Journal of Air Law and Commerce

Volume 69 | Issue 1 Article 6

2004

CAPPS II and the Fourth Amendment: Does It Fly

Rochow-Leuschner Deborah von

CAPPS II AND THE FOURTH AMENDMENT: DOES IT FLY?

DEBORAH VON ROCHOW-LEUSCHNER*

I. INTRODUCTION

THE WORST international terrorist attack ever—involving four separate but coordinated aircraft hijackings—rocked the United States on September 11, 2001. Suicidal terrorists used the aircraft as guided missiles to kill thousands of victims. The 19 hijackers, all young men of Middle-Eastern descent, are believed to have belonged to the al-Qaeda terrorist network.[1] The al-Qaeda network is alive and well, comprised of thousands of members operating in at least 62 countries. The network's goal is to fight a "holy war," or jihad, against the United States and the western world with the intent to destroy it.[2] To such terrorists, commercial aircraft are prized as convenient and dramatic weapons of mass destruction.

Hijackings have plagued the airlines since the beginning of civil aviation.[3] Hundreds of hijackings and bombings have resulted in thousands of deaths around the world.[4] Such incidents were more common prior to the installation of baggage screening detectors.[5] Before that fateful September 11th day, the air-

* J.D., George Mason School of Law. The author has worked in the airline industry since 1989.

[1] Biohazard News, *Profile: Al-Queda, The Osama bin Laden Terrorist Network, at* http://www.biohazardnews.net/binladen.shtml (last visited Jan. 20, 2004).

[2] *Id.*

[3] Between 1949 and 1985 alone, there were 498 successful and 281 failed hijacking attempts worldwide, and 1539 persons killed in eighty-seven aircraft bombings. *See* Michael S. Simons, *A Review of Issues Concerned with Aerial Hijacking and Terrorism: Implications for Australia's Security and the Sydney 2000 Olympics*, 63 J. AIR L. & COM. 731, 738 (1998). Also for extensive information on fatality rates for more than 100 airlines around the world see Airsafe.com, most requested information *at* www.airsafe.com (last visited Jan. 20, 2004).

[4] Simons, *supra* note 3, at 738.

[5] The metal detectors and security screenings we take for granted are a recent development. Such security measures were viewed as a threat to individual pri-

line strategy for hijackings involved obsequious compliance with hijacker demands. Obviously this technique no longer works on suicidal killers. The government and the airlines are currently struggling to protect the public from a new breed of hijackers that expect to die along with their victims.

Today's terrorists may be armed with plastic weapons, anthrax, explosives so small they can fit in the heel of a sneaker, and more. With fervor and lack of concern for self-preservation, would-be hijackers could even overtake a flight with no weapons at all. Thus, the traditional magnometer screening is losing its effectiveness.

El Al, Israel's airline, receives daily threats, yet its tight security has prevented terrorist attacks for over thirty years.[6] In essence, El Al's security system works from the assumption that every passenger is a threat, and treats him or her accordingly. Every passenger is scrutinized and questioned. El Al agents use phone

---

vacy, much as CAPPS II is today. "On February 17, 2002, the Federal Aviation Administration (FAA) was substantially reorganized under Public Law 107-71, the Aviation and Transportation Security Act (ATSA). On that date, the Transportation Security Administration (TSA) assumed all of the FAA's Civil Aviation Security functions, including aviation security research and development." The TSA managed to hire 44,000 new federal employee airport screeners in a matter of months. John H. Marburger III, Statement before the Committee on Science, U.S. House of Representatives (June 24, 2002), *at* http://www.house.gov/science/hearings/full02/jun24/marburger.htm.

[6] Stacy Perman, *The El Al Approach: A Look at the Israel Airlines Security Procedures*, Business 2.0 (Nov. 2001), *available at* http:www.business2.com/articles/mag/0,1640,17508, ff.html. Each passenger is psychologically evaluated. Carry-on bags are checked multiple times. Every car that enters Ben Gurion International Airport in Tel Aviv is examined. Plain-clothed guards help secure each airport building. Passengers are asked a series of specific questions including, "Who paid for your ticket?," "What is the purpose of your travels?," and "When did you book the flight?" The questions are designed to evoke an observable reaction. Officers carefully scrutinize the passengers' answers for tone of voice, body language, and quickness of response. If the passenger gives unsatisfactory answers, a different officer will ask the passenger more questions. Security personnel might also separate flight companions to make sure that their stories match. A psychological evaluation of the passenger is combined with information about the passenger previously obtained by El Al and Interpol.

El Al is also strict with luggage requirements. All luggage goes through a decompression chamber designed to trick bombs that are set to go off when the barometric pressure indicates that the plane is in the sky. X-ray technology detects liquid explosives. Security personnel examine every piece of carry-on luggage and all luggage is also matched to its owner. On layover stops, passengers must reclaim their luggage. Samidh Chakrabart & Aaron Strauss, *Carnival Booth: An Algorithm for Defeating the Computer Assisted Passenger Screening System*, 7 FIRST MONDAY 10 (Oct. 2002), *at* http://www.firstmonday.dk/issues/issue7_10/chakrabartv#note34.

contact or references in Israel to verify the passenger's identity or purpose for the trip. Strip searches are fairly routine. Every piece of luggage is both electronically and hand inspected.

Still, American flag carriers transport more people in two days than El Al does in a year. It is impracticable to implement invasive, expensive security procedures similar to those of El Al for every one of more than 600,000,000 passengers traveling annually.[7] Further, the vast majority of airline travelers are law-abiding citizens and should not be subjected to intrusive physical searches or interrogations like common criminals. If the United States government strips Americans of essential liberties as a result of September 11th, it is assisting the terrorists in their goal of destroying "America the free." There needs to be a better way to prevent known and suspected terrorists from ever getting another chance to use American aircraft as weapons of mass destruction.

II. JUSTIFICATIONS FOR THE COMPUTER ASSISTED PASSENGER PRE-SCREENING SYSTEM II

In the aftermath of the September 11th attacks, the Transportation Security Administration (TSA) was founded in 2001 as a division of the Department of Homeland Security.[8] Its mission is to protect the nation's transportation systems. The Computer Assisted Passenger Pre-Screening System II (CAPPS II)[9] is an automated screening system authorized by Congress as part of the TSA Enabling Act.[10] It is a threat assessment tool, with an emphasis on prevention, based on continuously changing intelligence information.[11] The TSA claims that CAPPS II will enhance aviation security, refine the passenger secondary

---

[7] In 2001, 622 million passengers boarded 8.8 million U.S. airline flights. Bureau of Transportation Statistics, Decline in Airline Passengers in 2001 Ends 10-year Growth, BTS Year-End Report Shows (May 2002), *at* http://www.bts.gov/PressReleases/2002/bts011_02.html.

[8] *See supra* note 6.

[9] The TSA selected Lockheed Martin Management and Data Systems to build CAPPS II. Transportation Security Administration Briefing Room, Press Release, TSA Selects Lockheed Martin Management and Data Systems to Build TSA Passenger Pre-Screening System (Feb. 2003), *at* www.tsa.gov/public/display?content=248.

[10] Description of CAPPS II as stated on the TSA website. *Id.*

[11] *Id.*

screening selection process, and improve airport passenger flow.[12]

Under CAPPS II, airline personnel will be required to electronically submit each passenger's name, address, and telephone number to the TSA prior to issuing a boarding card.[13] Although current regulations require passengers to present photo identification to the agent, there is currently no way of verifying the authenticity of the ID. The TSA's main computer is linked to various law enforcement and commercial databases.[14] First, the TSA will confirm the identities of passengers and identify known foreign terrorists or persons with terrorist connections.[15] Then, it will perform criminal and credit checks on each person. Through the use of sophisticated data-mining algorithms, it will also analyze patterns of travel, purchases, and a variety of other undisclosed classified factors.[16] The factors that CAPPS II will analyze will remain classified information in order to prevent terrorists from learning how to undermine the screening process.

From all this information, the TSA will assess whether an individual poses a potential threat, or appears harmless and "rooted in the community." The "passenger stability indicators" include length-of-residence, home ownership, and income.[17] Based on these indicators, each traveler will get a red, yellow, or green score. The vast majority of travelers will not have a suspicious background and will get a green score. They will pass through standard security procedures and may be subjected to an occa-

---

[12] Transportation Security Administration, Briefing Room, Testimony & Transcripts, Statement of Transportation Security Administrator Admiral James M. Loy before the Senate Appropriations Subcommittee on Homeland Security (May 13, 2003), *at* http://www.tsa.gov/public/display?content=405.

[13] Transportation Security Administration, Briefing Room, Press Release, TSA Selects Lockheed Management and Data Systems to Build TSA Passenger Pre-Screening System (Feb. 2003), *at* http:/www.tsa.gov/public/display?content=248.

[14] Torch Concepts, *Homeland Security: Airline Passenger Risk Assessment* (Feb. 25, 2003), *at* http://www.abditum.com/~rabbi/531B3_Roark.pdf.

[15] Transportation Security Administration, Briefing Room, Press Releases, CAPPS II News Release (July 31, 2003), *at* http://www.tsa.gov/public/display?content=634.

[16] *See* Torch Concepts, *Homeland Security: Airline Passenger Rise Assessment* (Feb. 25, 2003), *at* http://www.abditum.com/~rabbi/53B3_Roark.pdf.

