Biometrics: Your Bank's New High-Tech Method of Identification May Mean Giving Up Your Privacy*, 33 AKRON L. REV. 441, 442-43 (2000). For a discussion of the different types of data in computer-based profiling, see sources cited *supra* note 31 and accompanying text.

178. Jane Kaufman Winn & James R. Wrathall, *Who Owns the Customer? The Emerging Law of Commercial Transactions in Electronic Customer Data*, 56 BUS. LAW. 213, 218 (2000) ("The regulation of the airline CRS system is an early example of the importance of data warehousing and customer profiling to competition in global markets."). See generally Timothy M. Ravich, *Deregulation of the Airline Computer Reservation Systems (CRS) Industry*, 69 J. AIR L. & COM. 387 (2004) (discussing airline deregulation and the use of computer reservation systems).

179. See 28 U.S.C. § 1862 (2000); *Batson v. Kentucky*, 476 U.S. 79, 80 (1986) ("Purposeful racial discrimination in selection of the venire violates a defendant's right to equal protection . . .").

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).

try without due process of the law.<sup>182</sup> Later, during the Civil War, President Abraham Lincoln suspended the writ of habeas corpus on eight occasions.<sup>183</sup> 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.<sup>184</sup> In 1917, during World War I, federal authorities prosecuted opponents to the war under the Espionage Act.<sup>185</sup> 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*<sup>186</sup>—a now disgraced decision.<sup>187</sup> 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

---

182. See Act of July 6, 1798, ch. 66, 1 Stat. 577 (current version at 50 U.S.C. §§ 21–24 (2000)); Act of June 25, 1798 (Alien Enemies Act), ch. 58, 1 Stat. 570 (expired 1800).

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

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

185. Espionage Act (Barbour Espionage Act), ch. 30, 40 Stat. 217 (1917) (codified as amended at 18 U.S.C., 22 U.S.C., and 50 U.S.C. (2000)).

186. 323 U.S. 214, 223–24 (1944).

187. See Natsu Taylor Saito, *Symbolism Under Siege: Japanese American Redress and the “Racing” of Arab Americans as “Terrorists”*, 8 ASIAN L.J. 1, 11 (2001); Mark Tushnet, *Defending Korematsu?: Reflections on Civil Liberties in Wartime*, 2003 WIS. L. REV. 273, 273 (2003); Frank H. Wu, *Profiling in the Wake of September 11: The Precedent of the Japanese American Internment*, CRIM. JUST., Summer 2002, at 52, 54–55; Liam Braber, Comment, *Korematsu’s Ghost: A Post-September 11th Analysis of Race and National Security*, 47 VILL. L. REV. 451, 467–69 (2002).



security measure, and that at least in the realm of discrimination, liberty and security do not conflict.<sup>188</sup>

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.<sup>189</sup> Following the thwarted liquid-bomb plot of August 10, 2006 the *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

188. *Alshrafi v. American Airlines, Inc.*, 321 F. Supp. 2d 150, 152 (D. Mass. 2004).

189. See Albert W. Alschuler, *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, *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, *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, *The Citizen and the Terrorist*, 49 UCLA L. REV. 1575, 1576–77 (2002) [hereinafter *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, 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.").

public interest than the allocation of federal set-asides.<sup>190</sup>

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.<sup>191</sup>

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 Hizbullah, Salafi, and smaller non-Muslim ("single issue") groups—as posing a "persistent and evolving terrorist threat" to the United States.<sup>192</sup> 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.<sup>193</sup> The

---

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.").

