The TSA's New Precheck Is Beginning to Look a lot like CAPPS II: The Privacy Implications of Reviving the Tenets of the Failed Predecessor

Katie Cristina

Follow this and additional works at: https://scholar.smu.edu/jalc

Recommended Citation
https://scholar.smu.edu/jalc/vol78/iss3/5
THE TSA'S NEW PRECHECK IS BEGINNING TO LOOK A LOT LIKE CAPPS II: THE PRIVACY IMPLICATIONS OF REVIVING THE TENETS OF THE FAILED PREDECESSOR

KATIE CRISTINA*

TABLE OF CONTENTS

I. INTRODUCTION ........................................... 618

II. BRIEF HISTORY OF PASSENGER PROFILING SYSTEMS ........................................... 620
A. AUTOMATED TARGETING SYSTEM—CBP .................. 621
B. CAPS .................................................. 623
C. CAPPS II .................................................. 624
D. SECURE FLIGHT ........................................... 627
E. LESSONS LEARNED ....................................... 628

III. AIRLINE PASSENGERS AND THEIR RIGHT TO PRIVACY ........................................... 630
A. FOURTH AMENDMENT SEARCHES IN THE AIRPORT CONTEXT ........................................... 631
B. RECENT FOURTH AMENDMENT SCRUTINY OF TECHNOLOGICAL SEARCHES ...................... 633
C. THE PRIVACY ACT AND CHALLENGES TO PASSENGER PROFILING SYSTEMS ...................... 635

IV. TSA'S NEWEST RISK-BASED APPROACH TO SECURITY: PRECHECK ................................ 636
A. INTERNATIONAL AVIATION OBJECTIVES .................. 636
B. TSA PRECHECK ........................................... 639
C. PRECHECK'S NEW ANNOUNCEMENT FOR PRIVATE INFORMATION GATHERERS .................. 642

V. CAN PRECHECK SURVIVE IN A POST-CAPPS II AMERICA? .................................. 643

* J.D. Candidate, SMU Dedman School of Law, 2014; B.A., Political Science, Louisiana State University, 2011. The author would like to thank her family, friends, and fiancé, Andrew, for their love and support.
A. PreCheck + Secure Flight + Commercial Data = CAPPS II Reincarnated .................. 644
B. Fourth Amendment Scrutiny ....................... 646
C. The Privacy Act’s Weaknesses .................... 648
VI. CONCLUSION ........................................... 649

“We must not allow this piece of our past to become prologue. . . . We will lose . . . without a shot being fired if we sacrifice the liberties of the American people in the belief that by doing so we will stop the terrorists.”

- Senator Russell Feingold, October 2001

I. INTRODUCTION

In what has been artfully expressed as “The Bin Laden Exception,” post-September 11, 2001 (9/11) fear of terrorism has driven most American citizens to overlook governmental intrusions on their constitutional rights—particularly Fourth Amendment and Privacy Act rights—in exchange for what they assume means a safer nation. Nowhere is this “Exception” more preva-

---

3 Id.
7 Luna, supra note 5, at 238–42.
lent than in commercial air travel, which provides transportation to approximately 640 million passengers each year. Due to the terrorist attacks on 9/11, Congress passed the Aviation and Transportation Security Act, which created the Transportation Security Administration (TSA) to protect passenger safety through various screening measures. Civil rights groups usually challenge such measures as violations of privacy, and as a result, the TSA has become synonymous with negative depictions of "Big Brother" watching over travelers. Others argue that the TSA is largely successful in keeping travelers safe and that with such security comes some justifiable loss of civil liberty.

Most recently, the TSA implemented PreCheck, a passenger screening program that offers expedited screening to frequent fliers who volunteer personal information so that the TSA can conduct an extensive background check to prescreen the passengers. PreCheck seems to be an ideal solution to today's domestic travel inconveniences. At least that is how the TSA is marketing the program: if a traveler is willing to give up some information about herself, she will be able to enjoy a security experience that no longer consists of removing certain articles of clothing or unpacking liquids and laptops. Some people may agree with this program's goals, believing or perhaps accepting that we live in a world where informational privacy is limited, if not nonexistent. Yet others hold on to and fight for the "right to be let alone" and the right to be free from government knowledge of their every move or mouse click. To these

---

16 Groups such as the American Civil Liberties Union (ACLU) and Electronic Privacy Information Center (EPIC) have been particularly vocal against passenger prescreening programs. See Heather Mac Donald, Perils of Privacy, N.Y. Post
individuals, a closer look at the TSA's PreCheck program reveals its role as an initial step toward such invasions. Privacy advocates have succeeded in halting similar programs before, but this time, with the overwhelming popularity of the "voluntary" risk-based intelligence approach, travelers will likely not even realize that PreCheck is simply a newer, shinier version of the old programs.

This comment begins with a brief description of passenger prescreening or "profiling" programs that the U.S. government has either successfully implemented or merely attempted to implement since 9/11. Each program was met with resistance, and Part II attempts to illustrate the successes and failures of each system in light of the legal and political climate in which it was introduced. Next, Part III discusses the primary legal avenues under which aviation security measures have been challenged: the Fourth Amendment and the Privacy Act. That Part reflects upon how the current judicial standards, as expressed in recent case law, are extraordinarily deferential to the government and its policies furthering aviation security. Part IV then describes the current international shift toward a risk-based security model, Checkpoint of the Future, and the TSA's newest program, PreCheck. Lastly, Part V reconciles PreCheck with the Fourth Amendment and the Privacy Act through the lens of the past screening programs and their accompanying successes and failures. The comment concludes that the PreCheck program, due to its appeal to convenience and choice, will finally give the TSA the necessary amount of public approval to move forward with risk-based intelligence, or "profiling."

II. BRIEF HISTORY OF PASSENGER PROFILING SYSTEMS

In the past twenty years, the U.S. government has attempted to strengthen aviation security with several passenger profiling systems. Each program encountered resistance from multiple organizations, the loudest of which were the American Civil Liberties' Union (ACLU) and the Electronic Privacy Information Center (EPIC). Despite this resistance, the programs and their

18 See infra Part II (discussing CAPPS II and other similar programs).
19 See MacDonald, supra note 16.
evolution illustrate the importance of striking a balance between security and liberty, particularly considering the rapid advancement of technology and intelligence.\(^{20}\) Public memory is often short, and citizens frequently become desensitized to government privacy invasions, particularly ones that are deemed necessary for national security.\(^ {21}\) Hopefully the perspectives gained from past programs can more accurately frame the PreCheck program and the potential issues that will arise during its development.

A. AUTOMATED TARGETING SYSTEM—CBP

The Automated Targeting System (ATS) is an intelligence-based screening program that U.S. Customs and Border Protection (CBP) employs to evaluate the risk of passengers traveling through the country.\(^ {22}\) A grossly oversimplified explanation of the program is that the ATS attaches a risk score to each traveler, which remains on file with CBP for forty years.\(^ {23}\) The risk score is calculated by compiling a vast array of data, including: passenger travel information provided by airlines; information regarding trips across the U.S. border; automated commercial data; Treasury Enforcement Communications System (TECS)\(^ {24}\) data; and law enforcement data.\(^ {25}\)

Rampant criticism of the ATS amongst privacy groups focused largely on the means by which the public learned of the program’s application to passengers.\(^ {26}\) While the ATS was in place to scan individuals, their luggage, and carry-ons for at least four years,\(^ {27}\) the public did not find out about the program until 2006, when the DHS published an explanation in the Federal

---

\(^{20}\) See von Rochow-Leuschner, supra note 12, at 149.

\(^{21}\) Luna, supra note 5, at 238–47.