[17] *Id.* An airline's disclosure of such confidential information is the subject of much controversy and is also the subject of a class action lawsuit by JetBlue passengers who claim that their personal data went into this report without their consent. For more information on the lawsuit see http://www.dontspyon.us/jetblueclassaction.html; *see also,* Ryan Singel, *JetBlue Fesses Up, Quietly* (Sept. 19, 2003), *at* http://www.wired.com/news/politics/0,1283,60502,00.html

sional random search. Those who trigger the yellow rating will have their checked and carry-on baggage inspected and may be questioned. A red score is a "no-fly" indicator, resulting in a denial of boarding. It is certain that law enforcement will be summoned, but it remains unclear what the person's rights will be at that point.[18]

Thus, CAPPS II is an advanced profiling system created to determine which passengers are more likely to pose a threat to airline security.[19] This will enable the TSA to focus its heightened screening efforts on persons likely to pose a potential threat, the "selectees." Passengers will benefit from quicker security lines and being "cleared" electronically in the time it takes to print a boarding card. This focus on "the needle" rather than "the haystack" represents a major shift from today's screening protocols. Because profiling is so controversial due in part to racial sensitivities, airport security screeners have gone out of their way to ensure that security procedures are applied without regard to personal characteristics.[20] Airline and TSA employees are instructed to focus on specific behaviors and utilize a "but/for" test in evaluating suspicious passengers.[21] They are instructed to ask themselves, "but for this person's perceived race, ethnic heritage or religious orientation, would I have subjected this individual to additional safety or security scrutiny?"[22] Thus, ethnic considerations are not factored in. Yet, consciously ignoring racial factors requires an irrational denial of history and present circumstances. The result has been that flight crews, including pilots, little old ladies, and mothers with young children

---

[18] For example, upon getting a red light, does the suspect have the right to remain silent? To an attorney? To view the record that the accusations are based upon? It has been implied that one does not have the right to "walk away" at that point.

[19] *Id.*

[20] Ellen Baker, *Flying While Arab: Racial Profiling and Air Travel Security*, 67 J. AIR L. & COM. 1375, 1390 (2002). Although certainly not dispositive, the results of an informal survey conducted by a newspaper at two major airports in late January 2002 are interesting. Of the more than 1000 passengers observed, only between 5 and 10 percent were selected for extra inspection at the boarding gates. Of those passengers selected, most were white males followed by white females. "Although dozens of people who appeared to be of Middle Eastern descent boarded the flights, only two received extra screening." Bob Von Sternberg, *Arab-Americans Fear They Are Being Singled Out, But the Government and Airlines Say the Increased Security Checks Are Random*, STAR TRIB. (Minneapolis, MN), Feb. 3, 2002, at 23A.

[21] Von Sternberg, *supra* note 20.

[22] *Id.*

are searched at roughly the same rate as foreign-born young men.[23]

CAPPS II changes the presumption that everyone is an equal security risk. CAPPS II is an expansion of the original CAPPS system in use since 1998.[24] Additionally, the FAA has maintained a "no-fly" list and a "selectee" list since 1990.[25] The existence of these lists was suspected for many years, but was only confirmed after the Electronic Privacy Information Center (EPIC) won a Freedom of Information Act (FOIA) lawsuit against the TSA in April 2003.[26] These lists are based upon criminal records, suspicious travel history, and several dozen other unspecified factors.[27] However, unlike the current system, in which data stays within individual airlines' reservation systems, the new setup will be managed by the TSA. Accordingly, only government officials with proper security clearance will be able to use it. It is unknown how many dangerous people have been deterred by CAPPS I. Significantly, between nine and 11 of the 19 hijackers on September 11th were flagged as potential

---

[23] Even some members of Congress are unhappy about regularly being "wanded" by security. "You have 535 members of Congress who are frequent flyers," Rep. John Mica, Chairman of the House Transportation Committee's aviation panel, said in July 2002. "People are not happy when there aren't some common sense approaches to security. Shaking down 80-year-old ladies, Medal of Honor winners and 5-year-old kids makes no sense." AP, *Lawmakers Question Progress in Airline Security Since Sept. 11*, USA TODAY, TRAVEL NEWS (July 23, 2002), *at* http://www.usatoday.com/travel/news/2002/2002-07-23-security-hearing.htm

[24] Transportation Security Administration, Briefing Room, Press Releases, CAPPS II News Release (July 31, 2003), *at* http://www.tsa.gov/public/display?content=634. CAPPS I was implemented in January 1998—instituted in part by Northwest Airlines in response to the 1996 crash of TWA 800 and the Atlanta Olympics bombing, both initially thought to have been terrorist related. Subcommittee on Aviation, Hearing on Aviation with a Focus on Passenger Profiling (last visited Jan. 20, 2004), *at* http://www.house.gov/transportation/aviation/02-27-02/02-27-02memo.html.

[25] Electronic Privacy Information Center, *Documents Show Errors in TSA's "No-Fly" Watchlist* (Apr. 2003), *at* http://www.epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html. EPIC made an FOIA request in October 2002. *Id.* The TSA responded in March and April 2003. Letter from Patricia M. Riep-Dice, Transportation Security Administration, to Mihir Kshiroge-Electronic Privacy Information Center (Mar. 21, 2003), *available at* http://www.epic.org/foia_docs/airtravel/tsa_letter.pdf.

[26] Electronic Privacy Information Center, *Documents Show Errors in TSA's "No-Fly" Watchlist* (Apr. 2003), *at* http://www.epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html. EPIC has also posted on its website a large file of consumer complaints regarding mistaken placement on these watch lists, and the difficulty with clearing one's name from such lists. *Id.*

[27] Torch Concepts, *Homeland Security: Airline Passenger Risk Assessment* (Feb. 25, 2003), *at* http://www.abditum.com/~rabbi/53B3_Roark.pdf.

threats by the original CAPPS.[28] In a fatal error, none of the men were searched or questioned because the system gave a pass to passengers who did not check any bags.[29] People without checked bags are now included, and the CAPPS II system has added an undisclosed number of additional variables.[30]

Although airlines are not discussing the profiling system publicly, at least one airline is cautiously optimistic about the program. One more terrorist incident could ruin the struggling airlines not to mention the national economy. The airlines are desperate to prevent any type of incident and, therefore, must support some type of passenger screening. An added advantage of CAPPS II is that some of the stifling liability is taken off the airlines and placed on the government. This liability includes responsibility in the event of security failure, as well as individual lawsuits brought as a result of unjust profiling.

How effective will CAPPS II be? Would the "shoe bomber," Richard Reid, have been caught by a profiling program? The answer is "maybe." His criminal record, perhaps combined with his conversion to Islam and his name change,[31] would have probably triggered a yellow flag. If so, the heightened security procedures would have detected the explosives in his shoes. Instead, he nearly succeeded in bombing an American Airlines flight.[32] Clearly, something must be done to prevent radical criminals like Reid from sauntering through security while grandmothers are frisked.

---

[28] *See, e.g.*, CBSNews.com, War on Terror, *Hijackers Aroused Suspicion* (Mar. 2, 2003), *at* http://www.cbsnews.com/stories/2002/03/02/attack/main502689.shtml.

[29] *Id.*

[30] Torch Concepts, *Homeland Security: Airline Passenger Risk Assessment* (Feb. 25, 2003), *at* http://www.abditum.com/~rabbi/53B3_Roark.pdg.

[31] "Reid scraped by in his early years selling drugs, breaking into cars, and mugging people, according to recent news reports. These activities led to time in juvenile detention, then jail. In prison, he became interested in Islam, and on his release in 1995, he took up study at a mosque in south London. There, he may have met Zacarias Moussaoui, the suspected 20th hijacker in the Sept. 11 attacks. By 1998, Reid was moving with more radical Islamic groups. . .He grew a beard and changed his name to Abdel Rahim." Gail Russell Chaddock, *Lessons of Shoe-Bomb Incident Groups Like Al Qaeda May Now be Using Operatives who Don't Fit the Polic Profiles*, CHRISTIAN SCI. MONITOR, Dec. 28, 2001, *at* 1.

[32] *Id.* Reid had enough explosives in his shoes to blast a large hole in the fuselage. He may have succeeded if he had simply elected to ignite the explosives in the lavatory instead of at his seat, where he drew the attention of the flight attendants who heroically subdued him. *Id.*

The TSA and many members of the traveling public hope that the CAPPS II profiling system will offer a solution to this dilemma. After all, preventing terrorist attacks is an important national goal. If we have "nothing to hide," why should Americans be concerned about CAPPS II?

III. CAPPS II AS AN INVASION OF PRIVACY

Many Americans, not just civil libertarians, are alarmed about the CAPPS II profiling system.[33] The Internet is abuzz with concerns that "Big Brother is watching you."[34] A Californian was successful in promoting a consumer boycott[35] of Delta Air Lines when it was rumored that Delta was testing the CAPPS II system for the government.[36] Now it is rumored that JetBlue Airways has replaced Delta Airlines as the "testing platform" for CAPPS II.[37]

---

[33] Electronic Privacy Information Center, *In the Matter of Privacy Act Notice Concerning Aviation Security Screening Records* (Feb. 24, 2003), *at* http://www.epic.org/privacy/airtravel/tsacomments2.24.2003.html. As if CAPPS II were not enough, the TSA is currently testing biometric scanning for face recognition and the use of voice stress analysis. This utilizes the physiological characteristics of a human voice pattern to infer malevolent or deceptive intent.