191. Stuart Taylor Jr., *The Case for Using Racial Profiling at Airports*, NAT'L J., Sept. 22, 2001, at 2877. But see Naureen Kamdar, *'Muslim Americans are Americans, Too'*, *Airport Security's Stereotypical Act Shames System*, ATLANTA J.-CONST., Feb. 20, 2007, at 11A, for an editorial by an American college student of Pakistani heritage selected for heightened airport screening. "I even understand that suspicion of Muslims is inevitable. . . . What I don't understand is why of any of that—beards or scarves included—allows bullying of American Muslims by airport security officials," she said. *Id.*

192. NAT'L INTELLIGENCE COUNCIL, NATIONAL INTELLIGENCE ESTIMATE: THE TERRORIST THREAT TO THE US HOMELAND (July 2007), available at [http://www.dni.gov/press\\_releases/20070717\\_release.pdf](http://www.dni.gov/press_releases/20070717_release.pdf).

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.<sup>194</sup> 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.<sup>195</sup>

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.<sup>196</sup> As the U.S. Court of Appeals for the Fourth Circuit reasoned,

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

---

B. Darmer et al. eds., 2004); Susan M. Akram & Kevin R. Johnson, *Race, Civil Rights, and Immigration Law After September 11, 2001: The Targeting of Arabs and Muslims*, 58 N.Y.U. ANN. SURV. AM. L. 295, 296–97 (2002); Samuel R. Gross & Debra Livingston, *Racial Profiling Under Attack*, 102 COLUM. L. REV. 1413, 1413–14 (2002); Peter H. Schuck, *A Case for Profiling*, AM. LAW., Jan. 2002, at 59; Ronald J. Sievert, *Meeting the Twenty-first Century Terrorist Threat Within the Scope of Twentieth Century Constitutional Law*, 37 Hous. L. REV. 1421, 1450–56 (2000); Ryan L. Bangert, Comment, *When Airlines Profile Based on Race: Are Claims Brought Against Airlines Under State Anti-Discrimination Laws Preempted by the Airline Deregulation Act?*, 68 J. AIR L. & COM. 791, 817 (2003); Donna Smith, Comment, *Passenger Profiling: A Greater Terror Than Terrorism Itself?*, 32 J. MARSHALL L. REV. 167, 170 (1998).

194. See, e.g., John Rogers, Note, *Bombs, Borders, and Boarding: Combating International Terrorism at United States Airports and the Fourth Amendment*, 20 SUFFOLK TRANSNAT'L L. REV. 501, 511–12 (1997); Brett Andrew Skean, Comment, *The Fourth Amendment and the New Face of Terrorism: How September 11th Could Change the Way America Flies*, 22 N. ILL. U. L. REV. 567, 579 (2002).

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.”<sup>197</sup>

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.<sup>198</sup> 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”<sup>199</sup> is akin to “driving while black.”<sup>200</sup> Inflammatory remarks by politicians do not help: a

---

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.”).

198. See Volpp, *The Citizen and the Terrorist*, *supra* note 189, at 1598 (“Those who appear ‘Middle Eastern, Arab, or Muslim’ and who are formally citizens of the United States are now being thrust outside of the protective ambit of citizenship as identity.”); see also Muneer I. Ahmad, *A Rage Shared by Law: Post-September 11 Racial Violence as Crimes of Passion*, 92 CAL. L. REV. 1259 *passim* (2004) (discussing acts of violence against Arabs, Muslims, and South Asians and governmental profiling after September 11); Raquel Aldana-Pindell, *The 9/11 “National Security” Cases: Three Principles Guiding Judges’ Decision-Making*, 81 OR. L. REV. 985, 1032–33 (2002) (noting that in the course of the “domestic war on terrorism,” 3% of 1000 people detained—often as a result of racial, ethnic, or religious profiling—have been charged with terrorist acts or linked to al Qaeda); Adrienne Katherine Wing, *Civil Rights in the Post 9/11 World: Critical Race Praxis, Coalition Building, and the War on Terrorism*, 63 LA. L. REV. 717, 718 (2003) (discussing profiling, hate crimes, and detention directed at Arabs and Muslims after September 11).

