VIRGINIA JOURNAL OF LAW & TECHNOLOGY

FALL 2010 UNIVERSITY OF VIRGINIA VOL. 15, NO. 173

Failing to Secure the Skies: *Why America has Struggled to Protect Itself and How it Can Change*

IAN DAVID FISKE†

ABSTRACT

Since 9/11 America has become acutely aware of the security threat poised from the skies. The country has dedicated countless resources to defend against this threat. Yet nearly every year another terrorist successfully exploits American aviation security. This article identifies why these terrorists are successful by examining the past and present American civilian aviation anti-terrorism systems. An operational analysis reveals that the physical security measures have been successful and intelligence based measures have been largely ineffective. Moreover the intelligence based methods face stiff political and legal challenges, and even the most ambitious systems devised have not proven adequate. Yet a repeating pattern of trading physical security measures for intelligence based measures has existed since the first system's inception. Ultimately, this article shows how both operational results and the law suggest that the only way to prevent aviation terrorism in the near future is with stronger physical security measures.

† Ian David Fiske graduated from the University of Virginia School of Law in May of 2010. He received his M.A. in International Conflict Studies from the Department of War Studies at King's College London and his B.A. in Comparative Political Science from Queens College. He thanks Allison Weatherford and Mary Robinson for their editing and insightful comments on earlier versions of this article.

TABLE OF CONTENTS

I. INTRODUCTION

On December 25, 2009, Northwest Flight 253 from Amsterdam to Detroit began its initial descent.[1] A Nigerian national, Umar Farouk Abdulmutallab, rose from his seat and went to the bathroom for around 20 minutes.[2] He returned and covered himself with a blanket.[3] Suddenly, a loud popping was heard from Mr. Abdulmutallab's seat. Passengers spotted a fire consuming Mr. Abdulmutallab's legs and the plane's wall.[4] Yet Mr. Abdulmutallab sat quietly and pretended not to notice. The passengers suddenly realized that the man was, in fact, trying to destroy the plane, and in a daring rescue they overpowered Mr. Abdulmutallab and extinguished the flames.[5]

In the subsequent weeks, many disturbing facts were revealed about the attack. In perhaps the most spectacular intelligence breakdown since September 11, 2001, the American intelligence community had failed to communicate vital information about Mr. Abdulmutallab. The United Kingdom, his place of education, had denied him re-entry into the country in May 2009.[6] On November 11 of that year, British intelligence had sent the United States information that an "Umar Farouk" had vowed to wage *jihad*

[1] Andrew Johnson & Emily Dugan, *Wealthy, Quiet, Unassuming: the Christmas Day Bomb Suspect*, THE INDEPENDENT, Dec. 27, 2009, at Americas, *available at* http://www.independent.co.uk/news/world/americas/wealthy-quiet-unassuming-the-christmas-day-bomb-suspect-1851090.html; *see also How Nigerian Attempted to Blow up Plane in U.S.*, VANGUARD, Dec. 27, 2009, at Headlines, *available at* http://www.vanguardngr.com/2009/12/27/how-nigerian-attempted-to-blow-up-plane-in-us.

[2] Johnson & Dugan, *supra* note 1.

[3] *Id.*

[4] *Id.*

[5] Hagar Mizrahi, *Dutch Passenger Thwarted Terror Attack on Plane,* YNET NEWS, Dec. 27, 2009, *available at* http://www.ynetnews.com/articles/0,7340,L-3825447,00.html.

[6] Kevin Dowling, Chris Gourlay, Christina Lamb, Dan McDougall, Claire Newell, & Jon Ungoed-Thomas, *Umar Farouk Abdulmutallab: One Boy's Journey to Jihad*, THE SUNDAY TIMES, Jan. 3, 2010, *available at* http://www.timesonline.co.uk/tol/news/world/middle_east/article6974073.ece.

against the United States.[7] Eight days later on November 19, Mr. Abdulmutallab's own father had contacted CIA officials at the U.S. Embassy in Nigeria to warn of his son's extremist religious views and to provide them with information.[8] Though Mr. Abdulmutallab's name was eventually added to an intelligence database of suspected terrorists, it was placed at the lowest level in the system, three steps removed from the "watch lists."[9] Given the low priority attached to his profile, along with the intelligence breakdown that had already occurred, it is little surprise Mr. Abdulmutallab's American visa was not revoked.[10] He then successfully exploited this breakdown, leaving America's defense in the hands of the brave passengers onboard Northwest Flight 253. Stunningly, Secretary of the Department of Homeland Security Janet Napolitano would later announce on national television that "the system worked . . . and he was stopped before any damage could be done."[11]

This paper will review the American approach to aviation anti-terrorism systems (AATS) and argue that the best system is one based on physical security, not intelligence measures. The primary focus of this paper will be a historical analysis of AATS. This is not an examination of history for history's sake, but rather an attempt to understand what measures have worked, what measures have not worked, and why. This paper begins with an analysis of early AATS, reviewing their inception, their attributes, and their substantial flaws. It then discusses more recent AATS, including the system used today. The description of these systems assesses the legal and political pressures that helped shape them and their practical strengths and weaknesses. The next section examines how law clearly supports using a physical security-based AATS, but raises significant challenges to an intelligence-based AATS. The paper concludes by noting the disturbing trend in American history to favor unreliable but politically appealing intelligence-based AATS over effective traditional physical security-based AATS.

II. HISTORICAL PATTERNS

Though the United States is a relative newcomer in addressing the threat of terrorism, we have deployed AATS sufficiently to learn valuable lessons from our

---

[7] *Alleged Christmas Bomber Said to Flip on Cleric*, CBS News/KDKA Pittsburgh affiliate, Feb. 4, 2010, *available at* http://kdka.com/national/Umar.Farouk.Abdulmutallab.2.1471361.html.

[8] Dowling, *supra* note 6; Karen DeYoung & Michael Leahy, *Uninvestigated Terrorism Warning About Detroit Suspect Called Not Unusual,* WASH. POST, Dec. 28, 2009, at National Security News, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2009/12/27/AR2009122700279.html (though one U.S. official said the report was "very thin"); *Abdulmutallab Shocks Family, Friends*, CBS News/Associated Press, Dec. 28, 2009, at World, *available at* http://www.cbsnews.com/stories/2009/12/28/world/main6029782.shtml; *Father of Terror Suspect Reportedly Warned U.S. About Son*, Fox News, Dec. 26, 2009, at U.S., *available at* http://www.foxnews.com/us/2009/12/26/father-terror-suspect-reportedly-warned-son-1857952999/. While the information his father provided has not been revealed, it appears the information was distinct from thoughts on Umar Farouk's religious beliefs. Even basic facts identifying his son could have been critically important in preventing Umar Farouk Abdulmutallab from boarding Northwest Flight 253.

[9] *Father of Terror Suspect Reportedly Warned U.S. About Son*, *supra* note 8. This issue is explained in greater detail further in the paper.

[10] Dowling, *supra* note 6.

[11] Eileen Sullivan, *'The System Worked,' Napolitano Says; It Did? Americans Wonder*, Associated Press/CNSNews.com, Dec. 28, 2009, *available at* http://www.cnsnews.com/news/article/59044.

experience. But all too often Congress and the Presidency have chosen not to examine the past. Facing monumental political pressure after each terrorist attack, most political leaders have chosen to abandon each failed policy and start over from scratch. The following section illustrates how the American AATS of the past, when carefully examined, reveal a clear lesson for future AATS: relying on intelligence instead of physical security does not work.

A. Early Developments: 1958-1990

The first substantive Congressional action on airline anti-terrorism began with the Federal Aviation Act in 1958.[12] The Act's most significant achievement was the creation of the Federal Aviation Administration (FAA).[13] While various government entities previously provided some semblance of regulation,[14] the centralization of this authority was itself a security measure. In addition to establishing the FAA, the Act empowered it to set policies and regulations and to issue orders setting and enforcing airline safety regulations.[15] Most important for airline security, the FAA was granted the power to monitor and detect specific cargo and persons attempting to fly.[16] However, the FAA's inception and function were almost certainly far more concerned with regulating prices and routes than with terrorists.[17]

The FAA's focus was suddenly diverted in 1961. In May of that year, National Airlines Flight 337, en route from Marathon, Florida to Key West, Florida, was hijacked and diverted to Cuba.[18] It was the first hijacking of an American aircraft and ushered in a new era of American aviation security.[19] The remaining seven months of 1961 saw four additional hijackings of American aircraft.[20] Congress responded by federally criminalizing hijacking, and by increasing the penalties for hijacking to include capital punishment or twenty years of imprisonment.[21] The Sky Marshals Program was also instituted, training and placing U.S. Marshals on randomly-selected high-risk flights.[22]

---

[12] Federal Aviation Act of 1958, Pub. L. No. 85-726, 72 Stat. 731 (codified as amended at 49 U.S.C. § 40101 et seq. (2010)).

[13] 49 U.S.C. § 40113 (2006).

[14] *See* Federal Aviation Administration, *A Brief History of the FAA,* http://www.faa.gov/about/history/brief_history/ (last updated Feb. 1, 2010).

[15] James Fisher, *What Price Does Society Have to Pay for Security? A Look at the Aviation Watch Lists*, 44 WILLAMETTE L. REV. 573, 575 (2008) (describing the impact of the Act).

[16] *See* Yousri Omar, *Plane Harassment: The Transportation Security Administration's Indifference to the Constitution in Administering the Government's Watch Lists*, 12 WASH. & LEE J. CIVIL RTS. & SOC. JUST. 259, 267 (2006).

[17] *See* § 102, 72 Stat. at 740 (codified as amended at 49 U.S.C. § 40101 (2010)) (describing the policy intentions of the Act); John W. Gelder, Comment, *Air Law: The Federal Aviation Act of 1958*, 57 MICH. L. REV. 1214, 1214–15 (1959) (noting the reasons for creating the Act).

[18] JIN-TAI CHOI, AVIATION TERRORISM: HISTORICAL SURVEY, PERSPECTIVES AND RESPONSES 23 (1994).

[19] John Rogers, *Bombs, Borders, and Boarding: Combating International Terrorism at United States Airports and the Fourth Amendment*, 20 SUFFOLK TRANSNAT'L L. REV. 501, 504 (1997).

[20] CHOI, *supra* note 18, at 24.

[21] *See* Pub. L. No. 87-197, 75 Stat. 499 (codified as amended at 49 U.S.C. § 46502(a) (2010)).