\(^{24}\) TECS is an information database that identifies individuals suspected of federal law violations. Dep’t of Homeland Sec., Privacy Impact Assessment for CBP Procedures for Processing Travel Documents at the Border 4 (July 2, 2008).

\(^{25}\) Privacy Act of 1974; System of Records, 71 Fed. Reg. 64,543, 64,545 (Nov. 2, 2006).

\(^{26}\) Sniffen, supra note 23.

\(^{27}\) Some suggest that the use of the ATS for passenger screening actually dates back to 1999. EPIC, Comments of the Electronic Privacy Information Center
Register. In an attempt to appease privacy advocates, the DHS filed a subsequent Notice of Privacy of System Records and a Notice of Proposed Rulemaking, which sought to exempt certain information from the Privacy Act. EPIC filed a comment during the rulemaking process, citing several reasons why the program violates privacy, including the argument that it violates a constitutional right to travel. This effort to calm critics, however, was ultimately futile.

While privacy concerns remain, the ATS is here to stay. The DHS recently issued a Privacy Impact Assessment in which it reiterated its statutory authority to gather such information. Specifically, the Assessment cited 49 U.S.C. § 44909, the Enhanced Border Security and Visa Entry Reform Act of 2002, along with many other authorities. The immensely broad constitutional power of the government to protect the U.S. borders provides perhaps the strongest argument for CBP's authority to conduct such extensive screenings.
B. CAPS

Motivated largely by the perceived success of the ATS, President Clinton's Administration launched the original Computer Assisted Passenger Screening (CAPS) System to assess the risk of domestic travelers. The goal of CAPS was to shift security's focus away from "low-risk" fliers and toward "high-risk passengers" with suspicious characteristics. Marking a drastic switch to intelligence-based airport security procedures, CAPS allowed computers to assess passengers' airline travel information and other undisclosed criteria that the Federal Aviation Administration (FAA) refused to identify. The program did not extend far enough to include government data or law enforcement information. Although there was some evidence that the program used ethnicity in its assessment, the Department of Justice declared that the program was not discriminatory toward passengers.

This risk assessment dictates which passengers are subject to higher standards of screening. Shortly after implementation, CAPS was scaled back to screen only checked baggage as opposed to passengers and carry-on luggage, due in large part to the public's negative reaction. The effects of this limitation became strikingly apparent when the terrorist attacks of 9/11 occurred at the hands of nineteen individuals, nine of whom were identified by CAPS as high-risk but were not stopped because

---


40 Id.; Bankston & Gray, supra note 4 (internal quotation marks omitted).

41 Fiske, supra note 39, at 180.


43 Bankston & Gray, supra note 4 (explaining that confidential airline security manuals were leaked, and that these manuals evidenced racial consideration).

44 See U.S. Dep't of Justice Press Release, supra note 42.

45 Fiske, supra note 39, at 180–81.

they did not check any baggage. The 9/11 attacks reinstated passenger and carry-on bag screening, but the CAPS program remained inadequate and ultimately became the starting point for the newer Computer Assisted Passenger Prescreening System (CAPPS II).

C. CAPPS II

CAPPS II was a TSA-run passenger prescreening program that originally received its authority from Congress’s Aviation and Transportation Security Act, which was passed in the aftermath of 9/11. Due to U.S. citizens’ and lawmakers’ enhanced state of fear, CAPPS II immediately took a much more aggressive approach than its predecessor by considering substantially more passenger data in its evaluations. CAPPS II was designed to collect and analyze information from the government, airlines, and other commercial sources to categorize passengers into one of three levels of risk based on their individualized profiles.

CAPPS II sought to improve upon CAPS’s failings. Reliance on commercial data providers was intended to add a new level of security—a way to confirm an individual’s honesty in identification and other reported data. Similarly, government sources included criminal wanted lists and national security intelligence reports for an individual passenger’s name. After the databases collected the specific information, a passenger would receive a color-coded risk score, which, like CAPS, would determine the

47 von Rochow-Leuschner, supra note 12, at 144-45.
49 Fiske, supra note 39, at 182-83.
50 49 U.S.C. § 44903(j)(2) (2006) (“The Secretary of Transportation shall ensure that the Computer-Assisted Passenger Prescreening System, or any successor system—(i) is used to evaluate all passengers before they board an aircraft; and (ii) includes procedures to ensure that individuals selected by the system and their carry-on and checked baggage are adequately screened.”).
51 Fiske, supra note 39, at 182-83.
52 Id. at 183. The levels were Green for “low-risk”; Yellow for average or unknown risk; and Red for “high-risk” and potential no-fly orders. Leigh A. Kite, Comment, 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, 1399 (2004).
53 Fiske, supra note 39, at 182.
54 Id. at 182-83.
55 Id.
appropirate amount of screening that the individual would need to undergo before flying.\textsuperscript{56} One article suggested that factors under consideration "include[d] race, religion, political affiliations, credit history, employment, spending habits, charitable donations, unusual books purchased or checked out, and visits to certain websites."\textsuperscript{57} But, as is the case with most security measures to date, the TSA expressed that the databases and the precise sources relied on were confidential.\textsuperscript{58}

Citing privacy invasions under the Fourth and Fifth Amendments and the Privacy Act, critics' concerns focused on lack of proper redress, general political fear of large government, and concern about the effectiveness of such a process.\textsuperscript{59} Notably, the system was viewed as an alarming "black box"\textsuperscript{60} where American citizens' private lives were assessed in secret while travelers remained unaware of the information the government retained about them or how it translated into their "risk."\textsuperscript{61} The ACLU and others also cited due process problems with refusing to allow passengers to pass through security without telling them why or giving them a way to either defend themselves against their supposed risk or prevent being judged by their peers.\textsuperscript{62}

Advocacy groups also raised questions about the effectiveness of the program.\textsuperscript{63} Specifically, the error rate, which the TSA admitted could be 4\%, would generate many false alarms, which, in addition to the due process concerns expressed above, would then enlarge the pool of high-risk passengers.\textsuperscript{64} Such error dilution would diminish the importance of the high-risk label, creating a lower standard and defeating the purpose of the program.\textsuperscript{65}

---

\textsuperscript{56} Bankston \& Gray, supra note 4.

\textsuperscript{57} von Rochow-Leuschner, supra note 12, at 147.

\textsuperscript{58} Kite, supra note 52, at 1399.

\textsuperscript{59} See, e.g., von Rochow-Leuschner, supra note 12, at 149–53 (criticizing Fourth Amendment precedent and suggesting CAPPS II will likely be construed to be constitutional despite its novelty); DeGrave, supra note 46, at 133–34 (analyzing the constitutionality of CAPPS II as a "search"); Kite, supra note 52, at 1398–99 (analyzing due process concerns of Red-coded passengers); The Seven Problems with CAPPS II, ACLU (April 6, 2004), http://www.aclu.org/technology-and-liberty/seven-problems-capps-ii (discussing the problem with the vast amount of secrecy involved in what data will be analyzed).

\textsuperscript{60} The Seven Problems with CAPPS II, supra note 59.

\textsuperscript{61} Id.

\textsuperscript{62} Id.; Kite, supra note 52, at 1398–1401.

\textsuperscript{63} The Seven Problems with CAPPS II, supra note 59.

\textsuperscript{64} Id.

