COMPUTER ASSISTED PASSENGER PRESCREENING SYSTEM ("CAPPS II"): NATIONAL SECURITY V. CIVIL LIBERTIES

Valerie Alberto
Dominique Bogatz

Two and one half years have passed since the terrorist attacks of September 11, 2001. United States efforts in the war on terrorism and the measures taken to enhance United States security present the unique challenge of balancing national security and protecting our civil liberties. Computer Assisted Passenger Prescreening System ("CAPPS II"), a security measure taken to protect air travel, is indicative of the challenge to provide enhanced security without violating our civil liberties.

CAPPS II was proposed by the Department of Transportation ("DOT") to ensure international and domestic flight safety. The system promises to make air travel safer. There are, however, substantial risks associated with the implementation of CAPPS II including potential violations of passengers' civil liberties.

This paper will present an overview of the CAPPS II system. We consider the benefits and risks related to the implementation and operation of CAPPS II in U.S. airports. The civil liberties concerns include the right to travel, the right to privacy, and issues related to the First and Fourth Amendments. We also briefly discuss the recent Jet Blue incident, the European Union's reaction to CAPPS II and a recently settled lawsuit against the Transportation Security Administration ("TSA").

CAPPS II: THE BEGINNING OF THE FUTURE

> "Your papers, please!"
>
> "Mind if I check your secret dossier and perform some web searches on you?"
>
> "I see you plead guilty to marijuana possession in 1983?"
>
> "Wasn't that you who wrote a piece critical of the first Bush Administration?"
>
> "You have more than five outstanding parking tickets. I'll have your car seized."
>
> "You are due for an IRS audit soon; you seem to be flying a lot more than your reported income would support." [1]

The war on terrorism put "two vital, deeply grounded principles of American government on a collision course."[2] On the one hand, the President has an unquestioned responsibility to protect the nation against foreign attacks and to prevent hostile foreign powers from conducting covert intelligence activities within our borders. On the other hand, law enforcement power, always potentially dangerous to a free society, may operate only within boundaries established by law.[3]

Despite stiff resistance from airlines and privacy advocates, the U.S. government plans to push ahead this year with a vast computerized system to probe the backgrounds of all passengers boarding flights in the U.S.[4] CAPPS II will be used to facilitate the conduct of an aviation security-screening program, including risk assessments of passengers to ensure aviation security.[5]

The original CAPPS program was developed in 1996 by Northwest Airlines as a temporary measure to assist in passenger bag screening. The program was instituted as a response to the 1996 crash of TWA

800 and to the Atlanta Olympics bombing, both thought to have been terrorist acts.[6] CAPPS identified certain passengers as risky based on assumptions about how terrorists travel. Passengers were flagged for additional screening if they bought one way tickets or paid with cash.

Since September 11, the aviation industry has undergone many changes to strengthen airport security.[7] TSA was created and placed in charge of passengers and baggage screeners, who are now federal employees.[8] Some of the other measures considered to improve aviation security, such as improved training for airport screeners, checking luggage for bombs, strengthening cockpit doors and placing air marshals on flights, do not implicate privacy interests and may be sound security measures.[9] Others, however, present civil liberties issues for air travelers.

CAPPS II was proposed by TSA on August 1, 2003, to combat terrorism and prevent another hijacking of U.S. airlines. CAPPS II is designed to improve the screening of both dangerous things and people by relying on experimental data-mining algorithms to find patterns in government and commercial databases.[10] If implemented, CAPPS II would allow TSA to access personal information regarding airline passengers and to use it to "tag" them according to how much of a threat they appear to pose to the safety of those on a flight.[11]

Under the program, all airline passengers will be required to provide their full name, home address, home telephone number and date of birth. Selected information will be transmitted to commercial data providers, for the purpose of authenticating passenger identity. The commercial data providers will transmit back to TSA in as little as five seconds, a numeric score, that will indicate the percentage of match accuracy between the commercial data and the data held by TSA. This will allow TSA to have a reasonable degree of confidence that each passenger is who she or he claims to be. Once CAPPS II has authenticated a passenger's identity, it will conduct a risk assessment. The information will be pulled from disparate sources including public records, criminal records and intelligence information records, and will determine the likelihood that a passenger is a known terrorist, or has identifiable links to known terrorists or terrorist organizations.[12]