[34] *Id.*; American Civil Liberties Union, News, *ACLU, Conservatives, Civil Rights Groups Agree: CAPPS II Raises Serious Privacy and Security Concerns* (Aug. 25, 2003), *at* http://www.aclu.org/safeandfree/safeandfree.cfm?ID=1335480=206; *see also* Boycott Delta, *CAPPS II testing has been restarted, at* http://www.boycottdelta.com (last visited Jan. 20, 2004); Privacy Activism, *Passenger Profiling Violates Rights, Doesn't Improve Safety, at* http://www.privacyactivism.org (last visited Jan. 20, 2004).

[35] Boycott Delta, *CAPPS II testing has been restarted, at* http://www.boycottdelta.com (last visited Jan. 20, 2004).

[36] *Id.* Delta's official response to customer inquiries regarding CAPPS II is as follows:

> CAPPS II is a federal program administered by the Transportation Security Administration (TSA) as a result of the heightened threat of terrorism to our country. Delta's role in the CAPPS II program will be limited to providing data to the TSA that Delta already collects from passengers as part of our normal reservations and ticketing process. Delta is not running credit or background checks on customers. The security of Delta's passengers and safeguarding passenger information remains a top priority. For more detailed information regarding the program, please contact the TSA.

Customers may be directed to the TSA s Consumer Response Center at 1-866-289-9673.

[37] "A group of passengers has filed a class-action lawsuit against JetBlue Airways Corporation for its disclosure of passenger information to a Defense Department contractor. The lawsuit alleges fraudulent misrepresentation, breach of contract and invasion of privacy." New York-based JetBlue acknowledged that it had given information from about 5 million passenger records to Torch Concepts of Hunts-

The factors that will be analyzed by CAPPS II are largely classified and unknown. In addition to performing a criminal check, a credit check, and a confirmation of identity, one can speculate what additional factors would be both useful and technologically feasible to include. On its website, the TSA has said that it will access financial and transactional data, yet it is vague about what that will encompass. Certainly travel patterns and payment methods will be included in the search since they were already incorporated in the original CAPPS. In addition to government and public records, an astounding array of information is currently being collected by private firms on every person in America.[38] This information is available to the government and private parties for purchase.[39] Some factors that may be included in an individual's data dossier include race, religion, political affiliations, credit history, employment, spending habits, charitable donations, unusual books purchased or checked out, and visits to certain websites. All of this information will be aggregated to find not only convicted criminals, but also to identify those whose personal interests and backgrounds fit a profile for those likely to engage in certain forms of criminal activity.

Briefly, privacy concerns and ethical dilemmas that are likely issues with a large scale, surreptitious data-mining system include:

- The principle of treating everyone as a suspect without cause is wrong. Requiring citizens to submit to background investigations to travel in their own country is un-American.

---

ville, Alabama. Torch, a defense contractor, produced a study, "Homeland Security: Airline Passenger Risk Assessment," that was purported to help the government improve military base security. KCAL 9, *Passengers Sue JetBlue: Lawsuit Filed over Data Disclosure* (Sept. 23, 2003), *at* http://kcal9.com/finance/finance_story_266085701.html.

[38] For example, the private sector company ChoicePoint, Inc. has multi-million dollar contracts with about thirty-five federal agencies including the Federal Bureau of Investigation (FBI) and the Internal Revenue Service (IRS) to provide personal information. ChoicePoint's database contains over ten billion records indexed by Social Security numbers. The information is gathered from public records, private detectives, and credit records. *See* Glenn R. Simpson, *Big Brother-in-Law: If the FBI Hopes to Get the Goods on You, It May Ask ChoicePoint*, WALL ST. J., Apr. 13, 2001, at A1.

[39] *Id.* Since 2001, EPIC has been involved in a lawsuit with the Justice and Treasury Departments over a FOIA request it filed to learn more about government use of private data. The case is ongoing, but as EPIC's president David Sobel said, it revealed information such as a $67 million government contract with the data-collection agency ChoicePoint. William Wew, *Proposal Would Link Agencies' Funding to Privacy Protesting*, NAT'L J. TECH. DAILY (July 29, 2003), *at* http://www.govexec.com/dailyfed/0703/072903td1.htm.

- There is too much secrecy in the program. The government has no right to spy on its citizens.
- It is immoral to collect personal data on individuals and analyze them with sophisticated algorithms to try to predict a person's future behavior. There are no "thought crimes."
- Personal information can fall into the wrong hands and be misused. Never before has so much information from so many sources been collected in a single place.
- The government may use the information gathered for unauthorized purposes. "Function creep" is inevitable as the IRS, law enforcement, and various other agencies seek access to the data. Furthermore, people will be arrested at the airport for infractions that have nothing to do with security of the flight.
- Racial, ethnic, and even gender discrimination will rear its ugly head as people are scrutinized based on these immutable characteristics.
- Some indications suggest that the data will remain on file for 50 years.[40]
- There is the potential for identity theft, fraud, and sale of information to private interests and businesses.
- People may lose their fundamental right to travel if they have bad credit or owe fines or child support.

Furthermore, there are practical considerations:

- The error rate is unacceptable. If just one percent of the population scores a false positive, more than 6 million unjustified inquiries are performed per year.
- Once a person is erroneously targeted as a "red" or "yellow," the procedures for removing oneself from the list are onerous.[41]

---

[40] Many sources, such as Boycott Delta, *Delta Airlines Treats Americans like Terrorists*, *at* www.boycottdelta.com (last visited Jan. 20, 2004), stated that the data would remain for 50 years. In response, the TSA issued a press release on July 31, 2003, stating in pertinent part: "Eliminated from a Jan. 15 Federal Register notice was language that led some to believe that large amounts of information about individuals would be collected and maintained for up to 50 years." Unfortunately, the notice did not clarify how long this information would be maintained. Transportation Security Administration, Briefing Room, Press Release, CAPPS II News Release, New Notice Outlines Changes to CAPPS II System (July 31, 2003), *at* http://www.tsa.gov/public/display?content=634.

[41] EPIC has collected a file of TSA complaints that document the near impossibility of getting a name removed from the watch list, even if it was erroneously included. *See* EPIC, Complaint for Injunctive Relief, *available at* http://www.epic.org/privacy/airtravel/tsa_foia_suit.pdf (last visited Jan. 20, 2004).

- Frequent credit checks result in lower credit ratings for travelers.
- The system will not prevent future hijackings since hijackers will figure out and undermine the system.[42] For example, this can be accomplished via identity theft.
- The system will encourage airport employees to be complacent, as they will allow the computer to do evaluations for them.

IV. THE BALANCE BETWEEN SECURITY AND PRIVACY

This paper does not purport to judge the morality or efficacy of CAPPS II. Rather, it explains what is known so far about the program and the controversy surrounding the privacy-security tradeoff, and it analyzes this novel program against the privacy protections offered by the Fourth Amendment. CAPPS II is a technologically advanced tool that profiles travelers and analyzes their backgrounds to look for lifestyle patterns that indicate a potential threat to a flight. The surreptitious use of personal data may be considered an illegal search and implicate the Fourth Amendment. By analyzing Fourth Amendment precedent, this paper attempts to predict how courts will balance the tradeoff between security and privacy, and either justify or strike down in whole or in part this revolutionary surveillance system.

Fourth Amendment jurisprudence is esoteric, complex, and frequently inconsistent.[43] Unlike other fundamental rights

---

[42] In a dissertation, two MIT graduate students developed a complex algorithm that allegedly undermines the methodology of the original CAPPS system.

> In this paper, we show that since CAPPS uses profiles to select passengers for increased scrutiny, it is actually less secure than systems that employ random searches. In particular, we present an algorithm called Carnival Booth that demonstrates how a terrorist cell can defeat the CAPPS system. Using a combination of statistical analysis and computer simulation, we evaluate the efficacy of Carnival Booth and illustrate that CAPPS is an ineffective security measure. Based on these findings, we argue that CAPPS should not be legally permissible since it does not satisfy court-interpreted exemptions to the U.S. Constitution's Fourth Amendment.

Samidh Chakrabarti & Aaron Strauss, *Carnival Booth: An Algorithm for Defeating the Computer-Assisted Passenger Screening System* (May 16, 2002), *at* http://www.swiss.ai.mit.edu/6805/student-papers/spring02-papers/caps.htm.

[43] Professor Wayne R. LaFave, in analyzing the Fourth Amendment, attempted to untangle the nine search and seizure decisions issued during the Supreme Court's 1982-83 term. He proclaimed these cases, as a group, to be "illogical, inconsistent with prior holdings and generally, hopelessly confusing." Wayne R.

cases, such as the Second Amendment, the Supreme Court has not shied away from making sweeping proclamations over the meaning of the Fourth Amendment. In addressing the privacy concerns posed by technological advances, the pendulum continues to swing back and forth between autonomy and interference. Many exceptions to the search and seizure prohibitions have been added in the past several decades to allow for greater law enforcement powers. Yet while Fourth Amendment privacy is being eroded, its protections are simultaneously more important than ever. Public and private technological marvels are now capable of removing all vestiges of privacy. In the recent past, an information super-network like CAPPS II was unthinkable and threatening. Now many Americans are understandably afraid to fly and willing to sacrifice privacy for a promise of security.