199. See, e.g., *Mustafa v. City of Chicago*, 442 F.3d 544, 546–47 (7th Cir. 2006); Tracey Maclin, “Voluntary” Interviews and Airport Searches of Middle Eastern Men: The Fourth Amendment in a Time of Terror, 73 MISS. L.J. 471, 472–79 (2003); Dalia Hashad, *Stolen Freedoms: Arabs, Muslims, and South Asians in the Wake of Post 9/11 Backlash*, 81 DENV. U. L. REV. 735, 735 (2004); Michael J. Whidden, Note, *Unequal Justice: Arabs in America and United States Antiterrorism Legislation*, 69 FORDHAM L. REV. 2825, 2879–80 (2001); Ellen Baker, Comment, *Flying While Arab—Racial Profiling and Air Travel Security*, 67 J. AIR L. & COM. 1375, 1375–77 (2002); Charu A. Chandrasekhar, Note & Comment, *Flying While Brown: Federal Civil Rights Remedies to Post-9/11 Airline Racial Profiling of South Asians*, 10 ASIAN L.J. 215, 215–16 (2003).

200. See, e.g., David A. Harris, *The Stories, the Statistics, and the Law: Why “Driving While Black” Matters*, 84 MINN. L. REV. 265, 269 (1999); Lenese C. Herbert, *Bête Noire: How Race-Based Policing Threatens National Security*, 9 MICH. J. RACE & L. 149, 172 (2003); Floyd D. Weatherspoon, *Racial Profiling of African-American Males: Stopped, Searched, and Stripped of*

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.”<sup>201</sup> 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.<sup>202</sup>

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 imagineprecedented 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.<sup>203</sup> These questions are likely to endure as long as any terrorist threat to commercial aviation persists.

---

*Constitutional Protection*, 38 J. MARSHALL L. REV. 439, 440–42 (2004). The DOJ has stated that racial profiling

at its core concerns the invidious use of race or ethnicity as a criterion in conducting stops, searches and other law enforcement investigative procedures. It is premised on the erroneous assumption that any particular individual of one race or ethnicity is more likely to engage in misconduct than any particular individual of another race or ethnicity.

U.S. DEP’T OF JUSTICE, GUIDANCE REGARDING THE USE OF RACE BY FEDERAL LAW ENFORCEMENT AGENCIES (2003), [http://www.usdoj.gov/crt/split/documents/guidance\\_on\\_race.htm](http://www.usdoj.gov/crt/split/documents/guidance_on_race.htm); cf. Deborah A. Ramirez et al., *Defining Racial Profiling in a Post-September 11 World*, 40 AM. CRIM. L. REV. 1195, 1197 (2003) (noting that the use of racial profiling raises questions “as to whether law enforcement officials exercise their [discretionary powers] fairly and without discrimination”).

201. Dennis Camire, *Muslim Council Seeks Action Against Cooksey for Slur*, GANNETT NEWS SERV., Sept. 21, 2001.

202. See, e.g., R. Richard Banks, *Racial Profiling and Antiterrorism Efforts*, 89 CORNELL L. REV. 1201, 1203–04 (2004); Stephen J. Ellmann, *Racial Profiling and Terrorism*, 46 N.Y.L. SCH. L. REV. 675, 685–87 (2002–2003); David A. Harris, *Racial Profiling Revisited: “Just Common Sense” in the Fight Against Terror?*, CRIM. JUST., Summer 2002, at 36, 37 (2002); R. Spencer Macdonald, Note, *Rational Profiling in America’s Airports*, 17 BYU J. PUB. L. 113, 118–19 (2002); John Derbyshire, *In Defense of Racial Profiling*, NAT’L REV., Feb. 19, 2001, at 38.

203. See, e.g., Emanuel Gross, *The Struggle of a Democracy Against Terrorism—Protection of Human Rights: The Right to Privacy Versus the National Interest—The Proper Balance*, 37 CORNELL INT’L L.J. 27, 29–31 (2004).