[22] CHOI, *supra* note 18, at 31. While the project was cancelled in 1972 due to concerns of a high-altitude gun fight between the U.S. Marshals and terrorists, it was re-instituted in 1980. *Id.*; *see also* Rogers, *supra* note 19, at 507 n.34.

Including Air Marshals on those flights changed the nature of the hijacking "game," since hijackers could no longer assume they were the only armed passengers on the plane. As the Marshals were inconspicuous and randomly placed, no hijacker could ever be certain of the true risk of his operation. Though the legislation and Sky Marshals Program appeared to have an immediate impact, within seven years hijackings had hit new highs.[23] In 1968 alone, twenty-two hijackings of American aircrafts occurred.[24] In 1969, this number nearly doubled.[25]

Realizing the magnitude of the problem, the United States took action to combat the new threat.[26] Tactically, the most significant response to hijacking was the creation of a new FAA Task Force in 1968.[27] Comprised of representatives from the Department of Justice, Department of Commerce, and FAA, the Task Force proposed the country's first AATS.[28] At the system's macro level, airport terminals would post notices and advise the public to inform authorities of suspicious activity.[29] At the next level, airlines applied a behavioral profile to potential passengers at check-in counters.[30] The behavioral profile was the main thrust of the system; it compared behavior, background, and known travel history of potential passengers to the traits of previously apprehended hijackers.[31] As a final line of defense, the system used a magnetometer to test the passengers matching the hijacking profile for the presence of metal.[32] If a magnetometer was alerted and the passenger could not account for all metal found, U.S. Marshals and U.S. Customs Service agents questioned the passengers and searched their luggage and persons.[33]

Though it is impossible to determine how many hijackings were prevented by this early AATS, these measures were clearly insufficient as hijackings of American aircraft

---

[23] CHOI, *supra* note 18, at 24.

[24] *Id.*

[25] *Id.* For context, there were 151 hijackings worldwide during this time period. Brian Michael Jenkins, THE TERRORIST THREAT TO COMMERCIAL AVIATION 4 (1989), http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA228285.

[26] It had also taken some steps internationally over the years. *See* Tokyo Convention of 1963, Convention on Offenses and Certain Other Acts Committed on Board Aircraft, Sept. 14, 1963, 20 U.S.T. 2941, 704 U.N.T.S. 219; Hague Convention of 1970, Convention for the Suppression of Unlawful Seizure of Aircraft, Dec. 16, 1970, 22 U.S.T. 1641, 860 U.N.T.S. 105; Montreal Convention of 1971, 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; *see generally* Paul Stephen Dempsey, *Aviation Security: The Role of Law in the War Against Terrorism*, 41 COLUM. J. TRANSNAT'L. L. 649 (2003) (providing a thorough analysis and application of these treaties to AATS).

[27] *See* United States v. Davis, 482 F.2d 893, 898 (9th Cir. 1973) (detailing the Task Force's establishment); Gregory Schrorer, *Doomed to Repeat the Past: How the TSA is Picking Up Where the FAA Left Off*, 32 TRANSP. L. J. 73, 75–76 (2004); CHOI, *supra* note 18, at 30.

[28] *See* CHOI, *supra* note 18, at 30; Rogers, *supra* note 19, at 506. It also seems highly likely that the airlines worked with the task force, as the AATS could not have worked without airline implementation, and could not create such a nuanced profile without knowing what information the airlines possessed.

[29] Rogers, *supra* note 19, at 506 n.29.

[30] *Davis*, 482 F.2d at 898.

[31] CHOI, *supra* note 18, at 30; Rogers, *supra* note 19, at 506.

[32] *Davis*, 482 F.2d at 898.

[33] *Id.* at 899; 5 WAYNE LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT §10.6(a) (4th ed. 2009).

continued at an alarming rate.[34] Recognizing the vulnerability of the AATS, the FAA mandated universal screenings of passengers and luggage in late 1972.[35] In addition, Congress enacted the Anti-Hijacking Act of 1974 to implement anti-terrorism measures contained in international aviation agreements and to delegate full supervisory functions of airline security to the FAA.[36]

From even these early systems, a number of trends in the nature of airline security are clear. In both the initial (1968) and revised (1972) systems, intelligence and physical security were paired together. Yet from the very beginning, intelligence was given precedence over physical security measures. In the 1968 system, the approaches were facially balanced: two intelligence approaches (public announcements and behavioral profiling) and two physical security approaches (magnetometer scans and searches). Yet upon closer analysis, the effectiveness of the intelligence approach controlled and limited the application of the physical security approach. Only passengers that fit the hijacking profiles created by intelligence were passed through the magnetometer, and only those that triggered the magnetometer were searched.

The 1972 revisions saw marked improvements in physical security and a significant decrease in hijackings from 1973 through at least 1979.[37] Instead of relying on intelligence to determine which passengers to pass through the magnetometer, each passenger was scanned.[38] This improvement was important because it rejected the strict use of a rigid profile derived from previous attacks. While intelligence gathered from previous attacks was undoubtedly helpful, the first AATS' blind reliance on intelligence severely restricted physical security measures. Once the limitations of intelligence based profiling were acknowledged, universal scanning could be implemented and threats could be neutralized before they reached the skies.

Though the 1972 revisions proved effective, the 1980s witnessed serious changes in the nature of airplane hijackings.[39] First, the 1985 hijacking of the American aircraft Trans World Airline (TWA) Flight 847, departing from Greece, challenged the FAA because of the lack of jurisdiction over foreign airports.[40] Though Congress quickly passed the Foreign Airport Security Act to encourage the FAA to assist with foreign airport security standards, it lacked any enforcement powers.[41] Second, hijackers began using explosives undetectable by conventional magnetometers.[42] Following the

---

[34] Rogers, *supra* note 19, at 507 (noting that 125 cases occurred between 1968 and 1973). One likely problem with this system was its implementation, which was largely left to the airlines. As will be further discussed, commercial airlines, like any for-profit entity, have a greater interest in generating revenue than in providing security.

[35] *Davis*, 482 F.2d at 900–02. The policy evolved from a February 1972 rule issued by the FAA that required screening of all passengers and luggage by either behavioral profile, identification check, physical search or magnetometer. *Davis,* 482 F.2d at 900. In December 1972, the method of screening was restricted to a physical search of the luggage and magnetometer or physical search of the person. *Davis,* 482 F.2d at 902.

[36] AntiHijacking Act of 1974, Pub. L. No. 93-366, 88 Stat. 409 (1974).

[37] CHOI, *supra* note 18, at 24.

[38] *Davis*, 482 F.2d at 901–02 (9th Cir. 1973).

[39] Rogers, *supra* note 19, at 508.

[40] *Id.* at 507.

[41] Foreign Airport Security Act, Pub. L. No. 93-83, 99 Stat. 222 (1985).

[42] CHOI, *supra* note 18, at 34, 137. *See generally* Rogers, *supra* note 19, at 508 n.42 (providing a thorough collection and analysis of information on this issue).

Lockerbie Bombing in 1988, Congress enacted the Aviation Security Improvement Act of 1990 and President George H. W. Bush created a Commission on Aviation Security and Terrorism to assess airline security.[43] The new legislation called for the FAA to develop measures to detect explosives in airports.[44] But the Commission also found that the U.S. AATS was "seriously flawed," with commentaries on the Commission's report citing a "lack of coordination and communication between the State department, the FAA, and the American intelligence gathering community" that left significant vulnerabilities.[45] The Commission's analysis and conclusions reflect a forty-year pattern that the American AATS were flawed.

Both the Commission's findings and historical analysis reveal that the flaws were based principally in the intelligence based defenses. The early AATS would continue for another decade and the primary threats to the system would remain transnational jurisdictional issues and the adaptation of terrorist weaponry to evade the magnetometers. Though neither American intelligence nor physical security could truly solve the transnational jurisdictional issues arising in the mid-1980s, the Aviation Security Improvement Act of 1990 was meant to minimize security gaps by facilitating both intelligence sharing and physical security training for foreign airports.[46] Yet the Act did not clarify how the intelligence would be used. At the time, there were no watch lists to bar potential threats and few, if any, coordinated law-enforcement efforts. It was, in many respects, sharing intelligence for intelligence's sake. While the increased use of undetectable explosives highlighted a physical security flaw, the fault was not with physical security itself; the government was simply losing an arms race.[47] The tools were available, but they were not widely employed until the Aviation Security Improvement Act demanded their use.[48] Once applied, they worked remarkably well. Thus, while both intelligence and physical security were used in the early anti-terrorist systems, a trend is clear. When more resources and flexibility are devoted to physical security, the system works. When physical security is restricted or otherwise supplanted by intelligence, the system fails.

---

[43] Aviation Security Improvement Act of 1990, Pub. L. No. 101-604, 104 Stat. 3066 (1990); Exec. Order No. 12,686, 54 Fed. Reg. 32,629 (Aug. 9, 1989).

[44] §§ 103, 107, 104 Stat. at 3069, 3076.

[45] Report to the President by the President's Comm'n on Aviation Security and Terrorism, I (May 15, 1990) (noting the American AATS was "seriously flawed"); Nancy Jean Strantz, *Aviation Security and Pan Am Flight 103: What Have We Learned?*, 56 J. AIR L. & COM. 413, 464 (1990). *See generally* 136 CONG. REC. S6270 (May 15, 1990) (statement of Sen. Lautenberg, member of the Commission on Aviation Security and Terrorism, concerning the Findings and Recommendations of the Commission); 136 CONG. REC. S9172 (Jun. 28, 1990) (statement of Sen. Lautenberg, introducing the Aviation Security Improvement Act of 1990, noting that "virtually every link" in the system was weak). In hindsight, the Commission's report was chilling: the report fell on deaf ears; just fifteen years later, the 9/11 Commission would repeat the same message. Nat'l Comm'n on Terrorist Attacks Upon the U.S., The 9/11 Commission Report, xvi (2004) [hereinafter 9/11 Commission Report]. *See also* Omar, *supra* note 16, at 269.

[46] § 2, 104 Stat. at 3066–67.

[47] 136 CONG. REC. S9172 ("We need a more focused and higher profile research and development program. We can't continue to allow third world terrorists to have the technological edge on us.").

[48] Act of July 5, 1994, Pub. L. No. 103-272, § 44912, 108 Stat. 745, 1212–13 (codified as amended at 49 U.S.C. § 44912(a)(1) (2010)) (requiring the Under Secretary of Transportation for Security to "accelerate and expand" the application of technologies to combat terrorist efforts).