Based on the discovered information from commercial, national security sources and intelligence data, TSA will assign a red, yellow or green score to the risk assessment, which will be encrypted on the passenger's boarding pass. A red score means that a passenger appears to pose an imminent threat to the physical safety of the people on the plane and will not be allowed to board the flight. If one is flagged as red, he may not only be denied boarding, but may also undergo police questioning and possible arrest. A yellow score means that a passenger appears to pose a potential threat and must undergo further security checks before being allowed to board. A green score means that a passenger does not appear to pose a threat to safety and is free to board the plane.[13]

The benefits of CAPPS II include authentication of a passenger's identity and a terrorist risk assessment. Bank and medical records will not be used, nor will information regarding an individual's creditworthiness. For the vast majority of passengers, the information collected will be discarded within a few days of the successful completion of the itinerary.[14] Commercial database operators will be prohibited by TSA from storing or using the passenger's records for commercial purposes. No link between the passenger's records in the private sector and that individual's records within the CAPPS II system will be created.[15] In addition, CAPPS II promises to lower passenger wait times by reducing the number of people who must undergo secondary screening or who are consistently misidentified as potential terrorists.[16]

There are many potential problems with CAPPS II. Integrating data from different sources brings with it the problem of different meanings for the same terms, different terms for the same person or entity, and differing units and measures.[17] Various governmental agencies, which will serve as sources for CAPPS II information, may use simplified or shortened terms that are familiar to them, but unfamiliar to the CAPPS II program. Additionally, confusion may occur between units and measures as well as between persons or entities. There is also a possibility that terrorists could bypass the system by investigating it or by committing identity theft, obtaining a false driver's license or passport using the names and dates of birth of innocent individuals.

The cost of CAPPS II will likely be high due to the expense of sophisticated profiling systems, the need to reconfigure existing airline and travel agents' systems, and for the maintenance and transmission of data that CAPPS II will require. In addition, identifying patterns generated by terrorists through data mining may be difficult because there is no efficient way to identify terrorist behavior to identify such patterns.[18] CAPPS II could be used for purposes other than preventing terrorism, including locating drug dealers and deadbeat fathers. It could be utilized in train and bus stations, secure office buildings and thereby may fall victim to function creep.[19] It is unknown at this time whether passengers listing a cell phone number instead of a home phone number would be allowed to fly.[20]

There are potential serious legal issues that must be taken into account with the implementation of the CAPPS II system.[21] The proposed program could affect the right to travel, the right to privacy, and certain other First, Fourth and Fifth Amendment rights. It is unknown whether passengers who will not or cannot provide the information required by CAPPS II will be allowed to fly at all.[22]

THE RIGHT TO TRAVEL

The Supreme Court has held that there is a fundamental right to travel and to interstate migration within the U.S. protected by the Fifth Amendment. Laws that prohibit or burden interstate travel within the U.S. must meet strict scrutiny. Under strict scrutiny, the law will be upheld if it is necessary to achieve a compelling governmental purpose. The court must regard the law as the least restrictive or least discriminatory alternative.[23] The government may have a difficult time establishing that CAPPS II is the least restrictive alternative to prevent hijacking of U.S. planes due to the significant burden it places on U.S. citizens.