\textsuperscript{65} See id.
Finally, citizens exhibited fear and concern about the advanced level of the intelligence available and the potential "slippery slope" that could result from this initial step.\textsuperscript{66} For instance, while aviation security may be a justifiable concern, many citizens might feel differently if local law enforcement agencies obtained the information. Indeed, this result could raise constitutional issues. Therefore, concerns about the TSA either selling its accumulated information or risk scores to other law enforcement agencies, or using the information for all means of transportation, invoked public fear and skepticism.\textsuperscript{67}

Ultimately, the public's concerns spread to both the White House and Congress, and the TSA was not able to satisfy the public's demands regarding CAPPS II's requirements in time for implementation.\textsuperscript{68} A little over one year after the TSA announced its plans for CAPPS II, Congress put a stop to its implementation until the Government Accountability Office (GAO) could certify that the TSA could meet specific requirements.\textsuperscript{69} A GAO report stated that, as of January 1, 2004, the TSA had not addressed seven of the eight issues identified by Congress: accuracy of data, stress testing, abuse prevention, unauthorized access prevention, policies for operation and use, privacy concerns, and redress process.\textsuperscript{70} In addition to congressional challenges, the GAO report articulated three additional issues that it foresaw as major impediments to CAPPS II's success: "developing the international cooperation needed to obtain passenger data, managing the possible expansion of the program's mission beyond its original purpose, and ensuring that identity theft—in which an individual poses as and uses the information of another individual—cannot be used to negate the security benefits of the system."\textsuperscript{71}

Due largely to the TSA's failure to fully address the issues above, CAPPS II never came into existence.\textsuperscript{72} But the TSA announced a re-brand of CAPPS II, called "Secure Flight," which

\textsuperscript{66} Id.
\textsuperscript{67} Id.
\textsuperscript{70} U.S. Gov't Accounting Office, GAO-04-385, supra note 68.
\textsuperscript{71} Id.
\textsuperscript{72} Fiske, supra note 39, at 183–85.
focuses exclusively on anti-terrorism and only generates a "no-fly" list, rather than individual assessments.  

D. SECURE FLIGHT

In August 2004, after CAPPS II failed, the TSA announced a new program, Secure Flight. Initially, Secure Flight did not deliver as expected, due in large part to the TSA’s inability to comply with the Privacy Act or the requirements laid out by Congress. Does this sound familiar yet? Perhaps now it will—a major problem that the TSA faced was congressional disapproval of the TSA using commercial data in violation of the Privacy Act.

Nevertheless, Secure Flight prevailed throughout this series of mishaps and is now the screening system used for all domestic commercial flights. Significantly, Secure Flight is viewed by the public as a scaled-back version of CAPPS II, confined to seeking terrorists as opposed to analyzing all passengers. Like CAPS, the program demands a passenger’s travel information from airlines. Then, Secure Flight automatically compares the information from the airlines to terrorist databases to ensure that the passenger is not on any terrorist list. If the passenger is not on a designated watch list, Secure Flight sends the results back
to the airline to issue the boarding pass. Secure Flight is now generally seen as a more successful version of the CAPS and CAPPs II models because the program only identifies potential names from terrorist watch lists and transfers authority to the TSA to do such screening. Most significantly, its success results from the fact that it does not use commercial data to evaluate a passenger’s risk.

E. Lessons Learned

There are two important legacies arising from the privacy struggles of these past programs that continue to haunt subsequent passenger profiling programs: (1) the European resistance to cooperation; and (2) the public reaction. First, the U.S. government will continue to struggle with trying to share data with the European Union, which has stricter privacy laws than the United States. In 2006, the Court of Justice of the European Union struck down a passenger data sharing agreement that a European Union commission had entered into with the United States. Specifically, the Court found that the commission did not have the appropriate authority to authorize sharing passenger information. The United States and the European Union reached a new agreement that must be passed by European Parliament and that places restrictions on data use. This agreement is important because the reality of the internationally cooperative programs envisioned by organizations such as the International Air Transport Association (IATA) and the International Civil Aviation Organization (ICAO) depends on the ability of countries to negotiate data sharing amongst themselves.

---

83 Improving Pre-Screening of Aviation Passengers, supra note 76, at 5.
84 TSA: Secure Flight Program, supra note 77.
85 Id.
87 Id.
88 Id.
90 See infra Part IV.
Second, and most significantly, it was the response of U.S. citizens that spurred Congress and the Executive Branch to put pressure on the TSA to meet their demands.\footnote{See supra Part I.C.} Americans did not know then, and may not understand even now, that the information they assume is private may be collected by multiple commercial databases. Many Americans were driven by fear, the idea that this information was private, and the thought that the government was acting as “Big Brother.”\footnote{See The Seven Problems with CAPPS II, supra note 59.} In reality, commercial databases of personal information have already been compiled through private companies, such as eBureau.\footnote{See About Us, eBureau, http://www.ebureau.com/about (last visited June 4, 2013).} In fact, the Federal Trade Commission (FTC) has recently announced that it will begin analyzing these “data broker” companies for a greater understanding of their practices, including the “nature and sources” of the information collected; the method by which the companies “use, maintain, and disseminate” the data; and the accessibility of the information to consumers who would like to either correct or opt out of the information collection.\footnote{Press Release, FTC, FTC to Study Data Broker Industry’s Collection and Use of Consumer Data (Dec. 18, 2012), available at http://www.ftc.gov/opa/2012/12/databrokers.shtm.} Perhaps it is because the public was largely unaware of the underlying information collection techniques employed by these brokers that many reacted quite severely to the thought of the government having the information.\footnote{See supra Part I.C.} However, the reality is that similar information sharing occurs in the background of most organizations, including other federal agencies.\footnote{von Rochow-Leuschner, supra note 12, at 148.} Perhaps even more telling is the difference in public pressure toward the ATS as compared with CAPPS II.\footnote{See supra Part I.C.} Particularly, while privacy advocates continue to challenge the ATS with meager success,\footnote{See supra Part III.B–C.} CAPPS II was stopped in its tracks.\footnote{See supra Part I.C.} This illustrates the disconnect in public attitudes toward “important” border-patrol safety measures and the “inconvenient” or “invasive” domestic flight security measures the TSA imposes.
III. AIRLINE PASSENGERS AND THEIR RIGHT TO PRIVACY

While the "right to privacy" is a familiar phrase to most citizens, much confusion remains with respect to which aspects of "privacy" are actually protected and which part of the U.S. Constitution conveys such a right. An element of privacy is seemingly apparent in the First, Third, Fourth, and Fifth Amendments of the U.S. Constitution. While these amendments apply to specific situations in which citizens have a right to be left alone in their affairs, the U.S. Supreme Court has expressly refused to find a "general" or broad right to privacy in the Constitution.

Nonetheless, in a famous dissenting opinion often invoked by privacy advocates arguing for protection against government intrusion, Justice Brandeis declared that the Constitution dictates a "right to be let alone." Through a functionalist analysis of the Fourth and Fifth Amendments to the Constitution, Justice Brandeis recalls the Founders' limited capability to predict technological advances that could constitute a "search" without any physical intrusions. Since then, the Supreme Court has invoked the right to privacy in socially controversial situations, the

---


101 See U.S. CONST. amend. I ("Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech."); id. amend. III ("No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner."); id. amend. IV ("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."); id. amend. V ("No person shall be... compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law.").

102 See Nelson, 131 S. Ct. at 756–57 ("[W]e will assume for present purposes that the Government's challenged inquiries implicate a privacy interest of constitutional significance. We hold, however, that whatever the scope of this interest, it does not prevent the Government from asking certain questions in a background check.").

103 See Privacy & Technology, ACLU OREGON, http://www.aclu-or.org/content/privacy-technology (last visited June 4, 2013).