B. Modern AATS

The modern era of airline anti-terrorism measures began in the late 1990s. Following the puzzling in-flight explosion of TWA Flight 800 and a continued threat of terrorist attack, President Clinton created the White House Commission on Aviation Safety and Security.[49] A direct result of the Commission's recommendations was the creation of an automated profiling system to screen potential passengers.[50] This program, the Computer Assisted Passenger Pre-Screening System (CAPPS), became the keystone of the modern American AATS.

1. CAPPS I (1998 - ~2002)

The first CAPPS (CAPPS I) was applied in 1998 and operated at three levels.[51] The program began by identifying prospective passengers with certain suspicious "characteristics."[52] While the roughly forty characteristics have been kept secret, they are thought to have included passenger behavior in the airport, travel history, "the passenger's address, method of ticket purchase, travel companions, rental status, ticket purchase date, departure date, destination, origin," and round trip or one-way status.[53] In addition to the characteristics analysis, a watch list of the names of known terrorist threats was cross-checked against the names of potential passengers.[54] Finally, individuals were selected at random from the group of "cleared" passengers to be given higher scrutiny.[55]

The use of computers in applying CAPPS I was a great improvement in the AATS. It also raised the stakes for the intelligence approach in significant ways, however, as the characteristics analysis and the watch lists relied almost solely on intelligence. This amplified the effect of intelligence errors, leading to significant security flaws. First, because of concerns about intelligence being exposed or abused, significant barriers were erected that kept the system from being used to its fullest potential. The system was initially applied to airlines on a purely voluntary basis.[56] Though it would eventually become mandatory, CAPPS I would always be independently

---

[49] Fisher, *supra* note 15, at 576.

[50] *Id.*; WHITE HOUSE COMM'N ON AVIATION SAFETY AND SECURITY, FINAL REPORT TO PRESIDENT CLINTON 3.19 (Feb. 12, 1997), *available at* http://www.fas.org/irp/threat/212fin~1.html.

[51] Fisher, *supra* note 15, at 577.

[52] United States Government Accountability Office, Report to Congressional Committees, *Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should be Managed as System is Further Developed* (GAO-05-356), Mar. 2005, 1 [hereinafter GAO I] (applying "data related to a passenger's reservation and travel itinerary…against characteristics used to select" individuals who posed threats).

[53] Fisher, *supra* note 15, at 576; Stephen W. Dummer, *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, 588 (2006).

[54] Fisher, *supra* note 15, at 577.

[55] Mardi Ruth Thompson, *Providing Smarter Security and Customer Service: TSA's Secure Flight and Registered Traveler Programs*, 19-SPG AIR & SPACE LAW. 8 (2005).

[56] Dummer, *supra* note 53, at 588.

applied and funded by each airline.[57] This was problematic for multiple reasons. The primary purpose of commercial airlines, like that of most private entities, is to create profits. The responsibility of providing security lies primarily with the state. Airlines had a strong incentive to provide the most minimal security possible.[58] While customers required a certain threshold level of security, it made no sense from a profit standpoint to spend money to move beyond this threshold.[59] Because no two airlines were likely to establish identical threshold security levels,[60] this probably led to uneven implementation, meaning that "borderline" individuals could likely fly on some airlines even when blocked by others.[61] Additionally, as CAPPS I was designed by Northwest Airlines (in conjunction with the U.S. government), that company had a stronger incentive than its competitors did to ensure the system worked.[62] Finally, placing the system within each airline made updating information a tedious and monumental task.[63] Slow updates to the CAPPS I database weakened security.[64] These airlines performed this task with strict barriers erected to prevent information sharing between airlines and foreign intelligence services, all leading to considerable limitations in using this system.[65]

Second, the system was heavily dependent upon the passenger providing his or her true name, legitimate identification, and travel receipts.[66] This practice was dangerous due to the proliferation of fake identification cards and the myriad reasons

[57] Thompson, *supra* note 55, at 8–9.

[58] Fisher, *supra* note 15, at 575 (describing the effect and motivations of airlines having control over implementing security features).

[59] This point is made clear by the decision under CAPPS II to have the government pay for the system. GAO I, *supra* note 52, at 9. This problem was likely at issue in allowing the failed New York City bomber, Faisal Shahzad, to board an Emirates Airline flight. Despite having his name on the No-Fly list, he was allowed to both purchase and board the aircraft. Eileen Sullivan & Matt Apuzzo, *Security Slip Let Suspect on Plane, Near Takeoff*, Associated Press, May 4, 2010, *available at* http://www.huffingtonpost.com/2010/05/04/faisal-shahzad-gained-cit_n_562837.html [hereinafter Sullivan I].

[60] This is true for both establishing the threshold levels of security and for the method in which they are applied. While customers may usually demand a minimum level of security in order to use a company's business, they may be willing to relax their standards for price, service, or convenience. A recent example includes plans by the european low-budget airline RyanAir to use standing-room seats despite safety concerns. Laura Roberts, *RyanAir to Sell £5 Tickets for Standing-Room Only Flights,* THE TELEGRAPH, July 1, 2010, *available at* http://www.telegraph.co.uk/travel/travelnews/7864921/Ryanair-to-sell-5-tickets-for-standing-room-only-flights.html. Even assuming passengers would not compromise security standards, businesses, as previously discussed, have the incentive to achieve minimum security at the lowest possible cost. These airlines may determine that threshold level lies at different points without communicating these differences to customers.

[61] *See* Thompson, *supra* note 55, at 9 (noting there were inconsistencies among the airline applications).

[62] Dummer, *supra* note 53, at 587–88 (noting that the system was built by Northwest in conjunction with the FAA).

[63] *See* Fisher, *supra* note 15, at 579 (noting the benefits of governmental implementation and the expectation of updating becoming "more effective and efficient"). Additionally, continuously adding data to a never ending database might make some airlines question the utility of the exercise.

[64] *Id.*

[65] GAO I, *supra* note 52, at 2 (describing the 9/11 Commission highlighting that there was concern over sharing the intelligence with firms and other countries).

[66] Thompson, *supra* note 55, at 8.

why passengers might want to conceal their information.[67] The methods of using fake identification vary widely and include purchasing counterfeit identification cards, altering valid identification cards, and using the identification of another person with similar facial features.[68] Placing so much reliance on passenger self-identification therefore left a serious breach in CAPPS I.

Third, within one year CAPPS I was restricted to screening checked luggage.[69] While the program was originally applied to searching passengers, carry-on luggage, and checked luggage, the White House Commission on Aviation Safety and Security felt increasing pressure from the public to restrict its searches.[70] The result was a severe limitation on any effectiveness that CAPPS I could provide. Even if CAPPS I could detect the passengers posing a higher risk despite problems with intelligence, the restricted system could not keep hijackers from boarding with undetected weapons on their persons.

2. CAPPS II (~2002 – 2004)

The 9/11 attacks tragically illustrated the flaws in CAPPS I, leaving the nation stunned. As Congress re-grouped and re-focused in the subsequent weeks, it acknowledged that a stronger and more comprehensive anti-terrorist system was needed. It quickly passed the Aviation and Transportation Security Act (ATSA) to solve this problem.[71] The ATSA performed two significant functions. First, it established a new body, the Transportation Security Administration (TSA), to control most aspects of civil aviation security.[72] Second, it called for an improved version of CAPPS I to become operational in all domestic airports and in all foreign airports that provide flights to America.[73] This TSA program would become the second-generation computer assisted passenger prescreening system, known as CAPPS II.[74]

CAPPS II was designed "to screen all passengers flying into, out of, and within the United States."[75] Like CAPPS I, the system began by screening potential passengers

---

[67] There are many reasons why a passenger may want to travel under a fake name, ranging from keeping celebrity travel anonymous, to hiding an extra-marital affair, to concealing terrorist activity.

[68] While it is true that airport security may be taught to recognize falsified identification, such training would not help catch a passenger using another person's authentic, valid identification. For a recognition of this problem and attempts to solve it, see Intelligence Reform and Terrorist Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638, 3816, 3830 (2004) [hereinafter IRTPA].

[69] Michael J. DeGrave, *Airline Passenger Profiling and the Fourth Amendment: Will CAPPS II be Cleared for Takeoff?*, 10 B. U. J. SCI. & TECH. L. 125, 130 (2004); Fisher, *supra* note 15, at 579.

[70] DeGrave, *supra* note 69, at 130 (noting that the pressure came from the public and that the government had used similar programs to search for drug couriers); Fisher, *supra* note 15, at 579 (noting it was for civil liberties concerns). Interestingly, people seem much more tolerant now, which may be because they feel threatened. In an amazing policy shift from both the original 1968 program and the CAPPS I improvements, it is very possible the public pressure may have come from the perception that the intent of the program was not counter-terrorism, but counter-narcotics. It is debatable what initiated this short-sighted change in policy. Though conventional wisdom would advise that it was an overreach of 4th Amendment concerns, the fear of airline abuse of intelligence was clearly documented above. It is therefore more likely just another step in the concern over of the use of intelligence.

[71] Aviation and Transportation Security Act, Pub. L. No. 107-71, 115 Stat. 597 (2001).

[72] § 101, 115 Stat. at 597–602 (codified as amended at 49 U.S.C. § 114 (2010)).

[73] Dummer, *supra* note 53, at 588.

[74] GAO I, *supra* note 52, at 9.