Still, there is no way to make flying entirely safe, and there is no easy answer to the profiling issue. Whether the profiling system will actually be effective in deterring terrorism remains to be seen. Many questions are unanswerable due to the secrecy that is required of the project. Although this paper focuses primarily on the Fourth Amendment, the TSA must show that its CAPPS II system also comports with the First,[44] Fifth, and Fourteenth Amendments. For instance, it is settled law that claims asserting a search was motivated by race will be decided not under the Fourth Amendment, but under equal protection.[45]

The TSA's challenge is to "balance" the tension between security and privacy.[46] In the world of public opinion, the TSA

LaFave, *Fourth Amendment Vagaries (of Improbable Cause, Imperceptible Plain View, Notorious Privacy, and Balancing Askew)*, 74 J. CRIM. L. & CRIMINOLOGY 1171 (1983). Such decisions offer poor guidance to those responsible for conducting administrative searches. "Without understanding the individual Fourth Amendment protections at issue, how can society meaningfully participate in debates about the future of such protections in airline security?" Jamie L. Rhee, *Rational and Constitutional Approaches to Airline Safety in the Face of Terrorist Threats*, 49 DEPAUL L. REV. 847, 866 (2000).

[44] Obviously, the First Amendment implicates religion-based searches, but it also encompasses those based upon association and speech, as in the case of political activists.

[45] *See* Whren v. United States, 517 U.S. 806, 813 (1996).

[46] In a speech, Admiral Loy, director of the TSA, said the TSA would create an independent oversight board for the screening system. "TSA is committed to the very American proposition that our rights and our security are complementary, not competitive or contradictory," Loy said. Robert O'Harrow Jr., *Aviation ID Systems Stirs Dorlots; Senate Panel Wants Data on Impact on Passenger Privacy*, WASHINGTON POST, Mar. 14, 2003, at A16.

along with the airlines must demonstrate that advantages in prescreening passengers to prevent potential terrorists from boarding outweigh a rational and proportional decrease in Americans' expectation of privacy. Public opinion and political support are crucial to the implementation of CAPPS II. For example, a similar but broader data-mining program, the Total Information Awareness System, was put on an indefinite hold due to public outcry and Senate opposition to its secretive and invasive data collection and use.[47] Similarly, the European Union is very critical of the TSA's new program. CAPPS II conflicts with EU laws protecting personal data because the program also screens Europeans who fly to the United States.[48] Still, TSA's director and spokesman Admiral James M. Loy is optimistic that CAPPS II can be implemented, while maintaining respect for privacy rights. In a speech, Loy said, "TSA is committed to the very American proposition that our rights and our security are complementary, not competitive or contradictory."[49] Organizations ranging from the ACLU to the ACU disagree.

V. THE FOURTH AMENDMENT

This paper aims to see how this surveillance tool, both radical and revolutionary, will be viewed in the light of Fourth Amendment privacy protections. The Fourth Amendment to the Constitution states:

> 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

---

[47] Audrey Hudson, *Lawmakers Seek to Limit TIA*, WASHINGTON TIMES, Jan. 17, 2003, at A5. The Defense Advanced Research Projects Agency (DARPA), which administers the program, recently changed the name to "Terrorism Information Awareness." According to DARPA, the purpose of TIA is to identify potential terrorists by comparing information in a broad range of databases that might offer clues. DARPA often has cited the example of using TIA to prevent a truck bomb attack by searching for patterns indicating a group of foreigners who are traveling together, renting trucks and buying materials that could be used as explosives. Testing such a scenario would require the system to have access to credit-card records, airline itineraries and car-rental records. Ryan Singel, *Pentagon Defends Data Search Plan* (May 21, 2003), *available at* http://www.wired.com/news/privacy/0,1848,58936,00.html.

[48] Sara Kehaulani Goo, *Passenger-Screening Plan Assailed: EU, Budget Office Among Those Saying System Is Not Ready*, WASHINGTON POST, Mar. 26, 2003, at A8.

[49] O'Harrow, *supra* note 46.

describing the place to be searched, and the persons or things to be seized.[50]

VI. PROTECTION AGAINST ILLEGAL SEARCH AND SEIZURE

Basically, the Fourth Amendment regulates the overall ability of the government to obtain information through searches and seizures.[51] Searches and seizures are not limited to their literal meanings but encompass the taking of information reasonably believed to be confidential.[52]

The essential purpose of the Fourth Amendment is to safeguard individual privacy and security.[53] It prevents arbitrary governmental invasions by imposing a standard of reasonableness upon the exercise of discretion by government officials, including law enforcement agents.[54]

One of the central reasons that the Framers created the Fourth Amendment was to guard against general warrants.[55] Law enforcement is prohibited from conducting unwarranted searches into citizens' private lives, possessions, and records to look for evidence of wrongdoing.[56]

Since the purpose of the CAPPS II screening system is arguably to examine passengers' backgrounds, past actions, and affiliations in order to anticipate whether the individual poses a

---

[50] U.S. CONST. amend. IV.

[51] Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Freedom*, 75 S. CAL. L. REV. 1083, 1085 (2002).

[52] Boyd v. United States, 116 U.S. 616 (1886) (involving not a search and seizure but a compulsory production of business papers which the Court likened to a search and seizure). Katz v. United States, 389 U.S. 347, 351 (1967) (holding that the attachment of a listening and recording device to the outside of a telephone booth constituted a search).

[53] *Katz*, 389 U.S. at 350.

[54] *Id.* Also, the courts have established that airline searches, although administered by private airline employees, are considered state actions by state actors. Thus, the reasonableness standard applies to airline employees as well.

[55] Solove, *supra* note 51, at 1107 n.130.

[56] "Dataveillance gives the government essentially unlimited discretion to search through masses of personal information in search of suspicious activity, without specifying in advance the people, places or things it expects to find. Dataveillance allows fishing expeditions in which the government is trolling for crimes rather than criminals, violating the privacy of millions of innocent people in the hope of finding a handful of unknown and unidentified terrorists," said Jeffrey Rosen, law professor at George Washington University. Roy Mark, *Trolling for Crimes, Not Criminals* (Mar. 28, 2003), *at* http://www.esecurityplanet.com/trends/print.php/2169871.

potential threat to a flight, CAPPS II appears to be in conflict with the Fourth Amendment's protections. A complicated body of law has evolved to resolve Fourth Amendment issues, and various exceptions to the rule have been created. Much of the recent case law deals with technological advances that permit non-physical searches that could not have been anticipated by the original amendment. The technological capabilities of the CAPPS II system are remarkable, and were certainly not foreseen by the Founding Fathers. However, the principle of the Fourth Amendment protection of privacy against overreaching governmental intrusion has not changed.

VII. PROBABLE CAUSE AND WARRANT REQUIREMENTS

In order to intrude on an American's[57] person, belongings, or dwelling, the government must have probable cause to believe that a crime has been committed. Probable cause exists when "the facts and circumstances within the arresting officer's knowledge are sufficient to warrant a prudent person to believe that a suspect has committed, is committing, or is about to commit a crime."[58] By using CAPPS II, airlines are not expected to be criminal investigation units solving past crimes. They are focusing on suspects that are "about to commit a crime."

Courts have generally recognized searches as being reasonable if they properly balance the degree of intrusiveness, the magnitude and frequency of the threat, and the efficacy of alternatives to the search.[59] Unless an exception applies, a search warrant is required. Physical airport searches are done without warrants due to an exception carved out especially for this type of search.

---

[57] The Fourth Amendment does not apply to foreign visitors. The Fourth Amendment protects U.S. citizens who go abroad and aliens who have voluntarily entered U.S. territories and developed substantial connections with this country. The Supreme Court has determined that the Fourth Amendment's reference to "the people" refers to "a class of persons who are part of a national community or who have otherwise developed sufficient connection with the U.S. to be considered part of that community." *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 265 (1990).

[58] United States v. Hoyos, 892 F.2d 1387, 1392 (9th Cir. 1989), *cert. denied*, 489 U.S. 825 (1990) (citing United States v. Greene, 783 F.2d 1364, 1367 (9th Cir. 1986)).

[59] Michigan Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990). This is explained in the section called Administrative Search Exception. *See infra* section VII.C.

Generally, in order to get a warrant for a search, a law enforcement official has to present the evidence to a neutral magistrate and show suspicion or probable cause.[60] Court cases have further clarified exactly what constitutes a minimal level of objective justification.[61]

One could argue that search warrants are a moot point since more than 99% of search warrant requests are routinely granted.[62] Yet, warrants promote fair dealing by the police in several ways. Warrants require officers to document their requests for authorization, and therefore, officers are unlikely to use them unless their suspicions are substantiated.[63] Further, government officials are prevented from "dreaming up post hoc rationalizations."[64]

The CAPPS II system is in some ways analogous to the warrant requirement protection. CAPPS II gathers and analyzes pre-existing information in a manner similar to the way law enforcement might observe suspicious behavior and perform a background check of a person of known identity. Based upon this information, the computer system makes a determination as to whether a search of the party is justified, much as a neutral magistrate examines the preliminary evidence and decides whether to issue a warrant for additional search procedures. CAPPS II will then issue "warrants" for heightened security procedures only for those "selectees" whose profiles created suspicion, or "probable cause." Thus, warrants and "yellow scores" permit searching of individuals suspected of being "about to commit a crime."[65]

VIII. *KATZ V. UNITED STATES*: A REASONABLE EXPECTATION OF PRIVACY

In *Katz*, the Supreme Court modified its longstanding test for judging privacy violations.[66] Prior to this case, the Court held that absent physical intrusion, there was no unlawful search or seizure. Here, police officers surreptitiously affixed a listening

---

[60] *Katz*, 389 U.S. at 355.