### 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.<sup>204</sup> 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.<sup>205</sup> After September 11, Americans appeared to favor civil liberties over security in the abstract, rather than in actual situations.<sup>206</sup>

Like the concepts of liberty, privacy, and security themselves, society and its citizens are defined and moved by circumstance.<sup>207</sup> The national impulse to promote security over privacy and over personal rights has dissipated since September 11.<sup>208</sup> 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."<sup>209</sup> 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."<sup>210</sup> 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.<sup>211</sup> Indeed, a willingness to exchange civil liberties for security turns on trust and confidence in government.<sup>212</sup>

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.<sup>213</sup> 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.”<sup>214</sup> 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.<sup>215</sup>

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-

---

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).

212. Davis & Silver, *supra* note 12, at 30.

213. See, e.g., Rosa Ehrenreich, *Privacy and Power*, 89 GEO. L.J. 2047, 2047 (2001); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2381 (1996); Glenn Negley, *Philosophical Views on the Value of Privacy*, 31 LAW & CONTEMP. PROBS. 319, 319 (1966); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1170 (2000); Shaun B. Spencer, *Security vs. Privacy: Reframing the Debate*, 79 DENV. U. L. REV. 519, 554 (2002); Kimberly A. Horn, Note, *Privacy Versus Protection: Exploring the Boundaries of Electronic Surveillance in the Internet Age*, 29 FORDHAM URB. L.J. 2233, 2264–66 (2002).

214. Vincent, *supra* note 43, at 8.

215. Taipale, *supra* note 12, at 137–38 (footnotes omitted).

cerns, with less emphasis on individual self-policing and market-based mechanisms.”<sup>216</sup> 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.<sup>217</sup>

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.”<sup>218</sup> Whether data mining and airline passenger profiling constitutes a search under the Fourth Amendment remains an open question.<sup>219</sup> For now, controversial legislation like the PATRIOT Act<sup>220</sup> and abated or developing profiling systems like

216. James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 7 (2003).

217. Davis & Silver, *supra* note 12, at 32–33.

218. Ramasastry, *supra* note 56, at 763.

219. *See id.* at 763–64. *See generally* Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1185 (1997); Paul Schwartz, *Data Processing and Government Administration: The Failure of the American Legal Response to the Computer*, 43 HASTINGS L.J. 1321, 1345–47 (1992); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1151–56 (2002); Joseph T. Thai, *Is Data Mining Ever a Search Under Justice Stevens's Fourth Amendment?*, 74 FORDHAM L. REV. 1731, 1735 (2006); Kathleen A. Linert, Note, *Database Marketing and Personal Privacy in the Information Age*, 18 SUFFOLK TRANSNAT'L L. REV. 687, 693–95 (1995).

220. Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered sections of the U.S.C.). For more information on the PATRIOT Act, see, for example, Robert N. Davis, *Striking the Balance: National Security vs. Civil Liberties*, 29 BROOK J. INT'L L. 175, 176 (2003); Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 607–08 (2003); Peter G. Madrinan, Note, *Devil in the Details: Constitutional Problems Inherent in the Internet Surveillance Provisions of the USA Patriot Act of 2001*, 64 U. PITT. L. REV. 783, 790–96 (2003); John T. Soma et al., *Balance of Privacy vs. Security: A Historical Perspective of the USA PATRIOT Act*, 31 RUTGERS COMPUTER & TECH. L.J. 285 *passim* (2005); John W. Whitehead & Steven H. Aden, *Forfeiting “Enduring Freedom” for “Homeland Security”: A Constitutional Analysis of the USA Patriot Act and the Justice Department's Anti-Terrorism Initiatives*, 51 AM. U. L. REV. 1081 *passim* (2002); Michael F. Dowley, Note, *Government Surveillance Powers Under the USA PATRIOT Act: Is It Possible To Protect National Security and Privacy at the Same Time? A Constitutional Tug-of-War*, 36 SUFFOLK U. L. REV. 165 *passim* (2002); Jacob R. Lilly, Note, *National Security at What Price?: A Look into Civil Liberty Concerns in the Information Age Under the USA PATRIOT Act of 2001 and a Proposed Constitutional Test for Future Legislation*, 12 CORNELL J.L. & PUB. POL'Y 447 (2003); Michael T. McCarthy, Recent Developments, *USA Patriot Act*, 39 HARV. J. ON LEGIS. 435 *passim* (2002).