In 1999, the U.S. Supreme Court held, in *Saenz v. Roe*,[24] that the right to travel is fundamental, despite the fact that the word "travel" is not found in the text of the Constitution.[25] Quoting *Shapiro v. Thompson*,[26] the Court stated that "the right is so important that it is

'assertable against private interference as well as governmental action… a virtually unconditional personal right, guaranteed by the Constitution to us all.'"[27] In addition, the Court asserted that the right to travel embraces at least three different components; "…it protects the right of a citizen of one State to enter and to leave another State, the right to be treated as a welcome visitor rather than an unfriendly alien when temporarily present in the second State, and, for those travelers who elect to become permanent residents, the right to be treated like other citizens of that State."[28] At a minimum, the right to travel includes the right to go from one place to another, including the right to cross boarders while en route.[29]

CAPPS II could burden the constitutional right to travel. The system affects the right to pass through a state and the right to free movement from state to state.[30] If a passenger is assigned a yellow or red risk score, they will be questioned and possibly deterred from or even denied the right to travel, in violation of the Fifth Amendment.[31]

The secrecy surrounding the risk assessment phase may increase the risk of error, abuse and discrimination in its application. There is no real notice offered when it comes to describing the internal risk assessment process whereby travelers will be flagged as likely terrorists or as persons with links to terrorism.[32] It is unclear what internal government data will be examined during the risk assessment stage. Classified intelligence information may also be used to determine the likelihood that a passenger is a terrorist or has terrorist ties.[33]

FIRST AMENDMENT AND EQUALITY ISSUES

The Case Against CAPPS II & Airport Profiling

The CAPPS II program may create an undue burden on the First Amendment right to speak, associate and worship freely. The system may also result in racial profiling and unequal and discriminatory treatment.[34] The American Civil Liberties Union ("ACLU") suggests a three prong analysis to be used by Members of Congress before implementing additional security measures. First, any new security

proposals should be genuinely effective, rather than creating a false sense of security. Second, security measures should be implemented in a non-discriminatory manner. Individuals should not be subjected to intrusive searches or questioning based on their perceived or actual race, ethnic origin, and religion or based on proxies for such characteristics. And third, if a security measure is determined to be genuinely effective, the government should work to ensure that its implementation minimizes its costs to fundamental freedoms.[35] Opponents of profiling claim that profiling may be an ineffective security measure that may result in illegal discrimination and violation of individual rights.

Profiling is an ineffective security measure

From one perspective, profiling systems will always be one step behind terrorists. A terrorist who "fits the profile" can easily plant a bomb on someone who does not fit the profile.[36] From a security perspective, profiles are under-inclusive. A profile alone does not establish articulable suspicion.[37] Focusing on the many Arabs, South Asians, Muslims and Sikhs who clearly pose no threat to national security detracts from the anti-terrorism effort.[38] It diverts law enforcement resources away from investigations of individuals who have been linked to terrorist activity by specific and credible evidence. It ignores the possibility that someone who does not fit the profile may be engaged in terrorism, or may be an accomplice to terrorism.[39]

Profiling criteria could result in illegal discrimination

Under CAPPS II, TSA has instructed the airlines that when they are confronted by air travelers without identification who insist on their right to travel anonymously, they should either refuse to allow the traveler aboard the airplane or label the traveler as a "selectee", and then conduct a more intrusive search. Thus, it could be claimed, as it was by the plaintiff in *Gilmore v. Ashcroft*,[40] that CAPPS II unconstitutionally burdens the right to equal protection of citizens who seek to maintain their anonymity. This plaintiff claimed that CAPPS II creates an invidious classification of anonymous travelers, by arbitrarily forcing an entire class of citizens to endure a higher degree of intrusive searches than those endured by other citizens.[41]

The most offensive profiles are those that are based on immutable characteristics and have no causal relationship to terrorist activity such as race, religion, national origin, gender, sexual orientation or political opinion. In the month following the September 11 attack, many Arab Americans were thrown off airplanes even after they submitted to intrusive security procedures and were cleared by security.[42]

TSA has failed to include a safeguard mechanism to ensure that the system is not used to unfairly target racial, religious and ethnic minorities.[43] Instead, CAPPS II will contain a special registry of government officials, holders of security clearances, those in "positions of trust and confidence" and those "otherwise deemed not to require heightened security."[44] A trusted traveler list will provide for a privileged class of Americans who will receive special treatment at our airports. (Membership in the exclusive club of CAPPS II exemptees.)[45] Aside from the potential for this list to evolve into a privileged class of Americans who receive special treatment, it leaves open the potential for security breaches by those with security clearances such as the one committed by the military chaplain arrested last September for spying.