[75] *Id*.

for certain characteristics.[76] But while CAPPS I identified roughly forty characteristics, gathered its data from a single airline, and separated passengers into high- and low-risk categories, CAPPS II provided much greater latitude. It collected information on a greater number of characteristics from government and commercial databases.[77] This passenger data was applied to algorithms to produce multiple-dimensional profiles likely used to determine if a person was an "acceptable risk, unknown risk, or unacceptable risk."[78]

CAPPS II also boasted a number of expanded list-comparison capabilities. Like CAPPS I, CAPPS II compared the records of passengers' names (PNR) to the names of known terrorist threats.[79] But these "threats" were expanded to include people who could fly subject to extra screening (the "Selectee" list) as well as those barred from flying (the "No-Fly" list).[80] The PNR would also be checked against domestic and international criminal "wanted lists."[81] Temporary watch lists could also be created and implemented as determined by information produced by real-time intelligence reports.[82] To streamline all of these efforts, passengers who were cleared by the programs could be put on a list of individuals requiring less screening, thereby reducing the travel time and hassle for those passengers and focusing resources on screening more suspicious passengers.[83]

CAPPS II also solved other key flaws of CAPPS I. First, while CAPPS I was paid for and run by airlines, CAPPS II would be paid for and run by the government.[84] This single change removed the airlines' conflict of interest previously described and made the program simpler to update to respond to new security threats.[85] Second, while CAPPS I heavily relied on the information provided by passengers, CAPPS II used commercial data providers to confirm the passengers' identities.[86] These modifications closed two of the greatest security gaps in CAPPS I.[87]

But despite its improvements over CAPPS I, CAPPS II was never implemented.[88] While CAPPS I suffered from security flaws, CAPPS II suffered from legal and political challenges.[89] Citizens from across the political spectrum acknowledged the need for a

---

[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Id.* at 10.
[80] *Id.* at 13.
[81] *Id.* at 10.
[82] *Id.*
[83] *Id.* Congress also called on the Secretary of Homeland Security to work with foreign countries to make name translations more unitary. IRTPA, 118 Stat. 3638, 3819.
[84] GAO I, *supra* note 52, at 9.
[85] Fisher, *supra* note 15, at 579.
[86] GAO I, *supra* note 52, at 10; Omar, *supra* note 16, at 272 (indicating that passenger information would be sent to providers, who would then assign a numerical probability score to each passenger).
[87] Additionally, one final element to the CAPPS II program exists, but it qualifies as Sensitive Security Information and its value is therefore unknown. GAO I, *supra* note 52, at 9.
[88] Though CAPPS II was never implemented, it was tested using both fictional and actual PNR data. *See generally* Ryan Singel, *Data Disclosure Contradicts Feds*, WIRED NEWS, Apr. 12, 2004, http://www.wired.com/politics/security/news/2004/04/63025; Sara Kehaulani Goo, *Agency Got More Airline Records: Privacy Advocates Fear Extensive Transfer of Passenger Data*, The WASH. POST, June 24, 2004, A16.
[89] A credible argument can be made that many of CAPPS I's security flaws were also the result of legal and political challenges. The curtailing of the searches under CAPPS I was due to privacy concerns. By

better system, but attacked CAPPS II for the intrusive nature of its intelligence collection, the methods by which its information would be used, and the lack of a redress policy to help misidentified citizens.[90] Many rooted their concerns in the Fourth Amendment, Fifth Amendment, and in the Privacy Act, though their arguments were more political than legal.[91] Members of Congress eventually came to share these concerns and to argue that the Department of Homeland Security (DHS) should have oversight over the TSA. In the October 2003 Department of Homeland Security Appropriations Act, Congress ordered the TSA to address eight concerns about CAPPS II, specifically regarding the lack of a process to appeal the TSA's designation as a threat, the absence of internal quality control, the fact that the DHS had no oversight over the TSA's program, and legal questions about personal privacy.[92] Despite Congressional orders, when the General Accounting Office published its report on CAPPS II in February 2004, only one of the eight identified concerns had been addressed.[93] Faced with these failings and mounting criticism, the TSA cancelled the program in August 2004.[94]

The rejection of CAPPS II signaled what the American public and Congress considered to be an overreach of intelligence. As previously described, the CAPPS II system was based on an expansive new intelligence regime. Its system would have gathered highly detailed information, attempted to confirm identification with commercially-available data, and matched credible information against watch lists created from other sources of intelligence. It clearly corrected some of CAPPS I's major security defects. Yet there is serious doubt over how effective CAPPS II would have been in practice. Verifying passenger identity through commercial databases could not catch all instances of identity theft and purchasing fake identities.[95] Of greater concern is the tension between creating a database selective enough to prevent "False Positives" (improperly including non-threatening individuals) yet encompassing enough to prevent "False Negatives" (failing to include individuals who are dangerous).[96] Because missing

---

restricting searches only to certain customers, and then later to only their luggage, CAPPS I left gaping holes in security. But independent airline application and reliance on self-identification, two of CAPPS I's biggest flaws, were inherent from the program's inception.

[90] *See* American Civil Liberties Union, *The Five Problems with CAPPS II*, Aug. 25, 2003, http://www.aclu.org/national-security/five-problems-capps-ii [hereafter ACLU]; Kelley B. Vlahos, *Massive Travel Database Raises Eyebrows*, **FOXNEWS.COM**, Jan. 28, 2004, http://www.foxnews.com/story/0,2933,109675,00.html (noting statements from former Republican Congressman Robert Barr and Chuck Pena of the libertarian CATO Institute).

[91] *See* DeGrave, *supra* note 69, at 131 (citing arguments over search and seizure); Ryan Singel, *Life After Death for CAPPS II?*, WIRED NEWS, July 16, 2004, http://www.wired.com/politics/security/news/2004/07/64240 (statement by Sen. Collins that she is concerned about the "letter and the spirit" of the Privacy Act); ACLU, *supra* note 90 (criticizing the lack of procedural due process).

[92] Department of Homeland Security Appropriations Act, Pub. L. No. 108-90, § 519, 117 Stat. 1137, 1155–56 (2003); Fisher, *supra* note 15, at 579.

[93] Government Accountability Office, Report to Congressional Committees, *Aviation Security: Computer-Assisted Passenger Prescreening Faces Significant Implementation Challenges*, GAO-04-385, Feb. 4, 2004, *available at* http://www.gao.gov/new.items/d04385.pdf [hereinafter GAO II]. *See* Omar, *supra* note 16, at 272 for a good analysis of this problem.

[94] GAO I, *supra* note 52, at 11.

[95] *See* ACLU, *supra* note 90.

[96] *See* Daniel J. Steinbock, *Designating the Dangerous: From Blacklists to Watch Lists*, 30 SEATTLE U. L. REV. 65, 95-8 (2006) (noting that the current watch list program at that time was running into these

a single name could allow a terrorist attack, the false negative rate would need to be reduced to zero to properly rely on the system.[97] Creating such a database would almost certainly require more intrusiveness than was intended under CAPPS II. Therefore, if an intelligence-based AATS is to succeed, it needs access to an even greater amount of information than that allowed under CAPPS II, and certainly no further restrictions. Yet it is clear that CAPPS II, unlikely to be highly effective, was already too intrusive for the American public and Congress. CAPPS II's rejection is strong evidence that an intelligence-based AATS will not work in the near future.

3. CAPPS IE and Secure Flight (2004 - Present)

After the TSA cancelled CAPPS II, it created an enhanced form of CAPPS I ("CAPPS IE"). Like CAPPS I, CAPPS IE offered a characteristics analysis, comparing roughly forty pieces of data supplied by passengers to terrorist characteristics criteria.[98] Also like CAPPS I, individuals were randomly selected and the names of passengers were compared to watch lists.[99] However, CAPPS IE's watch lists were more comparable to those proposed in CAPPS II, dividing passengers into the "no-fly" and "selectee" lists previously described.[100] To solve the redress problem of CAPPS II, CAPPS IE allowed mistakenly "flagged" passengers to undergo an extensive identification process to become "cleared."[101]

CAPPS IE also corrected some of the flaws of CAPPS I; the government maintained its watch lists, and all passengers and baggage were subject to search.[102] The program initially shared a major weakness of CAPPS I, as airlines controlled its application and enforcement.[103] But this was soon corrected after Congress received a report from the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission Report) and directed the TSA to take control of CAPPS IE's implementation in the Intelligence Reform and Terrorism Prevention Act (IRTPA) in December 2004.[104] Concurrently, the IRTPA challenged the TSA to create a new anti-terrorism passenger screening system to replace CAPPS altogether.[105] The TSA responded by creating "Secure Flight," the system used today on every commercial flight involving U.S. airspace.[106]

Secure Flight acts as a coordinated effort to combine many of the security measures of CAPPS IE, CAPPS II, and the 9/11 Commission's recommendations with a

---

problems). Today, the case of Najlah (Mikey) Feanny Hicks, an 8 year old boy on the Selectee List, illustrates the accuracy problems involved with using these lists. Lizette Alvarez, *Meet Mikey, 8: U.S. Has Him on Watch List*, N.Y. TIMES, Jan. 13, 2010, at A1.

[97] *See* Steinbock, *supra* note 96, at 98.

[98] GAO I, *supra* note 52, at 8.

[99] *Id.* at 8–9 (detailing the watch lists).

[100] *Id.*

[101] Thompson, *supra* note 55, at 8–9.

[102] GAO I, *supra* note 52, at 8–9. However, the search of passengers, carry-on, and checked baggage had been re-instituted soon after 9/11. Fisher, *supra* note 15, at 578.

[103] GAO I, *supra* note 52, at 8.

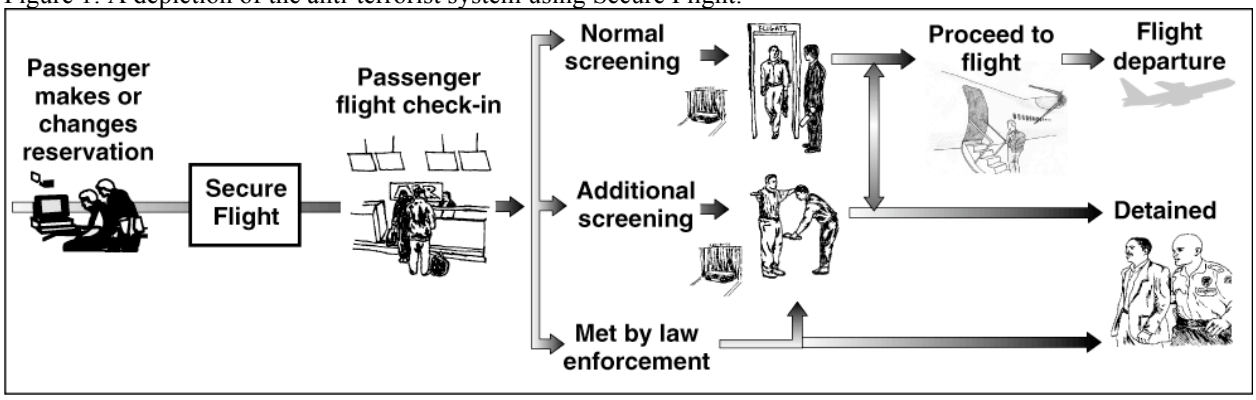
[104] *See* 9/11 Commission Report, *supra* note 45, at 392–93; Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 4012(a)(1), 118 Stat. 3638, 3714–15 (Dec. 17, 2004).

[105] Thompson, *supra* note 55, at 9.