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.<sup>221</sup> "[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."<sup>222</sup> 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.<sup>223</sup> 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

---

221. See *supra* Part II. See generally S.K. GHOSH, AIRCRAFT HIJACKING AND THE DEVELOPING LAW 13 (1985) (stating that aircraft hijacking is often intended to gain "world-wide publicity"); NANCY DOUGLAS JOYNER, AERIAL HIJACKING AS AN INTERNATIONAL CRIME (1974) (noting that the international community recognizes the existence of threats to global air safety); EDWARD McWHINNEY, 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).

222. *Motivation and Aviation as a Terrorism Target*, *supra* note 139.

223. *In re Air Disaster at Lockerbie Scotland on Dec. 21, 1988*, 37 F.3d 804, 811 (2d Cir. 1994), *cert. denied sub nom.* Pan American World Airways, Inc. v. Pagnucco, 513 U.S. 1126 (1995); *Smith v. Socialist People's Libyan Arab Jamahiriya*, 886 F. Supp. 306, 308 (E.D.N.Y. 1995); Nancy Jean Strantz, *Aviation Security and Pan Am Flight 103: What Have We Learned?*, 56 J. AIR L. & COM. 413, 414–15 (1990); Aphrodite Thevos Tsairis, *International Terrorism: Prevention and Remedies: Lessons of Lockerbie*, 22 SYRACUSE J. INT'L L. & COM. 31, 31 (1996). A former Director of the Office of Policy and Planning for Civil Aviation Security at the Federal Aviation Administration found a disturbing irony in the fact that the bombing of Pan Am Flight 103 over Lockerbie, Scotland in 1988 did not catalyze significant upgrades to aviation security, but the TWA Flight 800 accident in 1996, an event unrelated to terrorism, did: "[S]everal other events had come together at about the same time [as TWA Flight 800] to enable this tidal change to occur. First, several major terrorist events within the United States [occurred], beginning in 1993. . . . [They] include[d] the World Trade Center bombing and the murders at the headquarters of the Central Intelligence Agency. . . . [They also included] the revelation in early 1995 of the plot . . . to destroy a large number of U.S. civil aircraft in Asia . . . ." Anthony Fainberg, *Aviation Security in the United States: Current and Future Trends*, 25 TRANSP. L.J. 195, 196–97 (1998).

behavioral change in the world that corresponds to desired political goals.”<sup>224</sup>

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.<sup>225</sup> These differences are not quaint cultural variations, but significant impediments to securing the airways between sovereign nations in a uniform way.<sup>226</sup>

Whereas Americans approach privacy as a safeguard of their liberty interests, Europeans conceptualize privacy as a basic human right ensuring personal dignity.<sup>227</sup> 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-

224. *Terrorist Motivation and Preferred Aviation Targets*, IBPPONLINE, Nov. 5, 2003, [http://security.pr.erau.edu/read.php?kind=html&article\\_volume=15&article\\_issue=10&article\\_title=Terrorist%20Motivation%20and%20Preferred%20Aviation%20Targets](http://security.pr.erau.edu/read.php?kind=html&article_volume=15&article_issue=10&article_title=Terrorist%20Motivation%20and%20Preferred%20Aviation%20Targets).

225. See, e.g., Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. 609 (2007); Edward C. Harris, *Personal Data Privacy Tradeoffs and How a Swedish Church Lady, Austrian Public Radio Employees, and Transatlantic Air Carriers Show That Europe Does Not Have the Answers*, 22 AM. U. INT'L L. REV. 745 (2007).