[61] *Sitz*, 496 U.S. at 452.

[62] 2002 Wiretap Report, *at* www.uscourts.gov/wiretap02/contents.html (last visited Oct. 28, 2003).

[63] William J. Stuntz, *O.J. Simpson, Bill Clinton and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 848 (2001).

[64] Solove, *supra* note 51, at 1127.

[65] *Hoyos*, 892 F.2d at 1392.

[66] *Katz*, 389 U.S. at 352.

device to a telephone booth that Katz regularly used.[67] Although the Court was expected to debate the intrusiveness of the device on the phone booth, it instead made the broad statement that the Fourth Amendment protects people not places.[68] Thus, *Katz* shifted the definition of privacy from being place-based to being person-based. As a result, any discussion about CAPPS II need not involve the importance of locations in an airport or on an airplane. Rather, *Katz* indicates that the Fourth Amendment may protect anything a person "seeks to preserve as private" without regard to where the information is located:

> What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[69] [That is,] the capacity to claim the protection of the Amendment depends not upon a property right in the invaded place but upon whether the area was one in which there was reasonable expectation of freedom from governmental intrusion.[70]

Furthermore, *Katz* propounded a test to determine whether there is an expectation of privacy upon which one may "justifiably" rely.[71] This is regarded as one of the most fundamental shifts in privacy law.[72] To determine the threshold for justifiable reliance, Justice Harlan created the "reasonable expectation test" which balances the interest in protecting individuals from government intrusion with the interest in protecting society from criminals.[73] Two elements must be satisfied in order for an expectation of privacy to be reasonable:

---

[67] *Id.*

[68] *Id.*

[69] *Id.* at 351-52.

[70] Mancusi v. DeForte, 392 U.S. 364, 368 (1968) (holding an official had a reasonable expectation of privacy in an office he shared with others although he owned neither the premises nor the papers seized); Minnesota v. Olson, 495 U.S. 91, 96 (1990) (holding that an overnight guest in home has a reasonable expectation of privacy); *cf.* Rakas v. Illinois, 439 U.S. 128, 143 (1978).

[71] *Katz*, 389 U.S. at 353. Justice Harlan, concurring, formulated a two pronged test for determining whether the privacy interest is paramount: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Id.* at 361.

[72] Justice Harlan's opinion has been much relied upon. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 740-41 (1979); United States v. Salvucci, 448 U.S. 83, 91-92 (1980); Rawlings v. Kentucky, 448 U.S. 98, 105-06 (1980).

[73] *Katz*, 389 U.S. at 361.

(1) Subjective privacy—Did the person exhibit a personal *expectation* to be left alone from government intrusion?[74]
(2) Objective privacy—Is the personal expectation one that society is prepared to recognize as *reasonable*?[75]

Do airline travelers have an actual expectation that they will travel free of government intrusion? On the contrary, people demand protection from the government. Flying has its risks, and the government works with the airlines to minimize danger. Throughout the history of commercial aviation, the government has been regulating aircraft maintenance, air traffic control, licensing of pilots, and more. Passengers expect and demand that weapons and hazardous materials be confiscated from others at the security checkpoints. They willingly open up their baggage for inspection and subject themselves to metal detection machinery.[76] Without this important governmental oversight, people would be even more apprehensive about flying. Of course, the physical intrusions into baggage, "wanding," shoe inspections, and the like, routinely done by TSA agents are of a very different nature than the covert background checks that the CAPPS II system will require.

Does the knowledge that one is subject to a physical inspection at the airport imply that one has consented to a virtual data inspection? *Katz* asks whether a person has an actual expectation of privacy at that moment.[77] People are aware that their luggage might be inspected, but don't suspect that their credit is being checked. The CAPPS II program is being discretely implemented and neither flyers nor the majority of airline employees have heard of it. Then again, hardly anyone knows about the no-fly lists that the FAA has maintained for more than a decade. Most Americans are also unaware that their banks are required to collect data for the government and that personal data is being collected in various ways. If one is interested enough,

---

[74] Though this test was established in a concurrent opinion, it is widely used. *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 19 (1968); Rakas v. Illinois, 439 U.S. 128, 143-44 n.12 (1978).

[75] *Id.*

[76] Admiral Loy says that once CAPPS II is in place, passengers will be subjected to fewer incidents of high-level random screening. Transportation Security Administration, Statement of Transportation Security Administration Administrator Adm. James M. Loy Before the Senate Appropriations Subcommittee on Homeland Security (May 13, 2003), *available at* www.tsa.gov/public/display?content=486.

[77] *Katz*, 389 U.S. at 347.

this information is available on request or on the Internet. Is ignorance an excuse?

The government intrudes on one's privacy in a variety of ways without public outcry because few people are even aware of the intrusion. Even if the government was concerned with giving people notice of the data-mining system, it is unclear how it would proceed. It is impermissible for the government to condition "subjective expectations" by informing people that no privacy exists in a situation that is normally considered private. So, even if the government mandated that a privacy alert warning appears on the back of each ticket, it may not legitimately destroy a reasonable expectation of privacy. The Court held that, for example, "announcing that henceforth all homes would be subject to warrantless entry," thus destroying the legitimate expectation of privacy, is forbidden.[78]

That question leads to the second prong of the test: Is it reasonable to have an expectation of privacy in an airport or as an airline passenger? How has this expectation changed since the quadruple hijackings of September 11th? Just as people's apprehension about flying has gone up since that date, their expectations of privacy have clearly gone down. Travelers now expect to present identification at several points before boarding and to remove their shoes. Further, they see national guardsmen at the airport and possibly have armed air marshals and pilots on board their flight. Clearly, flying has changed.

A. Applying the Reasonable Expectation of Privacy Test

What seems to have emerged since *Katz* is a balancing of the tensions between individual and state interests. The balancing test requires "an assess[ment] of the nature of a particular practice and the likely extent of its impact on the individual's sense of security, balanced against the utility of the conduct as a technique of law enforcement."[79] In the CAPPS II context, the subjective test of "the impact on an individual's sense of security" is irrelevant as it is entirely impossible to apply to the nation as a whole, since one person's security is another's tyranny. Instead, the analysis must consider the overall intrusiveness of the program.

---

[78] United States v. White, 401 U.S. 745, 786 (1971); Smith v. Maryland, 442 U.S. 735, 740 n.5 (1979).

[79] *White*, 401 U.S. at 786-87 (Harlan, Jr., J., dissenting) (balancing test of *United States v. Martinez-Fuerte*).

The *Katz* balancing test was used in authorizing sobriety checkpoints where all vehicles were briefly stopped, and drivers questioned and observed for evidence of intoxication.[80] The Supreme Court held that, "[i]n sum, the balance of the State's interest in preventing drunken driving, the extent to which this system can reasonably be said to advance that interest, and the degree of intrusion upon individual motorists who are briefly stopped, weighs in favor of the state program."[81]

Contemporary airline security procedures commenced in 1968 with the Sky Marshals program and the use of the magnetometer.[82] A great deal of litigation ensued, charging that the common metal detectors and x-rays violated the right of privacy. Although private companies performed airport screening for decades, the level of government participation in airport search programs was enough to bring any such search within the reach of the Fourth Amendment.[83] Upon a 1973 challenge to these procedures, it was determined that pre-boarding screening of all passengers and carry-on articles sufficient in scope to detect the presence of weapons or explosives is reasonable under the Fourth Amendment if persons are able to avoid the search by electing not to board the aircraft.[84] The goal of safer skies justified the inconvenience and privacy intrusion to airline passengers.

Applying this balancing test, the Court would undoubtedly view the aim of prevention of terrorist hijacking and sabotage to be an important public interest. However, the utility of CAPPS II will be a contested issue. Given the classified nature of the

---

[80] Michigan Dept. of State Police v. Sitz, 496 U.S. 444 (1990).

[81] *Id.* at 455.

[82] A brief history of the air marshal program is located at The Marshals Monitor, *The Marshals Service Pioneered the Air Marshal Program, available at* http://www.usdoj.gov/marshals/monitor/jan-2002/jan02-1.html (last visited Jan. 20, 2004).

[83] United States v. Davis, 482 F.2d 893 (9th Cir. 1973) (holding that since late 1968, government's participation in airport search program has been such as to bring any search conducted pursuant to that program within the reach of the Fourth Amendment; that a pre-boarding screening of all passengers and carry-on articles sufficient in scope to detect the presence of weapons or explosives is reasonable under the Fourth Amendment, if a person is given the right to avoid search by electing not to board the aircraft; that such a search does not violate the constitutional right of travel; that choosing to board aircraft after being given the choice of leaving is essentially a "consent" to search).

[84] *Id.* The court required that such a search does not violate the constitutional right of travel and that choosing to board an aircraft after being given the choice of leaving is essentially a "consent" to search.

data, it is unclear how effective CAPPS II will be in furthering the goal of safer skies, especially as an incremental improvement over CAPPS I. It is also unclear how the courts would evaluate the degree of intrusion posed by CAPPS II data-mining, considering that in the name of national security, even the courts will not be privy to the classified system input.