[106] Transportation Security Administration, *Security Programs: Secure Flight Program,* http://www.tsa.gov/what_we_do/layers/secureflight/ (updated Nov. 1, 2010).

stronger oversight regime.[107] Its goals are to streamline screening, to have a more limited identity verification process, to use watch lists effectively, and to provide credible due process redress for mistakenly flagged passengers.[108] Secure Flight has the TSA analyze the passenger characteristics under the same rules and profiles used in CAPPS I.[109] It screens the register of passenger names for names on the "No-Fly" and "Selectee" lists.[110] But unlike CAPPS I, Secure Flight may also use other watch lists provided by the Terrorist Screening Center.[111] The TSA is exploring the use of commercial databases to verify information, though it is unclear if this measure is in operation today.[112] The TSA does not intend to use lists of criminals or to gather intelligence as proposed under CAPPS II.[113] All PNR will be submitted to the TSA approximately seventy-two hours prior to flight, or as soon as a reservation is made if the transaction occurs less than seventy-two hours before take-off.[114] PNR data is generally destroyed within the next seventy-two hours, unless a passenger complains that he or she was wrongfully flagged.[115] Secure Flight began screening all commercial domestic flights in August 2009 and all international departures, arrivals, and over-flights of the continental U.S. in October 2009.[116] A depiction of Secure Flight's implementation into airport security can be seen below.

Figure 1: A depiction of the anti-terrorist system using Secure Flight.[117]



Source: GAO analysis of TSA data.

Like CAPPS II, Secure Flight suffers from an over-reliance on intelligence, applying profiles based on algorithms and databases. Yet it uses substantially less collection and

[107] *See id.*; WILLIAM J. KROUSE & BART ELIAS, TERRORIST WATCHLIST CHECKS AND AIR PASSENGER PRESCREENING 16 (Congressional Research Service Dec. 30, 2009). Indeed, to some degree the abolishment of CAPPS II and the development of Secure Flight may be more political than practical.

[108] KROUSE, *supra* note 107, at 15–16.

[109] GAO I, *supra* note 52, at 11.

[110] *Id.* at 13.

[111] *Id.* at 12–13. The Terrorist Screening Center is "an interagency effort involving DHS, Department of Justice, Department of State, and intelligence community representatives, and is administered by the Federal Bureau of Investigation." *Id.* at 3 n.5.

[112] *Id.* at 12 (as of March 2005).

[113] *Id.*

[114] *Id.* at 13.

[115] *Id.* at 16.

[116] KROUSE, *supra* note 107, at 17–18; Transportation Security Administration, *supra* note 106.

[117] *See* GAO II, *supra* note 93, at 8.

analysis than what was allowed in CAPPS II. The TSA may not collect additional data about potential threats, and does not appear to be consulting commercial databases. The destruction of PNR data within seventy-two hours of flights prohibits any meaningful tracking of suspicious individuals. As described above, there were serious questions about CAPPS II's ability to adequately detect threats despite access to more information. Secure Flight, working with less information, has even less probability of identifying threats.

Recent revelations about the construction and use of the watch lists are cause for even greater security concerns. After intelligence is collected and analyzed by intelligence producers, the intelligence is then processed by two entities: the National Counterterrorism Center and the Federal Bureau of Investigation.[118] Those agencies then input select information from their intelligence reports into the Terrorist Screening Database (TSDB) for further processing.[119] The Terrorist Screening Center (TSC) mines the TSDB for information it deems important for the TSA.[120] The TSA then reviews the TSC's report for any names it wants to include on the "No-Fly" or "Selectee" lists.[121] In short, the TSA's "No-Fly" and "Selectee" lists are nothing more than heavily-processed subsets of the TSDB.[122]

The Secure Flight system depends completely on the quality of intelligence gathering, analysis, and communication at every step described above. It demands and presumes the effective and timely transfer of information about terrorist threats.[123] The system also requires that each bureaucratic layer of review find the threats credible and determinable, awarding every entity the opportunity to reject the inclusion of a name. For a Congress and public concerned with preventing excessive government intrusion, this process is an achievement. But its success requires four separate entities to operate without "false negatives." If an individual is a threat, and even one of the levels does not recognize this—or mishandles the information—the system fails. More than likely, the TSA will never know that the individual even existed until it is too late: the terrorist's identity is statistically more likely to be purged at one of the first three levels of review than a single review, and any previous PNR information is destroyed after seventy-two hours.

Even the application of Secure Flight information has been a point of weakness. Prior to late 2010, airlines still checked international flight PNR against "No-Fly" and "Selectee" lists, as under CAPPS I; the TSA relied on these private companies to secure the skies.[124] As already discussed, this is highly problematic because updating

---

[118] United States Department of Justice, Office of Inspector General, Audit Division, *Follow-up Audit of the Terrorist Screening Center* (Audit Report-07-41), Sep. 2007, iv, v, available at http://www.justice.gov/oig/reports/FBI/a0741/final.pdf (redacted for public release).

[119] *Id.*

[120] KROUSE, *supra* note 107, at 19; Mike McIntire, *Ensnared by Error on Growing U.S. Watch List, With No Way Out*, N.Y. TIMES, Apr. 7, 2010, at A1.

[121] KROUSE, *supra* note 107, at 19; McIntire, *supra* note 120.

[122] KROUSE, *supra* note 107, at 4 (admitting that they are "in some cases only subsets"). Yet the process described on page 19 of this report reveals they are entirely "subsets," not just "in some cases."

[123] *See* Frederick P. Hitz, WHY SPY? ESPIONAGE IN AN AGE OF UNCERTAINTY 19 (St. Martins 2008) ("If intelligence and domestic security are in a preemptive and preventative mode, they will need accurate and timely intelligence about future attacks before they occur . . . .").

[124] MARK A. RANDOL, THE DEPARTMENT OF HOMELAND SECURITY INTELLIGENCE ENTERPRISE: OPERATIONAL OVERVIEW AND OVERSIGHT CHALLENGES FOR CONGRESS, 41 (Congressional Research

information becomes a tedious and monumental task, and because the slower the updates, the weaker the system. Demonstrating this flaw, on May 3, 2010, attempted New York City bomber Faisal Shahzad was able to purchase a plane ticket, in cash, from New York City to the United Arab Emirates, despite being on the "No-Fly" list.[125] Mr. Shahzad was not only allowed to pass through TSA security and Customs and Immigration, but was sitting in his seat when the cabin door was closed.[126] Though airlines were subsequently required to compare PNR to lists within two hours of list updates,[127] relying on airlines to perform this function still left unchecked the conflict of profit versus security.

The repeated failures of an intelligence-based AATS provide tremendously strong reasons to believe Secure Flight will fail again. President George H. W. Bush's Commission in 1990 identified a lack of communication between intelligence agencies about potential threats.[128] That problem had not been fixed by the terrorist attacks of 2001, or by 2004 when the 9/11 Commission issued its report.[129] On Christmas Day, 2009, this flaw was illustrated and exploited by Umar Farouk Abdulmutallab, who attempted to destroy his plane before fellow passengers subdued him. And as noted in the last paragraph, on May 3, 2010, Faisal Shahzad was allowed to purchase a ticket and board a plane, despite being on the "No-Fly" list.[130] A message spanning across five decades, verbalized twice by presidential commissions, and illustrated on multiple occasions is perfectly clear: an AATS based on intelligence instead of on physical security does not work.

III. LEGAL PRESSURES

Given the historical and intrinsic failures of an intelligence-based AATS, it follows that a more physical security-oriented approach must be taken to successfully fight terrorism in the skies. Law provides support for this shift. The following discussion illustrates why an intelligence-based approach will be under constant attack while a physical security approach may be left largely intact despite minor legal challenges.

Service May 27, 2009); TSA, *supra* note 106. The TSA has likely taken over this function as of November 1, 2010. This date marked the end of the grace period for airlines to clear all airline reservations that had not included the required Secure Flight data. Posting of Blogger Bob, TSA Blog Team, to The TSA Blog, http://blog.tsa.gov/2010/10/talk-to-tsa-secure-flight-november-1st.html (Oct. 26, 2010, 13:16 EST). However no government announcement has been made expressly stating the TSA takeover of this function occurred. The government has, however, stated its intention to completely perform this function in late 2010 and indicated it is on pace to meet this goal. Press Release, Transportation Security Agency, TSA's Secure Flight Begins Vetting Passengers (Mar. 31, 2009), http://www.tsa.gov/press/releases/2009/0331.shtm.; Transportation Security Administration, *Security Programs: Secure Flight Program,* http://www.tsa.gov/what_we_do/layers/secureflight/ (updated Nov. 1, 2010).

[125] Sullivan I, *supra* note 59.

[126] *Id.*

[127] Eileen Sullivan, *Feds Didn't Call All Airlines to Warn of Suspect,* Associated Press, May 5, 2010, *available at* http://abcnews.go.com/Business/wirestory?id=10560833&page=1 [hereinafter Sullivan II].

[128] *See* Omar, *supra* note 16, at 269; Strantz, *supra* note 45, at 464. *See generally* Findings and Recommendations of the Commission on Aviation Security and Terrorism, 136 Cong. Rec. S6270 (1990) (statement of Senator Frank Lautenberg).

[129] 9/11 Commission Report, *supra* note 45, 77–80, 407–19.

[130] Sullivan I, *supra* note 59.

A. The Law Challenging an Intelligence Approach

There are a wide variety of legal challenges to CAPPS II and Secure Flight affecting their capabilities as intelligence-based AATS. Many of these are still academic or non-judicial, as the stronger intelligence regime, CAPPS II, was preemptively terminated. Yet the challenges are no less real. Indeed, because of the non-judicial threats to CAPPS II, Secure Flight was vulnerable to legal attacks even before becoming operational. In 2005, the Government Accountability Office (GAO), the investigative arm of Congress, concluded that the TSA had violated the 1974 Privacy Act while testing Secure Flight by using commercial databases and airline records to track nearly 100 million accounts without informing the public of the scope of the information used or of its procedural safeguards.[131] The TSA violation drew a sharp rebuke from Democratic and Republican Senate leaders who accused the TSA of jeopardizing both public trust and airline security.[132] Not surprisingly, this revelation initiated multiple civil lawsuits.[133]

Since Secure Flight has become operational, many other potential legal challenges have emerged, nearly every one based in constitutional safeguards. One argument is that Secure Flight and its predecessors violate the fundamental right to travel, defined in *Shapiro v. Thompson*, 394 U.S. 618 (1969).[134] In *Shapiro*, the Court held that as a fundamental right, classifications that restricted travel were only lawful if they passed a "strict scrutiny" test.[135] Strict scrutiny review requires that a compelling governmental interest be served, that the method be narrowly tailored to meet that goal, and that the process be the least restrictive means of achieving the goal.[136] While preventing

---

[131] Letter from Cathleen A. Berrick, Director of Homeland Security and Justice Issues of the Government Accountability Office, and Linda D. Koontz, Director of Information Management Issues of the Government Accountability Office, to various Congressional members (July 22, 2005), at 1, *available at* http://www.gao.gov/new.items/d05864r.pdf.