226. The International Civil Aviation Organization, an agency of the United Nations, has adopted three international multilateral conventions on aviation security: the Hague Convention, Convention for the Suppression of Unlawful Seizure of Aircraft, Dec. 16, 1970, 22 U.S.T. 1641, 860 U.N.T.S. 105 (entered into force Oct. 14, 1971); the Montreal Convention, Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, Sept. 23, 1971, 24 U.S.T. 565, 974 U.N.T.S. 177 (entered into force Jan. 26, 1973); and the Tokyo Convention, Convention on Offenses and Certain Other Acts Committed on Board Aircraft, Sept. 14, 1963, 20 U.S.T. 2941, 704 U.N.T.S. 221 (entered into force Dec. 4, 1969). See Dionigi (Dan) M. Fiorita, *Aviation Security: International Response*, 3 ALB. L.J. SCI. & TECH. 267, 281–93 (1993).

227. Jeffrey Rosen, *Continental Divide*, LEGAL AFF., Sept.–Oct. 2004, at 49 (“‘Why is it that French people won’t talk about their salaries but will take off their bikini tops? . . . Why is it that Americans comply with court discovery orders that open essentially all of their documents for inspection,’ but refuse to carry national identity cards?”) (quoting James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1160 (2004)); see also Ruwantis Abeyratne, *Attacks on America—Privacy Implications of Heightened Security Measures in the United States, Europe, and Canada*, 67 J. AIR L. & COM. 83, 91, 98–99 (2002); David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 J. MARSHALL J. COMPUTER & INFO. L. 1, 8–9, 108 (1999).

vacy are focused on personal liberty and the right to be free from state surveillance, a right threatened primarily by government intrusions into the home.<sup>228</sup>

“Europeans are also far more trusting of government, and willing to allow it to regulate personal choices in ways that Americans would find intolerable . . . .”<sup>229</sup> 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.<sup>230</sup> Additionally, overseas profiling systems detailed information such as whether a “traveler contribut[ed] to certain suspect charitable organizations.”<sup>231</sup> Meanwhile, since 2001 Schiphol Airport in Amsterdam has operated a system called “Privium.”<sup>232</sup> 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).<sup>233</sup> Ironically, what often is

[l]ost 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.*

230. E.g., Michael Satchell, *Everyone Empty Your Pockets?*, U.S. NEWS & WORLD REP., Apr. 1, 2002, at 18.

231. Armstrong & Pereira, *supra* note 144, at Al.

232. Nicola Clark, *EU Weighs Voluntary Plan To Speed Airport Check-ins*, INT’L HERALD TRIB., Aug. 19, 2006, at 6.

233. *Id.* Meanwhile, on June 18, 2007 Canada implemented “Passenger Protect,” an online system through 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 McClennan & 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.<sup>234</sup>

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.”<sup>235</sup> 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.<sup>236</sup> 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.<sup>237</sup> 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.*

236. Eric Lipton, *Officials Seek Broader Access to Airline Data*, N.Y. TIMES, Aug. 22, 2006, at A1.

237. Boggan, *supra* note 99. See generally Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 174 (1999) (examining the differences and conflicts between the European Union and the United States’ data protection policies); Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 BERKELY TECH. L.J. 461 (2000) (stating that the European Union will not transfer personal data to the United States because the United States does not meet the proper level of data protection); Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT’L L. 1 (2000) (discussing the current dispute between the United States and the European Union regarding the protection of data-privacy rights); Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445 (1995) (summarizing the development of the European Union’s directive regulating the processing of personal data and what the directive entails).

of E.U. law or withhold protected passenger information and be denied landing rights in the United States.<sup>238</sup> 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.”<sup>239</sup> 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.”<sup>240</sup> 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.<sup>241</sup>

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.<sup>242</sup> 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/