105 Olmstead, 277 U.S. at 478 ("When the Fourth and Fifth Amendments were adopted... [f]orce and violence were then the only means known to man by which government could directly effect self-incrimination.").
backlash of which has been detrimental to the right’s already fragile existence.\textsuperscript{106} The right to privacy in the context of aviation security’s incorporation of technological advancements is typically subject to the confines of the Fourth Amendment and the Privacy Act.\textsuperscript{107}

A. Fourth Amendment Searches in the Airport Context

The current physical search procedures\textsuperscript{108} prompt most privacy challenges to airport security to invoke the Fourth Amendment.\textsuperscript{109} The Fourth Amendment protects an individual’s right to not suffer unreasonable searches and seizures and “to be secure in their persons, houses, papers, and effects.”\textsuperscript{110} While this language includes mostly tangible property or areas,\textsuperscript{111} the U.S. Supreme Court broadened the scope of this protection in \textit{Katz v. United States}, which overturned \textit{Olmstead} (vindicating Justice Brandeis’s philosophy, some would argue).\textsuperscript{112} The Court held that “the Fourth Amendment protects people” and what they seek to preserve as private, regardless of whether the search was in a public area.\textsuperscript{113} However, the majority clearly expressed that the Fourth Amendment is not a “general right to privacy.”\textsuperscript{114} Courts have subsequently adopted Justice Harlan’s test for

\begin{thebibliography}{99}
\bibitem{107} While a due process analysis is a very worthwhile discussion of risk-based security programs, this comment will not discuss its effect on the PreCheck program because the PreCheck program is, for now, exclusively for low-risk passengers. Therefore, PreCheck is not yet a means to deny travelers a seat on a plane. See \textit{Kite}, \textit{supra} note 52, at 1993 (analyzing due process concerns of Red-coded passengers).
\bibitem{108} Throughout the years, various procedures have been used, including passing through magnetometers, pat-downs, enhanced pat-downs, and, more recently, Advanced Imaging Technology (AIT), such as millimeter imaging machines. See \textit{United States v. Davis}, 482 F.2d 893, 900 (9th Cir. 1973), \textit{overruled by} \textit{United States v. Aukai}, 497 F.3d 955 (9th Cir. 2007); \textit{Advanced Imaging Technology (AIT), TSA}, \text{http://www.tsa.gov/traveler-information/advanced-imaging-technology-ait} (last updated May 21, 2013).
\bibitem{110} U.S. Const. amend. IV.
\bibitem{112} \textit{Katz}, 389 U.S. at 353.
\bibitem{113} \textit{Id.} at 351.
\bibitem{114} \textit{Id.} at 350–51.
\end{thebibliography}
whether a warrantless search violates the Constitution: (1) a person must show “an actual . . . expectation of privacy”; and (2) a person must demonstrate “that the expectation [is] one that society is prepared to recognize as ‘reasonable.”115 While the Fourth Amendment traditionally limited searches to those with warrants, judicially crafted exceptions to the Fourth Amendment have sufficiently eroded this view and have allowed for substantial suspicion-free searches.116

Airport searches typically fall under an administrative exception to the Fourth Amendment.117 Although airport security screenings have passed Fourth Amendment scrutiny under other theories, such as consent,118 reasonableness, or some combination,119 the administrative search exception has recently been more successfully invoked.120 For instance, the Ninth Circuit explicitly stated that airport screenings are administrative since they are a “part of a general regulatory scheme in furtherance of an administrative purpose” that focuses on eradicating potential danger or violence on aircrafts, rather than on providing general crime control.121 Administrative searches, often referred to as “special needs” searches,122 are consistently held constitutional even though they do not require a warrant, as

---

115 See, e.g., Ohio Civil Serv. Emp. Ass’n v. Seiter, 858 F.2d 1171, 1174–75 (6th Cir. 1988); see also Katz, 389 U.S. at 361 (Harlan, J., concurring).
117 United States v. Marquez, 410 F.3d 612, 616 (9th Cir. 2005) (citing United States v. Davis, 482 F.2d 893, 908 (9th Cir. 1973)).
118 While the administrative search exception appears to be the most clear-cut argument, the theory of consent plays a significant role in the Fourth Amendment analysis. In Davis, the Ninth Circuit, through an administrative search analysis, included a requirement that a potential passenger must be able to avoid the search by choosing not to fly. Davis, 482 F.2d at 910, 913. While subsequent courts have expressed that consent is not necessary to validate an administrative search, at least one court has recognized that the consent theory is not an appropriate avenue for upholding airport searches. United States v. Albarado, 495 F.2d 799, 806–07 (2d Cir. 1974); see, e.g., United States v. Biswell, 406 U.S. 311, 315 (1972). The Albarado court found that making a passenger choose between exercising his or her Fourth Amendment right and flying simply amounts to coercion. Albarado, 495 F.2d 799 at 806–07.
119 For an in-depth discussion of the various theories courts have relied upon to uphold the constitutionality of airport screenings, see Reinert, supra note 116, at 208.
121 United States v. Aukai, 497 F.3d 955, 960 (9th Cir. 2007) (quoting Davis, 482 F.2d at 908).
122 Reinert, supra note 116, at 218 (internal quotation marks omitted).
long as they meet certain requirements.\textsuperscript{123} As opposed to a typical search, administrative searches do not require "individualized suspicion,"\textsuperscript{124} but they "must be reasonable."\textsuperscript{125}

The Fourth Amendment standard of administrative airport searches is not always consistent. The Ninth Circuit held that specific airport security screening searches are reasonable under the Fourth Amendment provided they are "no more extensive nor intensive than necessary, in the light of current technology, to detect the presence of weapons or explosives,'" and if they are "'confined in good faith to that purpose.'"\textsuperscript{126}

B. RECENT FOURTH AMENDMENT SCRUTINY OF TECHNOLOGICAL SEARCHES

In \textit{Electronic Privacy Information Center v. U.S. Department of Homeland Security (EPIC v. DHS)}, the D.C. Circuit expressly disagreed with the Ninth Circuit by upholding the constitutionality of the TSA's new Advanced Imaging Technology (AIT) machines.\textsuperscript{127} The standard articulated by the D.C. Circuit was more of a balancing test.\textsuperscript{128} Specifically, whether an administrative search occurred must be determined by weighing "'the degree to which [the search] intrudes upon an individual's privacy and . . . the degree to which it is needed for the promotion of legitimate governmental interests.'"\textsuperscript{129}

The court's reasoning,\textsuperscript{130} or lack thereof, is indicative of the current deferential attitude demonstrated by courts confronted with new forms of technology employed in airport screening. The challenged technology included the X-ray backscatter scan-
ner and the millimeter radio wave scanner.\textsuperscript{131} Both machines were heavily criticized as overly invasive when introduced in 2007.\textsuperscript{132} The public expressed concern about TSA employees observing their naked bodies and about whether the images would be stored.\textsuperscript{133} The court found that the government won the balancing test, due in large part to the particular importance of security.\textsuperscript{134} The court also noted that the TSA had taken certain steps to avoid potential privacy concerns.\textsuperscript{135} Of particular importance to the court was that the passenger had a choice—because he retained the right to refuse the scanners and receive a pat-down,\textsuperscript{136} but this is arguably no choice at all. In its brief opinion, the court did not discuss the underlying reasons why a passenger may feel violated, or whether such feelings were reasonable. Thus, with almost total deference to the government's interest in maintaining security in the skies, the court failed to analyze whether the technology-based body-scan approach was an unreasonable or unnecessary way to achieve passenger safety. \textit{EPIC v. DHS} suggests that the Fourth Amendment will offer little protection to citizens who feel that their privacy has been invaded by technological advancements in airport searches.

\textsuperscript{131} Id. at 3–4.


\textsuperscript{133} Cratty, \textit{supra} note 132.