[132] Letter from Susan Collins, U.S. Senator, and Joseph Lieberman, U.S. Senator, to Michael Chertoff, Secretary of the Department of Homeland Security, (July 22, 2005), at 1, *available at* http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MinorityNews&ContentRecord_id=57ec057d-8c26-4d30-b8a5-07c064bc02dc&Region_id=&Issue_id=baeab989-7f6a-4e7a-83b9-f18fa0a065c9.

[133] David Shucosky, *Federal Lawsuit Challenges Data Collection Under Secure Flight Program*, JURIST: LEGAL NEWS AND RESEARCH, Aug. 18, 2005, http://jurist.law.pitt.edu/paperchase/2005/08/federal-lawsuit-challenges-data.php; Martin H. Bosworth, *Judge Dismisses JetBlue Lawsuit*, CONSUMERAFFAIRS.COM, Aug. 2, 2005, http://www.consumeraffairs.com/news04/2005/jetblue_suit.html (noting that while the judge dismissed the lawsuit for lack of damages, JetBlue did violate its privacy policy); Thomas R. Burke, Privacy and Security Law Blog, http://www.privsecblog.com/2006/02/articles/surveillance/tsa-and-fbi-settle-no-fly-list-foia-lawsuit/ (Feb. 1, 2006).

[134] Dummer, *supra* note 53, at 599–600. Though international travel has fewer protections than domestic travel, restrictions on international travel are only valid if they are narrowly constructed. Kent v. Dulles, 357 U.S. 116, 129 (1958).

[135] Dummer, *supra* note 53, at 600.

[136] *See, e.g.,* Eugene Volokh, *Freedom of Speech, Permissible Tailoring and Transcending Strict Scrutiny,* 144 U. PA. L. REV. 2417, 2417 (1997) (citing Burson v. Freeman, 504 U.S. 191, 198 (1992) (plurality); Austin v. Michigan Chamber of Commerce, 494 U.S. 652, 655 (1990); Boos v. Barry, 485 U.S. 312, 334 (1988) (plurality); Board of Airport Comm'rs v. Jews for Jesus, Inc., 482 U.S. 569, 573 (1987); Cornelius v. NAACP Legal Defense and Educ. Fund, Inc., 473 U.S. 788, 800 (1985); United States v. Grace, 461 U.S. 171, 177 (1983); Perry Educ. Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37, 45

terrorism is certainly a compelling governmental interest, serious questions arise concerning the other two prongs of this test. To properly function, Secure Flight must collect a wide variety of passenger data. Such broad information gathering could easily exceed narrow tailoring. But the "least restrictive means" prong provides the biggest challenge, as the error rates under Secure Flight could reach between 800 to 1600 needless harassments per day.[137] Though citizens do not have a right to travel in the most convenient or efficient manner,[138] the burden is not on them to assert their right to travel. Rather, the government bears the burden of proving that their restriction is lawful under strict scrutiny.[139]

Another argument is based on the individual's fundamental property rights, which cannot be infringed upon without due process.[140] When an individual purchases an airline ticket, a contract similar to a rental or purchase agreement is formed by purchasing the right to a seat.[141] The right to receive that benefit is a property interest, and passengers have a contractual right to receive that benefit and occupy the seat.[142] Though an airline can revoke a seat, the ticket-holder should be able to sue under a breach of contract claim.[143] Through the TSA's intrusion into a ticket-holder's right to board the flight, the government may have infringed upon the passenger's property rights. Alternatively, an argument that repeated dealings build a legitimate property right to continue those dealings when no warning has been given otherwise (creating an "expectancy of interest") has been gaining traction in property law overall, particularly for ticket holders.[144] As Secure Flight's false positives may delay up to 1600 harmless passengers daily, it is highly probable that some portion of these passengers will miss

---

(1983)). *See generally* United States v. Carolene Products, 304 U.S. 144, 153 n.4 (1938) (establishing the strict scrutiny **STANDARD).**

[137] Audrey Hudson, *Airline Profiling System Defended,* WASH. TIMES, Feb. 13, 2004, at A11(citing a four percent error rate); Leigh A. Kite, Note, *Red Flagging Civil Liberties and Due Process Rights of Airline Passengers: Will a Redesigned CAPPS II System Meet the Constitutional Challenge?,* 61 WASH. & LEE L. REV. 1385, 1423–24 (2004) (proposing a two percent error rate as a low estimate, but noting error rates of 400 to 800 for two percent rates and 800 to 1600 for four percent rates); Sara Kehaulani Goo, *Fliers to be Rated for Risk Level: New System Will Scrutinize Each Passenger, Assign a Color Code*, THE WASH. POST, Sept. 9, 2003, at A01.

[138] Kansas v. United States, 797 F. Supp. 1042, 1050, 1052 (D.D.C. 1992) (holding that so long as other means of travel were available, preventing passengers from boarding planes was constitutional). *See* Dummer, *supra* note 53, at 602 n.100 for a full analysis.

[139] *But see* Rahman v. Chertoff, No. 05 C 3761, 2010 WL 1335434, at *1 (N. D. Ill. Mar. 31, 2010) (upholding the TSDB as providing rational basis for detentions).

[140] U.S. CONST. amend. V.

[141] Kite, *supra* note 137, at 1416–17.

[142] Perry v. Sindermann, 408 U.S. 593, 601 (1972) (holding that "a person's interest in a benefit is a 'property' interest for due process purposes if there are such rules or mutually explicit understandings that support his claim of entitlement to the benefit and that he may invoke at a hearing"); Marrone v. Wash. Jockey Club, 227 U.S. 633, 636 (1913) (holding that a contractual right to receive a benefit creates an interest in the property when the contract also operates as a conveyance).

[143] Marrone, 227 U.S. at 636, 637.

[144] Grossman v. Boston Red Sox Baseball Club Ltd. P'ship [*In re* Platt], 292 B.R. 12, 17 (Bankr. D. Mass. 2003); *In re* I.D. Craig Serv. Corp., 138 B.R. 490, 502 (Bankr. W.D. Pa. 1992); Yarde Metals, Inc. v. New Eng. Patriots Ltd. P'ship, 16 Mass. L. Rptr. 733, No. 03-3832-E, 2003 WL 22304072, at *4-*5 (Mass. Super. Ct. 2003), *aff'd*, 834 N.E.2d 1233 (Mass. App. Ct. 2005). *Contra In re* Liebman, 208 B.R. 38, 39, 41 (Bankr. N.D. Ill., E. Div. 1997).

their flights even after being "cleared."[145] Whether the TSA can infringe so heavily upon this right on a daily basis is highly questionable.

The use of illegal racial profiling has also posed a challenge to intelligence regimes. While the debate on the merits of racial profiling is a topic best saved for another venue, there are two known truths. First, each modern AATS until Secure Flight has rejected claims that it used race as a determining threat factor.[146] Second, each modern AATS has likely used race as a determining threat factor, despite contrary assertions.[147] Not surprisingly, these violations have led to lawsuits against the TSA, TSA employees, and airlines.[148] In an interesting distinction, a press release from the TSA regarding Secure Flight noted that it would not perform "inappropriate" racial or ethnic profiling.[149] By attempting to distinguish Secure Flight's treatment of race from that of the older AATS, the TSA has chosen to walk a very fine line. On one hand, it states that it may collect data, but on the other, it signals that it will not handle that data inappropriately. Three decades of secretly using racial data and half a century of repeating the same intelligence mistakes suggest otherwise.

Perhaps the most damaging challenge for security is that an intelligence-based AATS is a lightning rod for widespread criticism. At its very root, an intelligence based anti-terrorism system simply feels like spying on Americans.[150] If terrorism has brought a new relaxation of Fourth Amendment protections against searches and seizures,[151]

---

[145] Correcting any mislabeling of passengers will take time, likely requiring approval by personnel beyond the average "ticket agent." Given that many people do not arrive to the airport with much time to spare, such delays could easily cause passengers to miss their flights.

[146] *See* Office of Aviation Enforcement Proceedings, Dep't of Transp., Carrying Out Transportation Inspection and Safety Responsibilities in a Nondiscriminatory Manner (Oct. 12, 2001), http://airconsumer.dot.gov/rules/ 20011012.htm (explaining, just one month after 9/11, that "those carrying out transportation inspection and enforcement" would not use race or ethnicity); Dummer, *supra* note 53, at 588 (noting that the Gore Commission stated that race would not be used in the CAPPS databases); Press Release, Dep't of Homeland Sec., CAPPS II: Myths and Facts (Feb. 13, 2004), http://www.dhs.gov/xnews/releases/press_release_0348.shtm (explaining that CAPPS II would not use race or ethnicity).

[147] *See generally* Dummer, *supra* note 53, at 588 (citing evidence that CAPPS I and CAPPS IE allegedly used race); Bob Cuddy, *Caught In The Backlash: Stories from Northern California* (Rachel Swain ed., Am. Civil Liberties Union Found. of N. Cal. 2002), http://www.aclunc.org/issues/government_surveillance/asset_upload_file532_ 4380.pdf (documenting 20 individuals' experiences since Sept. 11, 2001). There is little reason to believe that CAPPS II would have addressed race differently; however, as previously noted, CAPPS II was never fully implemented.

[148] Press Release, Am. Civil Liberties Union of N. Cal., ACLU, ADC and Relman Law Firm Sue Four Major Airlines Over Discrimination Against Passengers (June 4, 2002), http://www.aclu.org/racial-justice/aclu-adc-and-relman-law-firm-sue-four-major-airlines-over-discrimination-against-pass; Mike M. Ahlers, *JetBlue, TSA Employees Settle Arabic T-shirt case for $240,000*, CNN.COM/US, Jan. 7, 2009, http://edition.cnn.com/2009/US/ 01/07/jet.blue.settlement/.

[149] Kip Hawley, *Secure Flight – Opportunity Knocks*, KIP HAWLEY'S JOURNAL, Nov. 1, 2007, http://www.tsa.gov/press/journal/secure_flight.shtm (explaining that Secure Flight does not perform "inappropriate" racial profiling).