The Case for CAPPS II & Airport Profiling

To achieve near perfect airline security, each passenger would have to be extensively questioned and have their luggage thoroughly searched.[46] This would burden passengers by requiring a longer boarding time and would harm the airlines and airports by requiring additional staff and expense to conduct the extensive searches.[47] In order to avoid the burden that searching every passenger would incur, profiling could be used selectively to target passengers for additional searches and questioning when flagged by the CAPPS II system as a potential threat. In 1997, USA Today reported that "some terrorism experts say it's prudent to look carefully at those with Middle Eastern connections because of terrorist groups with roots there."[48] This holds true today as the U.S. continues to fight its war on terrorism in Afghanistan and Iraq. Profiling could be a rational and reasonable response to the threat of terrorism because it would protect U.S. lives. Anyone who doubts the need for such a system need only look to a recent event, where two Pakistani individuals, on the terrorist watch list, were arrested attempting to board an airplane in Seattle after

apparently having just entered the country from Canada.[49] Both men were on the No Fly List and paid cash for their one way tickets. This is a demonstration of how agencies working together and sharing intelligence make our skies safer for the traveling public.[50]

Fourth Amendment Issues

A Fourth Amendment search occurs when a government intrudes into an area where a person has a reasonable expectation of privacy. What is reasonable under the Fourth Amendment depends on the circumstances. CAPPS II may impose an undue burden on the right to be free from unreasonable searches and seizures. The purpose of airport searches (including CAPPS II, x-ray and physical searches) is to detect weapons and explosives and prevent them from being brought aboard aircraft. This safety-related purpose is what makes airport searches constitutional under the Fourth Amendment.[51] CAPPS II will also be used for purposes of the detection of outstanding state or federal warrants and will be linked with the U.S.-VISIT system for checking the validity of immigration and visitor visas. Arguably, CAPPS II will convert every domestic airport to a "border" where people can be arbitrarily identified, searched and/or seized. So viewed, these purposes violate Fourth Amendment limits imposed in *U.S. v. Davis*,[52] which held that for an administrative screening to be a "reasonable search", it must be limited in its intrusiveness and consistent with the satisfaction of the administrative need that justifies it.[53] These purposes also conflict with *Torbet v. U.S. Airlines*,[54] where the Ninth Circuit held that searches to prevent airline hijacking or to detect the presence of weapons and explosives, must be "confined in good faith to that purpose."[55]

The precise contours of any rules relating to the use of any new technology or new program will depend, ultimately on exactly what the new program is capable of or intended to accomplish, the more powerful the system or program, the greater the safeguards necessary.[56]

Privacy Issues

The multiple interests protected by privacy rights include the "claim of individuals, groups or institutions to determine for themselves

when, how, and to what extent information about them is communicated to others."[57] Privacy protections limit governmental intrusion into a sphere of personal conduct and relations by defining the boundaries between the individual and the government.[58] As a general matter, an individual cannot expect to have a constitutionally protected privacy interest in matters of public record.[59]

CAPPS II will have the ability to facilitate the linkage of various fragments of data to comprise an amalgamated picture of a passenger and will in effect create a "dossier" on every passenger. Although much of the information used by CAPPS II will come from public records, courts have held that the right to privacy may be invaded through extensive cataloguing of information normally disconnected and anonymous.[60]