\textsuperscript{134} \textit{Elec. Privacy Info. Ctr.}, 653 F.3d at 10.

\textsuperscript{135} \textit{Id.} The TSA has taken further steps to improve privacy due to a congressional mandate. The millimeter wave machines have new software installations that eliminate the individual's actual image, replacing it with a general human outline containing illuminations where problem areas may exist. TSA: \textit{AIT: Privacy}, TSA, http://www.tsa.gov/ait-privacy (last visited June 4, 2013). Notably, the TSA appears committed to these initiatives, and it has now ordered removal of the backscatter machines because the companies could not formulate similar software in time. Jeff Plungis, \textit{Naked-Image Scanners to Be Removed from U.S. Airports}, BLOOMBERG (June 4, 2013), http://www.bloomberg.com/news/2013-01-18/naked-image-scanners-to-be-removed-from-u-s-airports.html.

\textsuperscript{136} \textit{Elec. Privacy Info. Ctr.}, 653 F.3d at 10.
C. THE PRIVACY ACT AND CHALLENGES TO PASSENGER PROFILING SYSTEMS

Due to claims that public notice of the specific criteria considered in determining individual passengers' risk levels would make airports and aircraft more vulnerable to terrorists, an ongoing struggle exists between electronic searches, the files they create, and the Privacy Act of 1974 (Privacy Act). The Privacy Act requires federal agencies to publish in the Federal Register a description of each system of records that the agency maintains, including the character and categories of information. The agency must also describe the uses of the information. The purpose of this mandate is to protect individual privacy so that each individual better understands how his or her information is being used and has the opportunity to correct any inaccuracies.

EPIC v. DHS recently held that to bring a claim under the Privacy Act, an individual must demonstrate that a specific retrieval of personal data occurred—one cannot simply offer evidence that the agency had the capability to retrieve such data. In that case, the fact that EPIC could prove that the AIT machines were still capable of saving images (and indeed had done so for training purposes) was insufficient; the D.C. Circuit required the plaintiff to show that the TSA actually created and maintained images of specific individuals, which a traveler has no practical way of discovering.

The Privacy Act expressly articulates various reasons why agencies may exempt certain records systems. When the DHS finally published a Notice of Record Keeping for the ATS, it simultaneously filed a proposed rulemaking stating that most of the information files collected would be exempted from the Privacy Act because of criminal, civil, and administrative en-

---

138 Id. § 552a(e)(4).
139 Id.
140 Henke v. Dep't of Commerce, 83 F.3d 1453, 1456 (D.C. Cir. 1996) (citing 5 U.S.C. § 552a(d)(2)).
142 Id. at 8–10.
143 See 5 U.S.C. § 552a(j)–(k).
The announcement of the final rule ignored protests by privacy advocates and successfully barred individuals from learning the substance of such records. Likewise, the TSA followed suit by publishing in the Federal Register its Notice of Proposed Rulemaking to exempt its Secure Flight records from the Privacy Act; this Notice ultimately became a final rule.

Lawsuits have challenged the ability of government agencies to exempt themselves from Privacy Act liability; however, there remains a split in authority. Recently, the Sixth Circuit, in Shearson v. Department of Homeland Security, joined the D.C. Circuit in holding that government agencies do not have an absolute right to exempt their records under the Privacy Act. These two courts have offered litigants at least a chance to challenge government security agencies and their authority under the Privacy Act.

IV. TSA'S NEWEST RISK-BASED APPROACH TO SECURITY: PRECHECK

A. INTERNATIONAL AVIATION OBJECTIVES

A current goal of international aviation, termed the "Checkpoint of the Future," seeks to create a scenario where passengers will have a nonstop walk from their cars until they board a plane. According to Tony Tyler, Director General and CEO of

149 Compare Alexander v. United States, 787 F.2d 1349, 1351-52 (9th Cir. 1986), and Kimberlin v. Dep't of Justice, 788 F.2d 434, 436 n.2 (7th Cir. 1986), and Ryan v. Dep't of Justice, 595 F.2d 954, 958 (4th Cir. 1979), with Shearson, 638 F.3d at 504, and Doe v. FBI, 936 F.2d 1346, 1352-53 (D.C. Cir. 1991).
150 See Doe, 936 F.2d 1346.
151 Shearson, 638 F.3d at 504.
IATA, the Checkpoint of the Future is a risk-based and intelligence-driven approach to airport security, rather than a “one-size-fits-all” approach. According to the Checkpoint Roadmap published by IATA, “[u]ninterrupted passenger flow” and “[s]creening based on risk assessment” should be in place by the year 2020. More immediately, the 2014 Roadmap includes the following goals for risk assessment: “use of passenger data” to prescreen travelers; “[c]over and overt behavior analysis techniques”; trusted traveler programs; separate checkpoint systems; and methods to minimize random prerequisites. Essentially, the international aviation goal is to replace physical security screenings with a prescreening of each individual’s risk through analysis of provided information.

This new goal brings a new challenge—privacy concerns. The Checkpoint of the Future, as Tyler concedes, will require “fuller use of passenger information” but not “the [forced] collection of more information”; the program will “only [give] better effect to the information that is already mandated by governments . . . [and] supplement[ the information] with voluntary ‘known traveler’ programs.” The passenger data Tyler refers to is obtained “for border control purposes,” which is currently very different from data collected for U.S. domestic flights or general security purposes. Of utmost significance is the fact that CBP uses commercial and law enforcement data, which domestic
flights, through Secure Flight, expressly do not have congres-

sional authority to use.\textsuperscript{161}

While Tyler claims the expanse of passenger data use “is not a
show-stopper,”\textsuperscript{162} he admits it is a “sensitive subject”\textsuperscript{163} that “will
require legislative change in many [s]tates.”\textsuperscript{164} However, Tyler
cites “‘known traveler’ programs” as a definitive step toward the
Checkpoint of the Future,\textsuperscript{165} including the CBP’s Trusted Traveler Programs and the TSA’s new PreCheck program.\textsuperscript{166}

CBP has in place several Trusted Traveler Programs, which
“provide expedited travel for pre-approved, low risk travelers
through dedicated lanes and kiosks.”\textsuperscript{167} CBP created Global En-
try for pre-approved frequent international travelers who agree
to a $100 fee,\textsuperscript{168} a “rigorous background check[,] and [an] inter-
view.”\textsuperscript{169} During the interview, the passenger is asked questions,
has his or her picture taken, and is asked to give biometric infor-
mation, such as fingerprints or iris scans.\textsuperscript{170} Although the eligi-
bility requirements are unknown, the website lists several factors
that result in guaranteed ineligibility, such as “provid[ing] false
. . . information,” “hav[ing] been convicted of any criminal of-


cence,” or more broadly, failing to “satisfy CBP of their low-risk
status (e.g. CBP has intelligence that indicates that the applicant
is not low risk; [or] CBP cannot determine an applicant’s crimi-
nal, residence or employment history).”\textsuperscript{171} Despite the unclear
application guidelines, Global Entry has been popular: the CBP