A recent case used the balancing test to determine what type of public interest was required to justify an intrusive state sponsored program under the Fourth Amendment.[85] The Indianapolis police set up a checkpoint to look for drug trafficking and other wrongdoing with a secondary purpose of finding drunk drivers.[86] Although it is generally accepted that a person has a lower expectation of privacy while in a vehicle than one has in a more permanent type of structure,[87] the Court struck down this type of roadblock. Seizing illegal drugs apparently was indistinguishable from the general interest in crime control, and general searches for evidence of wrongdoing are prohibited under the Fourth Amendment.[88] The Court explained its rationale: "the constitutionality of such checkpoint programs still depends on a balancing of the competing interests at stake and the effectiveness of the program."[89] Indianapolis' checkpoint program is not justified by the "severe and intractable nature of the drug problem."[90]

However, in an earlier case, *Delaware v. Prouse*,[91] the Supreme Court suggests that it would approve a similar checkpoint program with the goals of getting unlicensed drivers off the road and locating stolen vehicles, even absent probable cause. The Court suggested that the states check drivers' licenses and registrations using "methods for spot checks that involve less intrusion or those that do not involve unconstrained exercise of discretion. Questioning of all oncoming traffic at roadblock-type stops is one possible alternative."[92] In fact, some states have been doing this type of checkpoint for several years.[93] Thus, the

---

[85] City of Indianapolis v. Edmond, 531 U.S. 32 (2000).

[86] *Id.*

[87] Arkansas v. Sanders, 442 U.S. 753, 761 (1979) (collecting cases); United States v. Ross, 456 U.S. 798, 804-09 (1982).

[88] *Edmond*, 531 U.S. at 32.

[89] *Id.* at 47.

[90] *Id.* at 42.

[91] Delaware v. Prouse, 440 U.S. 648, 663. (1979).

[92] *Id.*

[93] *See* Robert L. Farb, *The Fourth Amendment, Privacy and Law Enforcement*, POPULAR GOVERNMENT, Spring 2002, at 13.

Court implies that it would accept a program like CAPPS II where all travelers are subject to scrutiny, as long as the check is not too intrusive and officials have limited discretion. Apparently the Court believes that enforcing licensing and registration rules outweighs the burden on an individual's privacy, yet enforcement of drug laws does not.

Given these prior rulings, the Court would most likely view the need to prevent airline hijacking as being at least as important as roadside checkpoints to stop unlicensed drivers. It is also likely that it will view passenger prescreening as being at least somewhat effective in preventing such crime. Further, prevention of hijacking is distinguishable from intercepting illegal drugs. For one, drug use, unlike hijacking, does not put anyone in imminent danger of death except maybe the user. Thus, using the *Katz* standard for reasonable expectation of privacy balanced against intrusion, the CAPPS II program is likely to be upheld.

B. *Kyllo v. United States*: A Technological Invasion of Privacy

In *Kyllo*, agents, suspicious that the defendant was growing marijuana in his home in a triplex, used a thermal imaging device to scan the building for heat associated with high-intensity lamps used for indoor marijuana cultivation.[94] After the exterior scan detected heat, the agents obtained a warrant to search the home. They found marijuana and the defendant was indicted on federal drug charges.

In a 5-4 decision authored by Justice Scalia, the Supreme Court vacated the conviction because the use of the heat scan to discover what was happening inside the home was an unlawful search.[95] "Where, as here, the government uses a device that is not in general public use, to explore details of a private home that would previously have been unknowable without physical intrusion, the surveillance is a Fourth Amendment 'search,' and is presumptively unreasonable without a warrant."[96]

It is unclear how this expansion of privacy protection would apply to CAPPS II. On one hand, *Kyllo* addresses searches of the home and may be limited to these cases. However, a case can be

---

[94] Kyllo v. United States, 533 U.S. 27 (2001).

[95] *Id.*

[96] *Id.*

made that there are similar expectations of privacy in one's person, one's luggage, and one's private information.

On the other hand, *Kyllo* implies that the Court rejects "virtual" invasions of privacy made feasible by technological progress. Privacy groups rejoiced at the ruling, which they hope will place new limits on technology-assisted searches in a variety of areas.[97] Presumably this would include biometric scanning of crowds, X-ray scanners to see through clothes, and possibly even the type of data-mining utilized by CAPPS II. The CAPPS II system certainly can be considered a "device that is not in general public use," and it can be used to analyze information that would have previously been unknowable without intrusion.

Even the government is unsure how *Kyllo* will apply to a host of new technologies. Three days after this ruling, House Majority Leader Dick Armey asked U.S. Attorney General John Ashcroft to review the constitutionality of Carnivore, the FBI's Internet sniffer.[98] The TSA has not asked the Justice Department for an evaluation of its program in light of *Kyllo*. Whether *Kyllo* will be interpreted broadly or narrowly remains to be seen.

C. Potential Fourth Amendment Exceptions for Airport Searches

It has been established that passengers have a privacy interest in both their carry-on and checked luggage.[99] Thus, a literal reading of the Fourth Amendment makes one wonder why airport searches are permitted at all, since there is no claim that the person being searched is dangerous or has committed a crime.[100] In fact, it was only after extensive litigation that today's security checkpoints and metal detectors were permitted.[101] In order to accommodate such airport searches, an entire body of law evolved, creating two exceptions to Fourth Amendment search and seizure protections. The administrative search doctrine and the "stop and frisk" doctrine allow for searches with little or no individualized probable cause.[102]

---

[97] Jeffrey Benner, *Kyllo: Taking the Fifth on the Fourth* (July 3, 2001), *at* http://www.wired.com/news/privacy/0,1848,44785,00.html (last visited Jan. 20, 2004).

[98] *Id.*

[99] United States v. Chadwick, 433 U.S. 1, 11-13 (1977).

[100] Jamie L. Rhee, *Rational and Constitutional Approaches to Airline Safety in the Face of Terrorist Threats*, 49 DePaul L. Rev. 847 (Spring 2000).

[101] United States v. Davis, 482 F.2d 893, 908 (9th Cir. 1973).

[102] *Id.*

As a result, searches conducted as part of a general regulatory scheme, done in furtherance of administrative goals rather than to secure evidence of a crime, may be permissible under the Fourth Amendment without any particularized showing of probable cause.[103] An example of a permissible warrantless search involves certain stops at border control checkpoints. Under the judicially created administrative search exception, the Supreme Court upheld the practice of border control agents who stop and briefly inspect vehicles at checkpoints in order to search for illegal aliens.[104] First, the Court recognized that governmental interests may in some situations trump Fourth Amendment protections.[105] The Court wrote, "government or public interest in making such stops outweighs the constitutionally protected interest of the private citizen."[106] Furthermore, the Court's opinion relied on the fact that the search was brief in duration, usually consisting of only a couple of questions and visual inspection. Since it did not greatly impede the flow of traffic or consume too much of the traveler's time, the Court ruled that the search was minimal in its intrusiveness given the government's compelling interest in border control.[107]

D. The Fourth Amendment Test for Administrative Searches

Through case law, the Supreme Court established a three-prong balancing test for warrantless administrative searches.[108] First, the government must establish a compelling need for the intrusion.[109] Second, it must be shown that the intrusion will be strictly limited to fulfilling that need and not be utilized for general law enforcement purposes.[110] Third, the decision to search

---

[103] See *Davis*, 482 F.2d at 908. Limited administrative searches may be conducted at the border. *See, e.g., Martinez-Fuerte*, 428 U.S. at 543 (1976); *Davis*, 482 F.2d at 893 (in airports); McMorris v. Alioto, 567 F.2d at 897 (9th Cir. 1978) (in state courthouses).

[104] *Martinez-Fuerte*, 428 U.S. at 543.

[105] *Id.*

[106] *Id.*

[107] *Id.*

[108] Balancing test is derived from the opinion in *Brown v. Texas*, 443 U.S. 47 (1979).

[109] See *United States v. $124,570 United States Currency*, 873 F.2d 1240, 1244 (9th Cir. 1989), as cited in Rhee, *supra* note 100.

[110] *Id.*

a particular person must not be subject to the discretion of the officer in the field.[111]

A truly informed debate on these requirements relating to CAPPS II is impossible because the profiling criteria are necessarily secret. It is unknown what the limits will be. If the selection methods were disclosed, they could be used by terrorists to evade the profiles. However, the following section anticipates some of the government's arguments, and possible reasoning the courts might apply.

1. *A Compelling Need for the Search*

In the wake of September 11th, the government will be able to show that there is a compelling need for heightened airport security to prevent terrorist attacks. If illegal alien smuggling and sobriety checkpoints justify warrantless searches,[112] then surely the TSA will be able to justify heightened airport security standards.[113] However, the actual data-mining programs of CAPPS II may not pass scrutiny. The government must establish a compelling need for the intrusion, and a court may decide that there is no need to profile passengers if other means of security are more effective. For example, the court might question the need for CAPPS II since the FBI has maintained a no-fly and a watch list on passengers for more than a decade.[114] On the other hand, keeping dangerous people and items off of aircraft may justify more intrusive behavior than would most administrative searches.

2. *Government Intrusion Must be Strictly Limited*

Second, the government must show that the intrusion posed by CAPPS II will be strictly limited to fulfilling the compelling

---

[111] Camara v. Municipal Court, 387 U.S. 523, 536-37 (1967).

[112] *Martinez-Fuerte*, 428 U.S. at 543; *Edmond*, 531 U.S. at 32.

[113] Judge Friendly, generally regarded as political liberal, wrote: "[w]hen the risk is the jeopardy to hundreds of human lives and millions of dollars of property inherent in the pirating or blowing up of a large airplane, the danger alone meets the test of reasonableness" for a search. United States v. Bell, 464 F.2d 667, 675 (2d Cir. 1972) (Friendly, J., concurring).