Individuals may have a right to be free from government disclosure of personal information that was acquired for a specific, limited purpose.[61] The Privacy Act of 1974,[62] stands for the general proposition that secret files should not be maintained and kept on U.S. citizens by their government.[63] There are, however, several exceptions to the general rule, one of which concerns national security.[64] CAPPS II exempts risk assessments and profiles from the Privacy Act, including the information that went into the reports.[65] This is in marked contrast to other countries, such as the members of the EU, which have comprehensive national privacy legislation and have recognized the significance of travel data by putting it in the forefront of their privacy protection systems.[66] CAPPS II will permit collection of unprecedented amount of data on individuals.[67] Passenger name records ("PNRs") maintained by airline reservation systems and travel agencies do not just contain flight reservations and ticket records. PNRs include car, hotel, sightseeing and tour information as well.[68] Travel data information is the largest, most sensitive, and most significant category of personal information not yet subject, in the U.S., to any sector specific federal privacy regulations.[69]

In the Department of Transportation's ("DOT") Notice (the "Notice"), the DOT claims the purpose of the CAPPS II system will be to facilitate the conduct of an aviation security-screening program, including risk assessments, to ensure aviation security.[70] The Notice describes

the routine uses of collected information as ranging from release of information to federal, state and local law enforcement agencies; to contractors performing work to assist TSA in any function relevant to the purpose of the system; to news media which relate to civil and criminal proceedings; to international and foreign governmental authorities in accordance with agreements; to the Department of State and the Intelligence Community to further their efforts with respect to persons determined to be a risk; to airports and aircraft operators in the interest of transportation security, and to the National Archives and Records Administration ("NARA").[71]

The CAPPS II system may lack sufficient controls over who will have access to the sensitive personal information contained within the system. According to the Notice, information in this system will be safeguarded in accordance with applicable rules and policies, including the DOT's automated systems security and access policies. This means that system access will be limited to those individuals who require it to perform their official duties.[72] However, the federal government's record on computer security is poor, according to the GAO.[73] In 1998, the GAO failed 7 of 24 major agencies, including the Department of Health and Human Services ("DHHS"), Department of Justice and the Office of Personnel Management, for having poor computer security.[74]

CAPPS II does not directly collect information from the subject, nor does it inform the subjects of their rights, as the Privacy Act requires.75 Under 5 U.S.C. §§552(e)(2) and (e)(3), agencies are required to collect information to the greatest extent practicable directly from the subject, and, at that time, to give that individual a Privacy Act notice explaining the authority for collecting the information, whether the information is mandatory or voluntary, the purposes and routing uses which may be made of the information, and a statement of the effects on the traveler, if any, of not providing all or any part of the requested information.76 However, TSA does not plan to interact with the travelers themselves to obtain this information.77 TSA proposes to collect information from airlines, from passenger identification shown to airline employees, and from external databases.[78] Although the airlines advise that providing requested information is mandatory, there is no published regulation requiring passen-

gers to provide it and the Federal Aviation Association ("FAA") and TSA have denied that travelers are required to provide it.[79] The Notice provided in CAPPS II does not satisfy the statutory requirements of the Privacy Act and may violate travelers' privacy.[80]

The Notice cites 49 U.S.C. 114 §44901 and §44903 as authority for the maintenance of the CAPPS II system. However, nowhere within either section is there explicit authority to collect or maintain information on travelers. 49 U.S.C. §44901 requires screening of all passengers and property that will be carried in a cabin of an aircraft in air transportation or intrastate air transportation. The screening must take place before boarding and may be carried out by a weapon-detecting facility or procedure used or operated by an employee or agent of an air carrier, intrastate air carrier, or foreign air carrier.[81] However, the statute does not require or authorize the collection of identifying information from travelers, require its provision to the government, authorize its collection by the government, nor authorize a demand for identification by the government.[82]

49 U.S.C. §44903 requires TSA to promulgate "a uniform procedure for searching and detaining passengers and property," but does not authorize or require the collection of identifying information from any traveler, the building of a system of records to store that identifying information, nor a demand for an identification from any traveler. It also provides that "The Secretary of Transportation shall ensure that the CAPPS system or any successor system: (1) is used to evaluate all passengers before they board an aircraft and (2) includes procedures to ensure that individuals selected by the system and their carry-on and checked luggage are adequately screened."[83] However, this statute does not authorize the collection of any identifying information from passengers, building of a system of records to hold any such information or any demand that citizens present any identification documents.[84] CAPPS II purports to broaden "ultra vires" action by the government and to extend the authorization of 49 U.S.C. §44901 and §44903 beyond what is written into those statutes.[85]