[150] Indeed, it is included as spying in at least one influential depiction and analysis of spying. HITZ, *supra* note 123, at 14 ("Nonetheless, we shall not restrict our inquiry to cloak-and-dagger operations, dead drops, and microdots . . . . We shall need to understand better the possibilities of using modern computers to capture and analyze reams of data, i.e., data mining.").

[151] Illinois v. Caballes, 543 U.S. 405, 423–25 (2005) (Ginsburg, J., dissenting) (noting that a bomb sniffing dog would likely be treated differently than a drug sniffing dog in interpreting constitutional restrictions on

domestic intelligence gathering on American citizens inspires a strong correction. While the TSA has tried to manage this risk by quickly settling lawsuits,[152] this is a poor long-term strategy. Though many challenges to an intelligence based approach would be legally defeated, each one could lead to a parallel of Justice O'Connor's now infamous repudiation of the Executive's overreaching war powers in *Hamdi v. Rumsfeld*, 542 U.S. 507, 534-39 (2004). And, unlike the treatment of enemy combatants criticized in *Hamdi*, the TSA's intrusive methods have few supporters. As the intelligence regime is already weakened by privacy protections, any successful legal challenge could be devastating to its practical value.

B. The Law Supporting a Physical Security Approach

While law and politics threaten an intelligence-based AATS, both support a physical security approach. This paper's scope cannot fully describe the broad-ranging security powers awarded to the TSA, but a few general statements should be noted. Though most searches and seizures require the high threshold of a warrant and reasonable suspicion, searches performed by the TSA are administrative searches and therefore must only meet a reasonableness standard.[153] To be found reasonable, an airport search must only (1) be "no more extensive or intensive than necessary, in light of current technology, to detect the presence of weapons or explosives;" (2) be "confined in good faith to that purpose;" and (3) allow a potential passenger to "avoid the search by choosing not to fly."[154] This authority is derived from the need to prevent weapons, explosives, and other potentially dangerous items from being brought into the air.[155] Such a low legal standard very broadly supports the TSA searches for dangerous items while encouraging the

---

searches and seizures); Anne Coughlin, Professor of Law, Univ. of Va. Sch. of Law, Lecture on criminal investigation procedures (Mar. 23, 2010).

[152] *See* Gordon v. Fed. Bureau of Investigation, 388 F. Supp. 2d 1028 (N.D. Cal. 2005); Press Release, Am. Civil Liberties Union, TSA and FBI Ordered to Pay $200,000 to Settle "No Fly" Lawsuit (Jan. 24, 2006), http://www.aclu.org/national-security/tsa-and-fbi-ordered-pay-200000-settle-no-fly-lawsuit?tab=legaldoc. Though the TSA may have intended to take these actions anyway, it cost $200,000 in the process.

[153] Though the Supreme Court has not directly ruled on the reasonableness of domestic airport searches, it has suggested that they are administrative searches in dicta. City of Indianapolis v. Edmond, 531 U.S. 32, 47–48 (2000) (noting that its ruling did not "affect the validity of . . . searches at places like airports . . ."); Chandler v. Miller, 520 U.S. 305, 323 (1997) (noting that suspicionless searches such as "searches now routine at airports" may be reasonable under Fourth Amendment standards); Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 675 n.3 (1989) (noting favorably the government's practice of suspicionless searches of airline passengers and luggage and the lower courts' findings that such searches are reasonable administrative searches under the Fourth Amendment). Additionally, Appellate circuits have supported this proposition. *See*, *e.g.* United States v. Dalpiaz, 494 F.2d 374, 376 (6th Cir. 1974); United States v. Aukai, 497 F.3d 955, 958 (9th Cir. 2007); United States v. Hartwell, 436 F.3d 174, 178 (3d Cir. 2006).

[154] United States v. Fofana, 620 F.Supp.2d 857, 862 (S.D. Ohio 2009) (citing *Aukai*, 497 F.3d at 962).

[155] *See generally* 49 U.S.C. § 44901; *Aukai*, 497 F.3d at 960; *Dalpiaz*, 494 F.2d at 378. A full list of prohibited items may be found at http://www.tsa.gov/assets/pdf/prohibited_and_permitted_items_10-24-07.pdf.

adaptation and use of newer, better technological devices.[156] This powerful combination gives the TSA a firm foundation for strong physical security measures.

The search standard is even lower for flights originating from or departing to foreign destinations. The TSA may "'conduct routine searches and seizures at the border, without probable cause or a warrant,' but may need some level of suspicion to conduct nonroutine searches."[157] The "routineness" of a search depends on the invasiveness of the search, as considered in the totality of the circumstances.[158] Searches of purses, wallets,[159] computers, personal documents, outer clothing, luggage, shoes, and "pat downs" have all been held routine searches allowed at borders.[160] Individuals may be detained for extended periods of time without warrants or charges, depending upon the nature of the expected threat.[161] This standard also interprets photographing, intensive questioning, and fingerprinting the suspects as routine.[162] Thus, while domestic measures enjoy adequate legal support, physical security measures on international flights—where threats are arguably most likely—are awarded the most freedom.

Though broadly supported, the physical security approach has not been awarded *carte blanche* to search and seize passengers. First, "mission creep" in the TSA has led to security searches being used to uncover non-security related offenses.[163] The courts

---

[156] The drive for better technological devices is to detect the most threats and prevent losing the arms race again to "third world terrorists." 136 CONG. REC. S9172 (1990) (statement of Sen. Lautenberg, member of the Commission on Aviation Security and Terrorism, concerning the Findings and Recommendations of the Commission).

[157] Rahman v. Chertoff, 2010 WL 1335434 at *1 (N.D. Ill. Mar. 31, 2010) (quoting United States v. Montoya de Hernandez, 473 U.S. 531, 537, 541 n.4 (1985)).

[158] United States v. Tsai, 282 F.3d 690, 694–96 (9th Cir. 2002).

[159] United States v. Irving, 452 F.3d 110, 123 (2d Cir. 2006) ("Routine searches include those searches of outer clothing, luggage, a purse, wallet, pockets, or shoes . . . ."). *But see* United States v. Fofana, 620 F.Supp.2d 857, 863, 866 (S.D. Oh. 2009) (holding that the TSA was only authorized by Congress to search for guns and explosives). This would restrict wallet searches. However this case (number 09-4397) is being appealed to the Sixth Circuit. *See* Pending Cases, Southern District of Ohio, http://www.ca6.uscourts.gov/case_reports/rptPendingDistrict_OHS.pdf.

[160] *Rahman*, 2010 WL 1335434 at *1–2; United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008) (holding that the search of a computer by customs officials does not require a showing of reasonable suspicion); United States v. Johnson, 991 F.2d 1287, 1291 (7th Cir. 1993) ("A search at the border of a traveler's luggage and personal effects is routine."); United States v. Carreon, 872 F.2d 1436, 1442 (10th Cir. 1989) ("Inspector Gordon's inspection of the Carreon vehicle, documents and belongings, the subsequent 'pat down' of the female passenger and the detention of Carreon while Gordon went for his electric drill were all reasonable, routine border search procedures.").

[161] Montoya de Hernandez, 473 U.S. at 542–44 (finding that holding a suspect for 16 hours for narcotics suspected in her alimentary canal was reasonable); Darulis v. Clark, No. 08cv2344 DMS, 2010 WL 962938 at *3–4 (S.D. Cal. Mar. 16, 2010) (holding that a search in which the border entrant was handcuffed for fifteen minutes was routine). Further, border detentions of up to six hours are considered routine. United States v. Flores-Montano, 541 U.S. 149, 155 n.3 (stating that "delays of one to two hours at international borders are to be expected"); Tabbaa v. Chertoff, 509 F.3d 89, 99–101 (2d Cir. 2007) (holding that a six-hour detention was "not . . . out of the realm of what is considered routine").

[162] *Tabbaa,* 509 F.3d at 98–99 (holding that a stop involving fingerprinting, photographing, and "intrusive questioning" is routine).

[163] *See, e.g.,* City of Indianapolis v. Edmond, 531 U.S. 32, 37–42 (2000) (noting that administrative searches cannot be used to detect ordinary criminal activity);United States v. $124,570 U.S. Currency, 873 F.2d 1240, 1244 (9th Cir.1989) (recognizing the "risk that administrative searches will be infected by general law enforcement objectives, and the concomitant need for the courts to maintain vigilance"); United States v. Epperson, 454 F.2d 769, 771 (4th Cir.1972) (holding that searches "for the sole purpose of

have continuously rejected the application of airline searches for such purposes and have excluded the "fruit" of these searches from admissible evidence. Second, the TSA has produced overeager officers who extend their authority to radical proportions. The most startling case occurred on a domestic flight in 2002. Federal Marshals subdued and detained an erratic suspect at gunpoint, then moved that passenger to the seat next to Dr. Bob Rajcoomar. When Dr. Rajcoomar asked to switch seats, a stewardess directed him to another seat. The Federal Marshals then drew their guns and demanded that no one else move.[164] After landing, the Federal Marshals arrested Dr. Rajcoomar, a retired U.S. Army Major, stating that he had been "watching [the suspect and Marshals] too closely."[165] A lawsuit was filed but settled out of court in return for changes in TSA policies, a written apology from the Administrator of the TSA, and $50,000.[166] In a 2009 case, the TSA detained a man named Steve Bierfeldt who intended to fly from St. Louis to Washington D.C. carrying around $4,700 in cash he had generated selling bumper-stickers for "Campaign for Liberty," a Ron Paul-led organization.[167] As the state of Missouri had warned the TSA that illegal militia members were likely supporters of third-party organizations and candidates, he was temporarily detained.[168] Though the TSA has maintained that the initial search and seizure were lawful, the event turned into a public relations fiasco as Mr. Bierfeldt secretly recorded his extended interrogation, in which TSA agents appeared needlessly aggressive.[169]

While the overreach of TSA search and seizure procedures raises legitimate concerns, they are hardly comparable to the serious legal problems with an intelligence approach. This is indicated by the minimal media coverage awarded to potential violations, as well as the lack of political diatribe from the mainstream left or right. The most intrusive and controversial of the new measures, the use of full body scanners, recently received extensive media attention when a video surfaced of a passenger's boisterous refusal to enter the machine or receive an alternative full body "pat down."[170]

---

discovering weapons and preventing air piracy and not for the purpose of discovering weapons and pre-criminal events" was constitutionally permissible); Scott McCartney, *Is Tougher Airport Screening Going Too Far?*, THE WALL STREET JOURNAL, The Middle Seat, July 16, 2009, http://online.wsj.com/article/SB10001424052970204556804574261940842372518.html.