[114] A recent FOIA lawsuit brought by Electronic Privacy Information Center (EPIC) confirmed the existence of "no fly" and "selectee" lists maintained by the TSA. An additional concern raised by EPIC was the near impossibility of getting a name removed from the watch list, even if it was erroneously included. *See* Electronic Privacy Info. Ctr. v. Transp. Sec. Adminin., *at* http://www.epic.org/privacy/airtravel/tsa_foia_suit.pdf (last visited Jan. 20, 2004).

need for airline security.[115] Courts have stressed the importance of keeping administrative searches from becoming "infected by general law enforcement objectives, and the concomitant need for the courts to maintain vigilance."[116] Courts have expressed an aversion to executive branch overreaching. One judge warned that if the government is allowed to freely conduct discriminatory searches under the guise of an administrative search, then "officials [will] routinely invade the privacy and property of countless millions; hardly anyone [will escape] their clammy grasp."[117]

This limitation precludes sharing of data between agencies. "Function creep" is something that scares a lot of people as they fear their private information will end up in the hands of other agencies such as the IRS or the local police. Needless to say, it also precludes use for non-official purposes. It is not uncommon for personal records to be sold to marketers, or for individuals to try to benefit from insider knowledge.[118] Also, a person should not receive a yellow or red score based upon, for example, being a deadbeat dad, having a judgment against him, or even being convicted of a non-violent crime. The use of the powerful system must be restrained to selecting only those who pose a credible threat to the flight.

It is likewise unlawful to use a person's background to trigger a security check to gather evidence for a crime not directed at the aircraft. For example, every criminal background check that CAPPS II does will include any drug-related offenses. The TSA cannot flag that person as a selectee in order to get authorization to search the luggage and person for illegal drugs. If they do so, this unlawful evidence will be excluded under the exclusionary rule.[119] In contrast, if the contraband is discovered inadvertently in conjunction with a weapons search, the authorities

---

[115] *$124,570 U.S. Currency*, 873 F.2d at 1240.

[116] *Id.*

[117] United States v. Soyland, 3 F.3d 1312, 1316 (9th Cir. 1993).

[118] Indeed, it is not far-fetched for government officials to amass data for use in silencing or attacking enemies, critics, undesirables, or radicals. For example, J. Edgar Hoover accumulated an extensive collection of files with detailed information about the private lives of numerous prominent individuals, including presidents, members of Congress, and Supreme Court Justices. Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Freedom*, 75 SO. CAL. L. REV. 1083 (2002).

[119] *$124,570 U.S. Currency*, 873 F.2d at 1246.

will be called and the evidence is wholly admissible.[120] The fact that routine airport screening searches will occasionally lead to discovery of contraband and apprehension of law violators does not alter the essentially administrative nature of the screening process nor render the searches unconstitutional. However, if the screening process is subverted into a general search for evidence of crime, courts must exclude the evidence obtained.[121]

The government could meet this second burden by giving binding assurances that the security information gathered would not be used for any other purposes than airport security, including other law enforcement purposes. Perhaps it could create a private cause of action if it intentionally violates this agreement. However, it will be tempting to use the compiled information for a wider range of law enforcement objectives than is mandated. If CAPPS II can use its pattern matching to identify suspects and solve crimes while the suspect is standing unarmed in an airport, it is understandable that the government would want to take advantage of the opportunity to make an arrest. However, the suspect would have grounds to argue that the arrest was unlawful due to the violation of the administrative search exception.

3. *Administrative Searches Must Not Be Subject to an Individual Officer's Discretion*

In addition, to qualify as a warrantless administrative search, the government must demonstrate that all persons are searched equally no matter what level of suspicion they may arouse.[122] Another way the Court has phrased this is that the decision to search a particular person must not be subject to the discretion of the particular officer in the field.[123] For this reason, sobriety checkpoints where everyone is examined have been permit-

---

[120] *Davis*, 482 F.2d at 893. Passengers will be arrested when contraband is coincidentally found during a routine baggage search. In fact, as a result of tighter security in just one airport (Honolulu), in the six months following September 11, officials arrested 30 individuals and seized $273,000 in drugs. In the six months before stricter security was employed, only two persons were arrested with only $200 worth of drugs total according to Ed Howard, acting supervisor for the state Narcotics Enforcement Division. War on Terror Aids War on Drugs, HONOLULU STAR-BULLETIN (Mar. 19, 2002), *available at* http://starbulletin.com/2002/03/20/editorial/editorials.html.

[121] *Id.*

[122] *Martinez-Fuerte*, 428 U.S. at 543.

[123] *Camara*, 387 U.S. at 536-37.

ted.[124] In the past, all airline passengers have been subjected to exactly the same screening. In airline screening and sobriety checkpoints, if the rudimentary inspection gave the officer a reason to suspect driving under the influence or the carrying of a suspicious item to an aircraft, the officer is then authorized to make further findings.

To illustrate, in addressing border patrol checkpoints for illegal aliens, the Supreme Court held "that the stops and questioning at issue may be made in the absence of any individualized suspicion."[125] It was constitutional for the border patrol, after routinely stopping or slowing automobiles at permanent checkpoints, to refer motorists selectively to a secondary inspection area for questions about citizenship and immigration status on the basis of criteria that would not sustain a roving-patrol stop.[126] There was no constitutional violation even if such referrals were made largely on the basis of apparent Mexican ancestry.[127]

Most importantly, the Court said, what made the border control stops permissible was that everyone, regardless of suspicion, was democratically screened,[128] at least initially. This is the most difficult obstacle for CAPPS II to overcome because the primary purpose of the CAPPS II profiling system is to single out individuals who, because of undisclosed factors, pose a higher than average risk to the flight.

However, if the primary purpose of the third requirement is to remove the potential for human discretion and abuse, CAPPS II may prevail. In the border checkpoint case, the Court noted that officers were sufficiently divested of discretion by the immediate referral to a higher-ranking official for the secondary screening. The potential abuse was also curtailed by this immediate review and the official, permanent setting of the checkpoint.

Similarly, the objective algorithms of CAPPS II remove the discretion from any particular officer, whether an agent of the air-

---

[124] *Sitz*, 496 U.S. at 444.

[125] *Martinez-Fuerte*, 428 U.S. at 562.

[126] *Id.* Authorization for a secondary inspection for limited inquiry on the basis of criteria that would not sustain a roving-patrol stop, since the intrusion is sufficiently minimal that no particularized reason need exist to justify it, is analogous to the stop and frisk exception described *infra* section VIII.E.

[127] For criticism of this policy, see Alfredo Mirandé, *Is There a Mexican Exception to the Fourth Amendment?*, 55 FLA. L. REV. 365 (2003).

[128] *Id.*

line, or a TSA security screener. If the passenger's name draws a yellow score, heightened security must follow. If a red score appears, law enforcement must be notified. CAPPS II will actually decrease the importance of having airline employees and security screeners "size up" and evaluate flyers for suspicious behavior. Airline employees and security personnel will still have to be vigilant for suspicious behavior, but they will be assisted by the program that tracks non-apparent suspicious patterns.

Although CAPPS II divests the individual airline agent or security guard of discretion, the criteria used in the profiles are undisclosed. Therefore, it is impossible to know whether any human biases were programmed into the system. Although a computer cannot make a visual assessment of appearance or behavior at a particular moment, there is no guarantee that the computer will select persons in a manner more or less arbitrary than a human agent.

Therefore, it is debatable whether the replacement of an official's human subjectivity with an ostensibly objective computer program will satisfy this prong. However, if the TSA mandates personal background checks in the name of safety, it is probably less intrusive and more practical to have a computer run them confidentially off-site than to have a security guard or agent evaluate your history and situation as you await a boarding card.[129] Further, the airlines would probably not agree to assume such a discretionary role because of the animosity and liability it would generate. A neutral off-site government computer is better suited for such decisions. Regardless of who does the screening, the ultimate result is the same whether conducted by an agent, an official or a computer: a green light through security, a more elaborate search perhaps accompanied by questioning, or a denial of boarding.

4. Administrative Searches Must Be Reasonable

Finally, administrative screenings must be reasonable under the circumstances. General Fourth Amendment standards of reasonableness in the search context are discussed in the *Katz* analysis. Additionally, in the administrative search context, the Court has specifically stated that the search must be "limited in its intrusiveness as is consistent with satisfaction of the adminis-

[129] On some international flights, particularly on El-Al, security personnel personally question travelers with such inquiries as, "Where are you going? What is your purpose in going there? Who is meeting you?"

trative need that justifies it."[130] Airport screening personnel are bound to use restraint in intruding on the person and possessions of travelers. In addition, a privacy limitation may impact the selection of data that goes into the algorithms. The government is not justified in using all of the private individual information that it has available through its myriad of databases. It must limit collection and use of information to that which specifically indicates peril to airlines, neither human faults or foibles, nor other conclusions that can be drawn from the array of information available.

Of course, the classified nature of the programs makes judicial review difficult to accomplish. Yet, due to the importance of carving exceptions into the Fourth Amendment and to the long-term ramifications of court decisions, the Court wants the administrative search exception construed narrowly.[131] When deciding whether an administrative search is permissible, courts must not merely consider just the facts of the case before them, but must consider all "searches permissible under the scheme."[132] To consider all possible searches resulting from hundreds of different factors on hundreds of millions of travelers per year is not possible, even in theory. Use of the reasonableness standard here is simply too vast to apply in every possible situation, including hypothetical situations. The Court would have to simply make a judgment as to whether the tests sound reasonable, and it probably will not venture to guess, given the lack of information forthcoming from the TSA on the variable factors. With the strict limits on the administrative search doctrine, it is uncertain whether the courts would approve of the reasonableness of CAPPS II or the use of profiling at all, even though the doctrine was developed partly for airline searches.