---

238. Boggan, *supra* note 99; see also Gehan Gunasekara, *The ‘Final’ Privacy Frontier? Regulating Trans-Border Data Flows*, 15 INT’L J.L. & INFO. TECH. 362, 364 (2007) (evaluating the scant value of “national safeguards and regimes for the protection of personal data or information about individuals . . . as technology allows the information to be whisked out of the jurisdiction at the proverbial click of a mouse”); Robert Block, *U.S. Reaches Tentative Deal with EU over Passenger Data*, WALL ST. J., Dec. 17, 2003, at D3 (“Washington required all airlines flying to the U.S. to provide passenger data within 15 minutes of departure and threatened fines of up to \$6,000 per passenger and the loss of landing rights for noncompliance.”); Kilroy, *supra* note 45; *supra* note 99 and accompanying text.

239. Paulina K. Dudzinski, Letter to the Editor, *Sharing Personal Data*, INT’L HERALD TRIB., Dec. 24, 2003, at 7; see also Audrey Hudson, *U.S. Data Collection Worries Europe; Airlines Caught in Legal Conflicts*, WASH. TIMES, Oct. 17, 2003, at A11 (“‘We understand the U.S.’s sovereign right to determine the conditions on which people enter the country, we understand the American reaction after September 11, but we need to find a solution to the privacy concerns raised because it puts us in a position that is at odds with our own privacy directive,’ [an unidentified E.U.] source said.”).

240. Frits Bolkestein, *Passenger Privacy and the War on Terror; Resisting U.S. Demands*, INT’L HERALD TRIB., Oct. 24, 2003, at 10.

241. See Tom Ramstack, *EU, U.S. Reach Deal on Air-Passenger Data*, WASH. TIMES, Dec. 17, 2003, at A06.

242. Joined Cases C-317/04 & C-318/04, *Parliament v. Council and Comm’n*, 2006 E.C.R. I-04721; John Ward Anderson & Keith L. Alexander, *Court Voids U.S.–Europe Passenger Agreement*, WASH. POST, May 31, 2006, at A11. See generally Allen Shoenberger, *Privacy Wars: EU Versus US: Scattered Skirmishes, Storm Clouds Ahead*, 17 IND. INT’L & COMP. L. REV. 355 (2007).

46, which governs processing operations concerning public security, defense, and State security.<sup>243</sup> 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.<sup>244</sup> 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.<sup>245</sup>

#### IV. CONCLUSION

The "freedom to travel throughout the United States has long been recognized as a basic right under the Constitution."<sup>246</sup> Airline travel in particular has become such a usual part of life that many Americans simply presume their freedom to it.<sup>247</sup> 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.<sup>248</sup> September 11 jolted the nation's focus from service to

---

243. See Joined Cases C-317/04 & C-318/04, *Parliament v. Council and Comm'n*, 2006 E.C.R. I-04721.

244. See, e.g., Jane Perlez, *U.S. Urges Deal on Passenger Data; Agreement with European Nations Expires at the End of July*, INT'L HERALD TRIB., May 14, 2007, at 3; Madhu Unnikrishnan, *TB Passenger Incident Fuels U.S.-EU Debate over PNR*, AVIATION DAILY, June 4, 2007, at 2.

245. In June 2007 the United States reached a provisional agreement with the European Union whereby it would be permitted to store nineteen (and not thirty-four) items of passenger name record data about air passengers on a government-operated database for a period of fifteen years for "scrutiny in serious crime and terrorism investigations." Jamie Smyth, *EU, US Agree Deal To Store Files on Air Passengers*, IRISH TIMES, June 29, 2007, at 12. However, in a July 11, 2007 resolution, the European Parliament stated that it "[s]trongly regrets the lack of democratic oversight of any kind" during negotiations and "[d]eplores . . . that EU citizens' PNR data are to be treated solely according to US law." European Parliament Resolution on the PNR Agreement with the United States, EUR. PARL. DOC. (EN 0278) (2007), available at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+MOTION+P6-RC-2007-0278+0+DOC+PDF+V0//EN>.

246. *United States v. Guest*, 383 U.S. 745, 758 (1966).