[164] Bob Herbert, Op-Ed., *High-Altitude Rambos*, N.Y. TIMES, Sept. 23, 2002, at A25, *available at* http://www.nytimes.com/2002/09/23/opinion/23HERB.html.

[165] Anita Ramasastry, *Airplane Security: Terrorism Prevention or Racial Profiling?*, CNN.COM, Oct. 2, 2002, http://archives.cnn.com/2002/LAW/10/02/ramasastry.security/.

[166] Rajcoomar v. United States, No. 03-2294, Settlement Order at 1 (E.D. Pa. June 30, 2003), http://www.aclufl.org/pdfs/Legal%20PDfs/Rajcoomar%20settlement%20order.pdf; Press Release, American Civil Liberties Union, Government Settles ACLU's Racial Profiling Lawsuit Against TSA, Agrees to Alter Agency Procedures Nationwide (July 31, 2003), http://www.aclu.org/national-security/government-settles-aclus-racial-profiling-lawsuit-against-tsa-agrees-alter-agency-.

[167] CNN Video, *Passenger Says TSA Agents Harassed Him*, CNN.COM, http://www.cnn.com/2009/US/06/20/tsa.lawsuit/index.html.

[168] *TSA Detains Official from Ron Paul Group,* WASH. TIMES, Apr. 6, 2009, *available at* http://www.washingtontimes.com/news/2009/apr/06/tsa-detains-official-from-ron-paul-group/?page=1.

[169] *Id.* The TSA later confirmed that the "tone and language used by the TSA employee was inappropriate." Posting of Blogger Bob, TSA Blog Team, to The TSA Blog, http://blog.tsa.gov/2009/04/incident-at-st-louis-international.html (Apr. 3, 2009, 15:13 EST).

[170] CNN Wire Staff, *TSA: Despite Objections, All Passengers Must be Screened*, CNN.com, Nov. 15, 2010, http://www.cnn.com/2010/TRAVEL/11/15/california.airport.security/index.html?hpt=T2; Mike Levine, *DHS Chief Says Abandoning Airport Scanners Would be "Irresponsible", CA Man Warns TSA Not*

Some travel industry organizations have expressed concerns, while others want the TSA to better explain the measures to the public.[171] Yet polling shows overwhelming public support for use of the machines.[172] TSA officials have been largely responsible in the performance of their duties and, as the previous examples show, they have corrected deficiencies when they appeared. But most importantly, the TSA can afford to make minor corrections to its physical security measures because, overall, the approach is both legally and operationally sound.[173] Unlike an intelligence approach, a physical approach can respond to political and legal pressure without precipitating a major decline in security.

IV. CONCLUSION

Within forty-eight hours of the Christmas Day Bomber's attempt, the TSA ordered strict physical security measures for all incoming flights to the United States.[174] The measures included a frisk at the point of departure for all passengers, regardless of citizenship.[175] But just nine days later, on January 2, 2010, the TSA limited these stringent physical security measures to planes arriving from just fourteen countries.[176] For planes arriving from these countries, the new procedures included frisks at the point of departure, restrictions on carry-on baggage, and placing passengers in their seats at least one hour before take-off.[177] The TSA announced the measures were "long term" and "sustainable," and would be constantly reviewed to ensure "the highest level of security."[178]

---

to "Touch my Junk," Becomes Online Hit, Nov. 15, 2010, http://politics.blogs.foxnews.com/2010/11/15/dhs-chief-says-abandoning-airport-scanners-would-be-irresponsible-ca-man-warns-tsa-not-to.

[171] CNN Wire Staff, *TSA: Despite Objections, All Passengers Must be Screened*, CNN.com, Nov. 15, 2010, http://www.cnn.com/2010/TRAVEL/11/15/california.airport.security/index.html?hpt=T2 (noting the U.S. Travel Association's concerns); Joan Lowy and Adam Goldman, *Scanners and Pat-Downs Upset Airline Passengers*, Nov. 15, 2010, http://www.forbes.com/feeds/ap/2010/11/15/general-us-airport-security_8107688.html (citing the Airports Council of U.S. and Canadian Airports' desire for better public education).

[172] Thomas Frank, *Most OK with TSA Full-Body Scanners,* USA TODAY, Jan. 11, 2010, at 1A, *available at* http://www.usatoday.com/travel/flights/2010-01-11-security-poll_N.htm.

[173] The most notable example is allowing passengers to substitute a private, full body "pat-down" instead of entering the full body scanner. Though a scanner could likely detect an object that pat-down could miss because of human error or not touching certain bodily areas, the pat-down is still highly effective.

[174] Posting of Blogger Bob, TSA Blog Team, to The TSA Blog, http://blog.tsa.gov/2009/12/dhs-statement-on-northwest-airlines.html (December 26, 2009, 1:00 EST).

[175] Thomas Frank, *TSA List Eyes Fliers From 14 Countries*, USA TODAY, Jan. 4, 2010, at 1A, *available at* http://www.usatoday.com/NEWS/usaedition/2010-01-04-1Aterror04_ST_U.htm [hereinafter *14 Countries*].

[176] *Id.*; Press Release, Transportation Security Administration, TSA Statement on New Security Measures for International Flights to the U.S. (Jan. 3, 2010), http://www.tsa.gov/press/happenings/010310_statement.shtm [hereinafter New Security Measures].

[177] *14 Countries*, *supra* note 176.

[178] *Passengers Again Free to Move Around Cabin*, MSNBC/ASSOCIATED PRESS, Dec. 29, 2009, http://www.msnbc.msn.com/id/34601479/ns/travel-news/ (reporting the statement by TSA spokeswoman Sterling Payne that the measures would be constantly reviewed "to ensure the highest level of security"); New Security Measures, *supra* note 177.

On April 2, 2010, the TSA and DHS abolished these physical security measures.[179] In their place, the DHS implemented a new intelligence-based system.[180] This new approach mandates additional screening only for individuals fitting a "terrorist" profile based on intelligence collected about previous terrorists.[181] Secretary Napolitano proudly described the measures as "a more intel- or information-based way to screen."[182] Congressman Peter King, the ranking Republican on the Homeland Security Oversight Committee, lauded the new system for its "better and more sophisticated use of intelligence" and argued that it "should have been done before."[183] Such statements only further reflect the dangerous and predictable pattern illustrated throughout this paper: the rejection of physical security measures that work in favor of intelligence measures that do not. The pattern follows a yo-yo effect, moving slowly from a strong physical security approach after an attack to an intelligence-based approach, then quickly snapping back to more physical measures after the next attack. It is a deadly pattern that America seems likely to repeat because we fail to consider our history.

There has been some recent hope of changing the trajectory. In early April 2010, Secretary Napolitano announced the TSA used, or would soon use, a variety of important physical security measures.[184] The measures include bomb-sniffing dogs and explosive-detecting "swabs," which are both important tools; more significantly and controversially, they add full-body scans and undercover agents trained in monitoring potential terrorist threats.[185] The advanced tools these programs use illustrate that choosing a physical security approach does not mean abandoning advanced technological intelligence for a primitive show of physical strength. Such measures are a welcome change; as *Scientific American* noted, physical security procedures coupled with better technology would have prevented Mr. Abdulmutallab from ever getting close to his plane.[186] The strong public defense in November 2010 by Secretary Napolitano and TSA Administrator John Pistole of using either full body scanners or full body "pat-downs" on every passenger suggests the government may have finally recognized there is no substitute for physical measures.[187] Paired with the current intelligence regime, physical

---

[179] Mike M. Ahlers, *U.S. Announces New Airport Security Measures*, CNN, Apr. 2, 2010, http://www.cnn.com/2010/TRAVEL/04/02/airline.security/index.html?hpt=T1.

[180] *Id.*

[181] *Id.*

[182] *Id.*

[183] Eileen Sullivan, *Airport Security Checks Revamped for Travel to U.S.*, THE HUFFINGTON POST, Apr. 2, 2010, http://www.huffingtonpost.com/2010/04/02/airport-security-checks-r_n_522694.html.

[184] Press Release, Department of Homeland Security, Secretary Napolitano Announces New Measures to Strengthen Aviation Security (Apr. 2, 2010), http://www.dhs.gov/ynews/releases/pr_1270217971441.shtm.

[185] Posting of Scott McCartney to The Middle Seat Terminal, http://blogs.wsj.com/middleseat/2010/04/02/new-security-measures-what-do-they-mean-for-travelers (Apr. 2, 2010 01:41 EST). The full-body scanners, while far from universally accepted, are supported by the majority of the public. *Fourteen Countries*, *supra* note 176. Of likely much greater controversy is the use of undercover agents who may be trained, among other things, to ethnically profile. Frederick Hitz, Professor of Law, Univ. of Va. Sch. of Law, Lecture (Feb. 24, 2010).

[186] Posting of David Biello to Observations, http://www.scientificamerican.com/blog/post.cfm?id=what-could-have-stopped-the-christm-2009-12-28 (Dec. 28, 2009 03:00 EST).

[187] Mike Levine, *DHS Chief Says Abandoning Airport Scanners Would be "Irresponsible", CA Man Warns TSA Not to "Touch my Junk," Becomes Online Hit*, Nov. 15, 2010,

security could make America's AATS truly outstanding. But if history is our guide, the new physical security measures will not last for long. The United States will soon divert resources dedicated to these measures toward more intelligence activities. If this happens, Secure Flight's techniques will meet the same fate as every other intelligence-based AATS before it.

It is obvious that American AATS's have not been successful. It is no surprise then that even the Department of Homeland Security's Assistant Secretary for Intergovernmental Programs, Juliette N. Kayyem, laments that "[n]o terrorist attack has ever been stopped at an airport . . . ."[188] The systems have not worked because they have been based on inadequate measures and wishful thinking. By pursuing a novel approach for an American AATS—sticking with measures that work—Kayyem's statistic can change.

---

http://politics.blogs.foxnews.com/2010/11/15/dhs-chief-says-abandoning-airport-scanners-would-be-irresponsible-ca-man-warns-tsa-not-to (quoting Secretary Napolitano); CNN Wire Staff, *TSA: Despite Objections, All Passengers Must be Screened*, CNN, Nov. 15, 2010, http://www.cnn.com/2010/TRAVEL/11/15/california.airport.security/index.html?hpt=T2 (quoting TSA Administrator John Pistole).

[188] Juliette N. Kayyem, *What Not to Take from Britain's Success,* THE WASH. POST, Aug. 12, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/08/11/AR2006081101399.html.