\begin{footnotes}
\footnote{See supra Part II (comparing the ATS with Secure Flight).}
\footnote{Tyler, supra note 154.}
\footnote{Id.}
\footnote{IATA, CHECKPOINT OF THE FUTURE EXECUTIVE SUMMARY 7 (last visited June
4, 2013), available at \url{http://www.iata.org/whatwedo/security/Documents/COF-
Concept-Definition-Executive-Summary.pdf}.}
\footnote{Tyler, supra note 154 (internal quotation marks omitted).}
\footnote{Mayerowitz, supra note 160.}
\footnote{Trusted Traveler Programs, CBP, \url{http://www.cbp.gov/xp/cgov/travel/
trusted_traveler/} (last visited June 4, 2013). The website lists the included pro-
grams: Global Entry, NEXUS, SENTRI, and FAST: Free and Secure Trade Pro-
gram. Id.}
\footnote{Stephanie Rosenbloom, \textit{Speedy Airport Security, Should You Apply?}, N.Y. TIMES
(Oct. 3, 2012), \url{http://travel.nytimes.com/2012/10/07/travel/speedy-airport-se-
curity-should-you-apply.html?ref=airportsecurity&_r=0}.}
\footnote{About, GLOBAL ENTRY, \url{http://www.globalentry.gov/about.html} (last visited
June 4, 2013).}
\footnote{How to Apply, GLOBAL ENTRY, \url{http://www.globalentry.gov/howtoapply.html}
(last visited June 4, 2013).}
\footnote{Eligibility, GLOBAL ENTRY, \url{http://www.globalentry.gov/eligibility.html} (last
visited June 4, 2013).}
\end{footnotes}
has “receive[d] 25,000 to 30,000 applications [per] month.”¹⁷² Notably, the number of Global Entry applicants is likely to increase because entry into that program leads to automatic qualification for the TSA’s domestic PreCheck program.¹⁷³

B. TSA PreCheck

In accordance with international aviation security goals, the TSA has been preparing to shift toward a more risk-based approach to security measures. For example, the TSA is relying on biometrics;¹⁷⁴ PreCheck; an expanded Behavior Detection Pilot;¹⁷⁵ and decreased screening for passengers who are “75 and older,” “12 and under,” and “[a]ctive [d]uty U.S. Service Members.”¹⁷⁶ However, PreCheck is the risk-based program that the TSA is making the most noise about.¹⁷⁷

PreCheck is a program that allows “expedited screening” at airport checkpoints for enrolled passengers who are willing to provide the TSA with personal information and undergo a risk assessment based on the provided information.¹⁷⁸ Although entitlement to expedited screening will be granted when a PreCheck member books his or her flight, the passenger will not be aware of the assessment results because the approval will be “embedded” in the boarding pass’s barcode.¹⁷⁹ Crucial to the integrity of the program is the principle that a member should be subject to “random, unpredictable security measures” and should not know whether he or she will receive expedited

¹⁷² Rosenbloom, supra note 168.
¹⁷³ Id.
¹⁷⁶ Risk-Based Security Initiatives, TSA, http://www.tsa.gov/traveler-information/risk-based-security-initiatives (last visited June 4, 2013). In addition, the TSA has recently announced that it will allow passengers to bring pocketknives, box cutters, and limited sports equipment on the plane, crediting its decision as part of a risk-based initiative. Mike M. Ahlers, TSA to Allow Pocketknives, Some Sports Equipment, CNN (Mar. 5, 2013, 6:36 PM), http://www.cnn.com/2013/03/05/travel/tsa-carry-on-changes/index.html.
¹⁷⁸ TSA Pre✓™ How It Works, supra note 14.
¹⁷⁹ Id.
screening on any given trip. When the member presents his or her boarding pass to a TSA employee, the employee will send that member to either the full-security lane or a special PreCheck queue, as instructed by the barcode. The expedited screening offered in the PreCheck line may include allowing passengers to keep shoes, light jackets, and belts on, and keep liquid "3-1-1 compliant bag[s] . . . [and] laptop[s]" in carry-ons. PreCheck is not for everyone. In fact, PreCheck is currently only available to certain CBP Trusted Travelers and frequent flyers of specific airlines. Global Entry participants and members of Trusted Traveler Programs such as NEXUS and SENTRI are allowed to enroll in PreCheck, subject to eligibility. Alternatively, only frequent fliers on the following airlines are currently offered membership in the program: Alaska Airlines, American Airlines, Delta Air Lines, Hawaiian Airlines, United Airlines, US Airways, and Virgin America.

As the TSA hoped, PreCheck has grown to be quite popular among the public, easily meeting the program’s milestones to date. The TSA successfully met its 2012 goal, with PreCheck “now available in 35 airports.”

---

180 Id.
181 Id.
182 Id.
184 NEXUS is a program for registered, prescreened travelers who will experience expedited screening at the border of the United States and Canada; many members are Canadian citizens. See Nexus Program Description, CBP, http://www.cbp.gov/xp/cgov/travel/trusted-traveler/nexusprog/nexus.xml (last visited June 4, 2013).
185 SENTRI is the Mexican border counterpart to the NEXUS program discussed above, except the TSA does not allow Mexican citizens to enroll in PreCheck as of January 2013. See Sentri Program Description, CBP, http://www.cbp.gov/xp/cgov/travel/trusted_traveler/sentri/ (last visited June 4, 2013).
187 TSA Pre™ Expedited Screening, supra note 13.
growth is also indicated by the fact that the TSA had already screened 3 million passengers by September 2012. PreCheck is even the subject of marketing for businesses. For example, Loews Hotels & Resorts, with others soon to follow, has offered its loyalty rewards customers the payment of PreCheck’s $100 application fee to ease their travel experience. The program’s success is important because, according to TSA leadership, it is indicative of the future move toward the IATA’s goal of achieving a risk-based intelligence structure. According to TSA Administrator John Pistole, PreCheck strengthens security because the TSA’s “ability to find the proverbial needle in the haystack is improved every time [it is] able to reduce the size of the haystack.”

As with all previous programs, critics point out the potential failings of PreCheck and, in a broader context, all Trusted Traveler Programs. Privacy advocates are zealously attacking such programs as ineffective and dangerous to privacy, even though they are currently voluntary.

First, similar to the ATS and Secure Flight, the TSA has exempted Registered Traveler files from the Privacy Act. The rationale for this exemption is that “disclosure would also permit the individual who is the subject of a record to impede the program suitability determination.” As discussed above, concerns generally arise from the secrecy involved in judging an individual’s risk without allowing access to the information used to judge such risk. Considering PreCheck functions to benefit

---


190 TSA Pre✓ Hits 3 Million Mark, supra note 188.
191 Rosenbloom, supra note 168.
192 Id.
193 Roger Yu, TSA Tests 'Pre-Screening' of Select Passengers at 4 Airports, USA TODAY (Oct. 4, 2011), http://travel.usatoday.com/flights/story/2011-10-04/TSA-tests-pre-screening-of-select-passengers-at-4-airports/50660780/1. “[PreCheck] is designed to test a possible shift to a method of screening of passengers that relies more on intelligence and a risk-assessment of travelers.” Id.
194 Pistole, Remarks to the National Press Club, supra note 177.
195 Stanley, TSA Once Again Considering Using Commercial Data to Profile Passengers, supra note 17.
197 See TSA Exempts Registered Traveler Files from Disclosure, 82 No. 24 INTERPRETER RELEASES 1002, 1003 (June 13, 2005) [hereinafter Immigration Report].
198 See supra Part III.D; see also Kite, supra note 52, at 1434 (discussing due process implications).
mainly "low-risk" passengers without forcing any individual to forfeit his ability to fly, the exemption alone did not initially raise concerns. But the DHS recently announced that it is adding a new watch list to its Secure Flight list—a watch list cultivated from none other than those disqualified from PreCheck.

Second, privacy advocates argue that this will create a two-tier class of passengers that could lead to a slippery slope of discrimination against minorities. Third, there are concerns that the cost expended will not be worth the benefit received, a lesson learned from previous failures. These concerns may be correct, because a fourth criticism centers around a security failure that has already occurred. Specifically, TSA has not properly encrypted the bar code that determines whether a passenger receives expedited screening for a particular flight. Therefore, simple computer programs could de-code and essentially give someone a free pass through security.