E. The Stop-and-Frisk Exception

The second type of Fourth Amendment exception under which a potential airport security technique may qualify is the stop-and-frisk exception. Under this type of exception, if security personnel have a minimal level of justification that a person may pose a threat of danger, they may conduct, without a warrant, a limited search of that person for the presence of weapons.

---

[130] *Martinez-Fuerte*, 428 U.S. at 543.

[131] *Soyland*, 3 F.3d at 1316.

[132] *Id.*

This exception was established in *Terry v. Ohio*,[133] where a Cleveland police officer frisked two suspects and found guns. He did not have a warrant to search the men. The Court allowed the evidence of the search to be admitted despite the fact that the officer was unable to prove a threshold level of probable cause.[134] It stated that the officer's objective observations of the men staring into a storefront window a total of 24 times showed suspicious behavior justifying a minimal search. The Court decided that although the officer had not established probable cause,[135] his objective observations of the men's suspicious behavior provided enough justification.

Subsequent cases have further clarified what exactly constitutes a minimal level of objective justification. In *United States v. Cortez*,[136] the Supreme Court decided that the "totality of circumstances" may be considered in determining if suspicion exists. Security personnel need more than a hunch to conduct a stop-and-frisk search, but they need not establish probable cause. At airports around the world, a hunch is not required, merely a beep from a metal detector. More precisely, given all of the circumstances, the suspicion must be based upon an enhanced likelihood that the person poses harm. To qualify for this test, the CAPPS II system must actually be effective in determining who poses an increased threat.

CAPPS II-based security screening appears to qualify for the motivational portion of the stop-and-frisk exception. By targeting people fitting a suspicious profile, the TSA would argue that CAPPS II establishes sufficient objective justification.

Whether the intrusion is minimal is another issue. Complaints from passengers who have been wrongly placed on the existing TSA "watch list" or no-fly list have complained, describing hours of interrogation, strip searches, and missed flights as a result of their "selection."[137] Airline passengers who get a green

---

[133] Terry v. Ohio, 392 U.S. 1, 19 (1968).

[134] *Id.*

[135] Probable cause is difficult to describe in the abstract, but basically, it is a reasonable belief that a person has committed a crime. The test the court of appeals employs to determine whether probable cause existed for purposes of arrest is whether facts and circumstances within the officer's knowledge are sufficient to warrant a prudent person to believe a suspect has committed, is committing, or is about to commit a crime. United States v. Puerta, 982 F.2d 1297, 1300 (9th Cir. 1992).

[136] United States v. Cortez, 449 U.S. 411, 417-18 (1981).

[137] In a recently resolved FOIA lawsuit between the TSA and EPIC, the TSA released approximately 100 complaint letters written to the TSA by passengers

light from the CAPPS II system will still be subject to random "stop and frisk" searches. Presumably those drawing a yellow light or a red light will be subject to more than a brief, minimal search. Depending on how far the courts are willing to stretch the definition of "limited searches," it is debatable whether CAPPS II will qualify for an exception under the stop and frisk standards, at least for those passengers requiring heightened scrutiny.

F. Consent and Implied Consent Doctrine

Like other civil rights, the Fourth Amendment may be waived. One may consent to a search of the person or premises by officials who have not complied with Constitutional requirements. The burden is on the prosecution to prove the voluntariness of the consent,[138] and awareness of the right to decline the search, and thus, not fly. The reviewing court must determine on the basis of the totality of the circumstances whether consent has been freely given or has been coerced.[139]

Officials are not required to inform a person of his Fourth Amendment rights to resist an airport search, as they are required to give a Miranda warning to an arrestee.[140] The only requirement is that the officials do not indicate that the suspect is not free to leave.[141] In other words, the person must not feel coerced, and must feel that he or she is free to leave. Of course,

---

who were detained, questioned, and/or denied boarding in recent months. The pattern establishes that these detentions were not minimal. *See* EPIC, *Recently Concluded Matters, at* http://www.epic.org (last visited Jan. 20, 2004).

138 *See* Schneckloth v. Bustamonte, 412 U.S. 218, 248-49 (1973) (discussing factors used to determine if consent is voluntary). Consent must be voluntary and free of duress and coercion. *Id.* The fact finder considers the totality of the circumstances to determine if voluntariness was present. The Court also decided that while knowledge of the right to refuse is a factor in the determination of voluntariness, it is not essential to demonstrating consent. *Id.* at 249. While it is clear that an individual may expressly waive constitutional rights through consent, the problem arises in the context of whether a passenger automatically consents to a search as a precondition to boarding the aircraft. Several commentators have held that under such circumstances, the "voluntariness" element is lacking.

139 *$124,570 U.S. Currency*, 873 F.2d at 1246. *But see Schneckloth*, 412 U.S. at 249 (stating that individual's knowledge of right to refuse is not element of valid consent).

140 *Id. See also* Miranda v. Arizona, 384 U.S. 436 (1966). Miranda is fundamentally a due process case and does not involve the Fourth Amendment directly. However CAPPS II may pose 14th Amendment due process concerns, but this is beyond the scope of this paper.

141 *Id.*

according to federal law, airlines must deny a person access to the flight if the person does not consent to the physical search or refuses to present identification so that the CAPPS II search can be performed.

Have we already waived our rights by passing through current airport security? The Second Circuit has hinted that implied consent is something that is inherent and obvious in airport screening.[142] The court in *Davis* recognized that in the airport screening area, the passenger has a choice of submitting to the search or leaving.[143] If the individual chooses to proceed, a relinquishment of Fourth Amendment rights occurs.[144] Of course, all of these rules apply to routine and random physical searches of individuals and luggage. These rules have not yet been applied to an electronic information screening technique where the violation is not to the person directly, but to privacy interests in the abstract. Furthermore, the vast majority of travelers are oblivious to the fact that their backgrounds are being checked. Even if they knew that they were being investigated, the secret nature of the CAPPS II system makes it impossible to give knowing, voluntary consent. If consent is not "knowing," it cannot be given or implied. Therefore, the implied consent doctrine applies to the physical portion of the search, but there is no waiver of consent to the surreptitious background check.

G. National Security Exception

Nothing like September 11th has happened before, so it is difficult to predict how Congress and the courts will view the liberty versus security tradeoff offered by CAPPS II. In times of war or national emergency, civil liberties have, for better or for worse, been sacrificed in the name of safety and security.[145]

Although the *Katz* test has many applications, it may not apply to issues of national security. In a concurrence of the *Katz*

---

[142] United States v. Edwards, 498 F.2d 496, 501 (2d Cir. 1974). "[I]t would outrage common sense to suppose that an intelligent woman, neither blind nor deaf nor ignorant of the language, was not aware as the district judge found 'that she was as free to step out of the line of passengers (as she had been to enter that line) if she did not want her baggage to be searched." *Id.* (quoting United States v. Edwards, 359 F. Supp. 764, 767 (E.D.N.Y. 1973)).

[143] *Davis*, 482 F.2d at 893.

[144] *Id.*

[145] For example, the detention of Japanese-Americans in World War II was justified using the national security exception. *See* Korematsu v. United States, 323 U.S. 214 (1944).

case,[146] Justice White explicitly preserved the possibility that in the case of "national security," electronic surveillance upon the authority of the President or Attorney General could be permissible without prior judicial approval. He reasoned that "domestic security surveillance may involve different policy and practical considerations from the surveillance of 'ordinary crime.'" In a foreshadowing of CAPPS II he explained,

> The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens . . . the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection.[147]

IX. CONCLUSION

Reasonable minds will differ on which is the bigger threat: sporadic terrorists or daily submission to intrusive government surveillance. CAPPS II is so novel that it doesn't precisely fit any of the Fourth Amendment prohibitions or exceptions. Further, the program is targeted at thwarting terrorism, which, unlike most crimes, has national security implications. CAPPS II involves public policy as much as law. Judges in favor of the program will find something in the Fourth Amendment that can sustain it, and those opposed will likewise find grounds to strike it down. However, the Department of Homeland Security is not investing billions of dollars into a system that it believes will be struck down by the courts.

In the court of public opinion, many people will be indifferent, and some fearful fliers will view the program with relief. Others will be outraged at being treated as criminal suspects by a massive government data surveillance system shrouded in secrecy. The issue is political and philosophical. In the words of Benjamin Franklin: "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor

---

[146] *Katz*, 389 U.S. at 363-64.

[147] *Id.*

safety."[148] And in the words of Sun Microsystems' CEO Scott McNealy: "You have Zero privacy anyway—get over it!"[149]

---

[148] The Quotable Franklin, *available at* ttp://www.ushistory.org/franklin/quotable/quote04.htm (last visited Feb. 24, 2004).

[149] Wired News, *Sun on Privacy: 'Get Over It'* (Jan. 26, 1999), *available at* http://www.wired.com/news/politics/0,1283,17538,00.html; Information Week, *Privacy Tools and Services Debut* (Aug. 20, 2001), *available at* http://www.informationweek.com/story/IWK20010816S0005.


SOUTHERN METHODIST UNIVERSITY
DALLAS, TEXAS

Casenotes


SOUTHERN METHODIST UNIVERSITY
DALLAS, TEXAS