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.").

248. See, e.g., Timothy M. Ravich, *Re-Regulation and Airline Passengers' Rights*, 67 J. AIR L. & COM. 935, 942-46 (2002). For a discussion of airline passengers' rights initiatives overseas, see Jeffrey Goh, *Air Passenger Rights: The Third Way*, 8 CONSUMER L.J. 407 (2000). On February 14, 2007 nine crowded JetBlue Airways airplanes sat on the snow-covered tarmac of JFK International Airport for six to ten hours. See Editorial, *Making Amends; JetBlue Isn't the Only One Thinking About a 'Bill of Rights' for Airline Passengers*, WASH. POST, Feb. 21, 2007, at

security.<sup>249</sup>

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.<sup>250</sup> 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.<sup>251</sup> 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.”).

250. See, e.g., *Aviation Security: Urgent Issues Need To Be Addressed, Testimony Before the H. Subcomm. on Aviation, Comm. on Transp. and Infrastructure*, 104th Cong. 7–10 (1996) (statement of Keith O. Fultz, Assistant Comptroller General); John M. Doyle, ‘I’m Looking Through You’; *TSA Seeks Improved Screening Technologies To Identify Carry-on Explosives and Weapons*, AVIATION WK. & SPACE TECH., June 18, 2007, at 143; Steven A. Mirmina, *Aviation Safety and Security—Legal Developments*, 63 J. AIR L. & COM. 547, 547–53 (1998). Regrettably, there is ample evidence showing the failure of devices designed to find explosives and dangerous objects. See, e.g., *Fake Bomb Fools British Airport Security*, SEATTLE POST-INTELLIGENCER, July 2, 1990, at A2.

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.<sup>252</sup> However, “the ‘magic’ attributed to isolated technological fixes must be jettisoned in favor of systems perspectives including the human element.”<sup>253</sup> 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.<sup>254</sup> SmartCheck is a \$110,000 radiation-emitting, “backscatter” machine that “peeks underneath [airline] passengers’ clothing to search for guns, bombs or liquid explosives.”<sup>255</sup> While SmartCheck will screen only volunteers initially, the ACLU has objected that it effects a “virtual strip-search.”<sup>256</sup> Nevertheless, as one reporter noted, “[i]f passengers . . . who were asked to undergo body scans are an indication, security

---

J. Sniffen, *Airports Warned About Terror Dry Runs*, ASSOCIATED PRESS, July 25, 2007, WL 7/25/07 APWIRE 04:42:51.

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.shtm](http://www.tsa.gov/press/releases/2007/press_release_07202007.shtm). 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).

253. *Special Article: Outline on Status of Post-9/11 Aviation Security Initiatives, Part I*, IBPPONLINE, May 3, 2002, [http://security.pr.erau.edu/read.php?kind=html&article\\_volume=12&article\\_issue=16&article\\_title=Special%20Article%3A%20Outline%20on%20Status%20of%20Post-9%2F11%20Aviation%20Security%20Initiatives%2C%20Part%20I](http://security.pr.erau.edu/read.php?kind=html&article_volume=12&article_issue=16&article_title=Special%20Article%3A%20Outline%20on%20Status%20of%20Post-9%2F11%20Aviation%20Security%20Initiatives%2C%20Part%20I); see also *supra* note 28 and accompanying text.

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.”<sup>257</sup> 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.’”<sup>258</sup> 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.<sup>259</sup> 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.<sup>260</sup> 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.’”<sup>261</sup> 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.<sup>262</sup> Airline

---

257. Faye Bowers, *With Full-Body X-ray, a Closer Look at Air Travelers*, CHRISTIAN SCI. MONITOR, Feb. 26, 2007, at 2.

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#1>.

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).

261. Alan F. Westin, *Privacy in the Workplace: How Well Does American Law Reflect American Values?*, 72 CHI.-KENT L. REV. 271, 273 (1996).

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 that ‘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.