C. PreCheck's New Announcement for Private Information Gatherers

The final and most significant concern stems from a recent announcement that the TSA will incorporate commercial data into its assessments under the PreCheck program. The TSA released a Market Research Announcement that sought bids from private third-party companies to create a system that can

---

199 TSA Pre✓ How It Works, supra note 14.


201 Stanley, TSA Once Again Considering Using Commercial Data to Profile Passengers, supra note 17.


204 Id.

205 Stanley, TSA Once Again Considering Using Commercial Data to Profile Passengers, supra note 17.

206 TSA Third Party Pre-screening, FEDBizOPPS.GOV (Jan. 8, 2013, 4:52 PM), https://www.fbo.gov/index?s=opportunity&mode=form&id=5f3d932eeef30941d0fc945a5c14346f&tab=core&_cview=0.
assess risk for the PreCheck program using a private source of commercial data. Particularly, the TSA is interested in evaluating techniques that use "non-governmental data elements to generate an assessment of the risk" while the "TSA [specifies] a few common core requirements for process and algorithm content."

V. CAN PRECHECK SURVIVE IN A POST-CAPPS II AMERICA?

In the words of TSA Administrator Pistole, "For the first time since 9/11, I think we have the conditions where it might be politically possible to have a serious debate about" risk-based intelligence assessments of travelers. First, does Mr. Pistole know something that the public does not? Part II of this comment analyzed government-implemented risk-based and profiling systems from the past decade, and it revealed that each system was met with continuous public resistance. The list of systems discussed was limited due to the exclusion of the private prescreening systems that have floundered and failed for years. Second, why would travelers feel more ready to "discuss" risk-based, intrusive measures now, when the fear of terrorists hijacking planes is likely at its lowest point since 9/11? To answer this question, one must analyze more than just the PreCheck program. PreCheck must be framed by its predecessors and by the unique result of a decade of struggle between security and liberty, where the strength of law is unknown and is often superseded by the overwhelming authority of the U.S. government in combating terrorism.

---

207 See id.
208 Id. The elements required by the TSA include full legal name, gender, date of birth, and the prospective enrollee's waiver to search various commercial databases. Desirable elements include current address, most recent past address, current employer, names used in the past, Social Security number, positive identity verification, and images on identification provided by the PreCheck enrollee. Id.
210 See supra Part II.
211 One example is a program called Clear; it had financial troubles and an extraordinary problem with data protection in the hands of failed management. Bankruptcy of Verified Identity Pass and the Privacy of Clear Registered Traveler Data, EPIC, http://epic.org/privacy/airtravel/clear/ (last visited Oct. 28, 2013). The company experienced bankruptcy, an immediate closing of its doors, and stolen passenger information. Id.
212 See, e.g., Kite, supra note 52.
A. **PreCheck + Secure Flight + Commercial Data = CAPPS II Reincarnated**

It is fair to say that the public is ready to discuss PreCheck. It is a typically well-liked program\textsuperscript{215} because of the convenience associated with membership. But one must actually break down what it accomplishes.\textsuperscript{214} Today, PreCheck is more or less a voluntary background check that the government runs on travelers—using information provided by individual travelers—to confirm that they are who they say they are.\textsuperscript{215} Additionally, PreCheck is a “positive” profiling experience because it allows passengers to reap benefits from leading scandal-free lives. The individual traveler, as a responsible citizen, has a sense of control over the process. He chooses to let the TSA deem him “safe” to fly.

There are additional relevant facts, though. For instance, the DHS will place an individual on a watch list should he somehow not appear to be as “low-risk” as when he originally applied for the PreCheck program.\textsuperscript{216} Couple that issue with the reality that he would then have a difficult, if not impossible, time trying to determine which piece of data from his past landed him on such a list.\textsuperscript{217} The potential movement toward including commercial data in the evaluation process\textsuperscript{218} would place the passenger at a loss because the TSA could have based its decision on an endless amount of unknown data not limited to information that he provided. What does the TSA think is so risky about this potential traveler? Suddenly left in the dark about his own ability to fly, this potential traveler may ultimately regret ever volunteering his information to the TSA for mere convenience.

CAPPS II never came to life for two main reasons: (1) the public, led by the Legislative and Executive Branches, was not comfortable with the government’s reliance on ordinary law enforcement and commercial data to evaluate them; and (2) the use of a computerized system to assign one of three levels of risk to all traveling citizens invoked fears of due process and other constitutional violations.\textsuperscript{219}

\textsuperscript{215} TSA Pre✓\textsuperscript{TM} Hits 3 Million Mark, supra note 188.
\textsuperscript{214} See Rosenbloom, supra note 168.
\textsuperscript{215} Id.
\textsuperscript{216} Sternstein, supra note 200.
\textsuperscript{218} See TSA Third Party Pre-screening, supra note 206.
\textsuperscript{219} See, e.g., Kite, supra note 52.
simply translated to an “overreach[ing] of intelligence”; the public was not ready to accept the idea that its government would have the type of power it perceived in CAPPS II’s capabilities. Passengers would no longer have choices or control over whether they even wanted to be rated “safe” by their government.

How is current aviation security different than that proposed by CAPPS II? The TSA’s recent announcement exhibits the likelihood that commercial databases, so forcefully rejected before, will be considered yet again. And even though citizens are no longer automatically grouped into three categories, as CAPPS II proposed, they will be grouped just that way for all practical purposes. The TSA promotes PreCheck’s expansion to all eligible passengers, not just frequent flyers of particular airlines. Additionally, the IATA’s goals stem from the same desire for expansion. Therefore, in a matter of years, the TSA plans for many individuals with clear backgrounds to be deemed “low-risk” in the TSA’s view, minimizing the “haystack” that Pistole alluded to. Also, the “high-risk” passenger group compiled by Secure Flight will be comprised of those who exhibit risky characteristics or were rejected from the PreCheck program. Lastly, passengers whose risk level is described as “average” or “unknown” will include individuals who either do not fly regularly or do not meet the unknown “safe” requirements necessary to be categorized as low-risk. An individual, for all practical purposes, will be a member of one of these three groups. Do the CAPPS II colors of Red, Green, and Yellow come to mind? This comparison is made to point out that the TSA PreCheck program may ultimately fulfill the goals of the failed CAPPS II.

With proper perspective, it is clear why there will be difficulties in assessing the constitutionality of PreCheck and the “Checkpoint of the Future” initiatives in general. CAPPS II cer-

---

220 Fiske, supra note 39, at 184.
221 See TSA Third Party Pre-screening, supra note 206.
222 Fiske, supra note 39, at 184.
223 See Stellin, supra note 209.
224 See TSA Pre✓™ Hits 3 Million Mark, supra note 188.
225 See, e.g., DeGrave, supra note 46, at 140–44.
226 See Fiske, supra note 39, at 183 (describing the CAPPS II color-coded levels as Green for “low-risk”; Yellow for average or unknown risk; and Red for “high-risk” and potential no-fly orders).
227 Pistole, Remarks to the National Press Club, supra note 177.
tainly invoked legal challenges, but was stopped in its tracks only by political pressures, not constitutional hurdles.

B. FOURTH AMENDMENT SCRUTINY

To hold that the prescreening capacity of PreCheck is an unconstitutional search under the Fourth Amendment, a court must first ask whether it is a search as intended under the Fourth Amendment. Therefore, under the Katz analysis, a court would look to (1) whether an individual has an actual expectation of privacy, and (2) whether society recognizes that expectation as reasonable. This would potentially be the first hurdle for any challengers because, as long as PreCheck is voluntary, a court will likely find that a person would not be able to show an actual expectation of privacy. However, to the extent that another program invokes commercial databases, as PreCheck has suggested it may, a passenger may very well expect that particular details of his financial situation would not become knowledge of the TSA simply because he chooses to fly. As PreCheck stands now, however, it will likely not even constitute a search worthy of constitutional protection under legal precedent.

Even if PreCheck, or any other risk-based program, is indeed a search, it would likely fall into one of the exceptions carved from the Fourth Amendment’s ban on warrantless searches. First, to the extent that PreCheck remains voluntary, courts will undoubtedly uphold the program due to the consent exception. Furthermore, even if PreCheck became a mandatory screening program, a court still might hold that a passenger consented because he had a choice to not fly. Courts have yet to recognize the right of an individual to choose to travel by plane. While there is a valid due process issue in that assumption, it is sufficient to say that passengers likely have no claims under the Fourth Amendment.
While technology has made the nature of a search completely different than any of our Founding Fathers could have imagined, the core reasoning behind PreCheck’s electronic searches is parallel to the goal of physical searches: to alleviate the dangers of flying. Therefore, just like its predecessor, AIT imaging, PreCheck’s informational searches will likely fall squarely into the administrative search exception, under either of the standards courts currently use. If passenger prescreening is categorized as an administrative search, a court will likely find that it falls within the confines of the Fourth Amendment. Particularly in light of the deference given by the court in EPIC v. DHS, it seems that the government’s interest in securing the nation against terrorists will overcome almost any level of intrusiveness on the government’s part.

Ultimately, the Fourth Amendment precedent sets up an extremely low hurdle for the TSA in crafting search techniques. The administrative search exception, the consent exception, and the strong governmental interest in security effectively create an atmosphere where almost any government action is constitutionally acceptable. As technology advances, it is becoming less appropriate to gauge the propriety of potentially serious invasions under the Fourth Amendment. While judges have expanded the Fourth Amendment’s literal language to mean more than the Framers likely contemplated, there is no indication that the Fourth Amendment and its precedential standards are flexible enough to accommodate the intricate details of complex data sharing systems or to overcome the huge governmental interest in safety. If the judicial test is a balance, the government will always win in court.

Importantly, however, Congress is a political body with the ability to codify a stricter definition of privacy that ideally cap-

---

236 See supra Part III.
237 Id.
238 An issue that is beyond the scope of this comment is the potential for the government to find misleading or false documents that do not affect aviation security but could be used as evidence for another crime. While physical evidence (i.e., drugs) has been routinely collected in physical airport screening despite its “administrative goals,” it would be interesting to examine whether an informational search could also recover and use such information against the traveler for purposes such as aiding the IRS in determining whether an individual has committed tax fraud.
240 Id.
tures the Fourth Amendment’s spirit in today’s evolving world. As mentioned above, the FTC is currently studying commercial databases to better understand the industry.\(^\text{241}\) As the public becomes more aware of the information collected about them, travelers should decide whether they feel comfortable with the TSA evaluating them based on this and other unknown information. Considering the public’s discomfort with prior profiling programs, citizens should recognize the constitutional weakness of the Fourth Amendment and express political concerns to their congressmen, as Congress is where the only available solution lies.

C. THE PRIVACY ACT’S WEAKNESSES

While the Privacy Act was originally intended to protect the rights of citizens from a government that maintains secret records of them, its ambiguous application with respect to passenger screening systems and aviation security in general is concerning. Allowing the Privacy Act to be easily circumvented through its exceptions, like many courts have done for the sake of fighting terror, shows that our society is still consumed by fear. Under the current standard, for up to forty years, citizens have either no right or a very limited right to know what records the DHS may keep about them.\(^\text{242}\)

Applied to electronic searches, it is significant that the ATS went unreported in the Federal Register for years before CBP found it necessary to make it public.\(^\text{243}\) This is directly contrary to the Privacy Act’s requirements and ideals.\(^\text{244}\) Additionally, the multiple cases challenging the TSA for AIT images and records have consistently failed and, through judicial line-drawing, have created an extremely high burden for any individual seeking to challenge such policies.\(^\text{245}\) If a traveler is denied PreCheck status or placed on a watch list as a result of being disqualified from PreCheck, he or she has no practical ability under the Privacy Act to seek his or her records because the TSA is exempt from

\(^{241}\) See Stanley, *TSA Once Again Considering Using Commercial Data to Profile Passengers*, supra note 17.

\(^{242}\) Sniffen, *supra* note 23.

\(^{243}\) Id.

\(^{244}\) *Privacy Program*, FDIC, www.fdic.gov/about/privacy/requirements.html (last visited June 4, 2013).

revealing the criteria relied on to assess that traveler. Specifically, an individual traveler will not be able to prove that there is a record kept about them because the TSA does not have to reveal that information.

If the Privacy Act were enforced by courts in challenging such search techniques, perhaps privacy advocates and the general public would be more open to a risk-based system because it would be more transparent. More simply, if courts exercised a more balanced approach to reviewing exemptions claimed by agencies and allowing individuals to more easily bring claims against the agencies, then privacy advocates would feel safer trusting the agencies to reasonably assess risk because they would know that there will be some transparency to the process. Considering the immense resistance intelligence agencies would likely launch at such a proposal, this seems like an unlikely route.

VI. CONCLUSION

As Senator Feingold predicted one month after 9/11, citizens have become driven by fear of terror to the extent that important personal liberties can easily be overlooked. With a proper perspective of PreCheck and the laws under which it would be scrutinized, it is easy to see that the TSA will likely be able to implement almost any measures it feels necessary to ensure safe air travel. However, the single most effective factor in curbing potential privacy issues in the past was the public's reactions to such proposals. Specifically, CAPPS II was stopped before it ever started due to public resistance and government officials' reactions to such resistance.

It is significant that although the ATS employs more invasive and private techniques than CAPPS II ever proposed and operated in secret for years before complying with the Privacy Act,
the ATS is still in use.\textsuperscript{253} Perhaps the difference in public reaction can be described by the disparity between the number of international and domestic travelers. Lower numbers of affected people would inevitably result in less resistance. However, the main reason is likely attributed to the much broader powers granted to CBP. Individuals know from an early age, whether from personal experience, the news, or CIA-themed movies, that crossing a national border immediately warrants the provision of identification to state officials. But until 9/11, it was not the domestic practice to extensively search individuals who fly commercially.

Is the public ready for a discussion about risk-based security? Perhaps. If the public is still afraid and outraged at the idea of commercial databases and secret risk scores, it will likely resist this concept. But what about desensitization to these issues? How many Americans simply accept that nothing they do is private anymore due to exposure to social media and targeted internet advertisements? Could the span of eight years really dull the outrage the traveling public felt toward CAPPS II? Desensitization will surely occur as more people opt to join PreCheck and other known traveler programs. This result is inevitable due to the way that the TSA has framed PreCheck: a voluntary, convenient, minimally invasive, “positive” profiling program that will help passengers save time and prevent aggravation. This shift from negative to positive profiling has helped the popularity of risk-based security tremendously. Meanwhile, many of the impressed individuals will be unwittingly handing the TSA their waiver to perform exactly the type of search that appalled them under CAPPS II.

Many travelers have and will continue to trade information for relief from the inefficiencies of today’s security processes. The questions that members of the public really need to ask themselves are (1) how much they understand about the process; (2) what value they place on the potential privacy implications of these measures; and (3) what benefits they believe will result, whether it be efficiency or security. Ultimately, political responses to such measures will be the only practical means of scaling back such policies in light of the courts’ failure to do so.

\textsuperscript{253} See Privacy Impact Assessment, \textit{supra} note 32, at 9.