Freedom of Information

The most intrusive element of the CAPPS II program, the construc-

tion of an infrastructure for conducting background checks and maintaining dossiers on people who fly, will depend on secret intelligence and law enforcement databases. The use of secret intelligence and law enforcement databases would remove public oversight and control over these background checks.[86]

Although the system is exempt from record access procedures pursuant to 5 U.S.C. §552a(k), the Passenger Advocate's Office, created by TSA, will work with and on behalf of passengers to identify and correct erroneous data that may have been utilized in the authentication or risk assessment modules. U.S. citizens or resident aliens who wish to contest, or seek amendment of, records containing information they provided, which is maintained in the system, may direct their written requests to the system manager.[87] Requests should clearly and concisely state what information is being contested, a copy of the record in question, the reason(s) for contesting it, and the proposed amendment to the record. The request must also contain the requester's full name, current address and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury.[88] If the CAPPS II Passenger Advocate cannot resolve the matter, an appeal for resolution can be made to the DHS Privacy Office. Although non-U.S. persons are not covered by the Privacy Act, such persons will still be afforded the same access and redress remedies. The remedies for all persons will be fully detailed in the CAPPS II privacy policy, which will be published before the system becomes fully operational.[89]

Although the Notice includes procedures for passengers to access their records and to contest or seek their amendment, the procedures only apply to the non-secret aspects of the program.[90]

JetBlue Incident

The danger in creating a program like CAPPS II was highlighted recently when it was revealed that JetBlue Airlines had shared over five million passenger records with an Army subcontractor, Torch Concepts, which then augmented those files by purchasing personal information including income, occupation, family size, and social security number, from a private data aggregator.[91] The end result was

the creation of a detailed dossier on the lives of JetBlue passengers.[92] That data was then used in a data mining experiment in which Torch tried to discover a way to detect terrorists using data on the personal lives of ordinary people.[93]

The "Airline Passenger Risk Assessment", presented by government subcontractor Torch Concepts on April 2, 2003 illustrates prototypes of the system that would use traveler's information and commercial databases to single out "suspicious" travelers. The presentation, available at *http://www.auchdieserschwachsinnmussinsinternet.de/ jetblue-spy.pdf*, shows the risk assessment process, the transactions employed across the broad spectrum, the passenger demographics data base, anomalous demographic information for one passenger, Torch's conclusions, and the risk assessment potential.

The discovery of the Torch Presentation has resulted in extensive news coverage focused on the privacy rights of travelers and on the expansion of CAPPS II. According to the New York Times, JetBlue Airlines' surrender of information on passengers amounts to one of the most serious betrayals of consumer privacy rights by an American business.[94]

Recently, the Electronic Privacy and Information Center ("EPIC") filed a complaint with the DOT alleging that Northwest Airlines committed an unfair trade practice when it released three months of passenger data to the National Aeronautics and Space Administration ("NASA"), in order to facilitate research into a data mining aviation security project.[95] Documents released to EPIC under the Freedom of Information Act indicate that it is likely that the disclosure of information involved more than ten million Northwest passengers.[96] In response to EPIC's complaint, the DOT will review the complaint and determine what action, if any, should be taken.[97]

CAN THE EUROPEAN UNION STOP CAPPS II?

If the European Union refuses to cooperate with the U.S. on CAPPS II, the implementation of the program would be practically impossible. Technically, it would be difficult to separate domestic from foreign

travel records.[98] However, in December 2003, after long negotiations, the EU agreed to share information about its passengers with the U.S., thus enabling implementation of CAPPS II. The Aviation and Transportation Security Act, Public Law 107-71, enacted on November 19, 2001, required international airlines to turn over data about their passengers or face penalties or even lose landing rights in U.S. airports.[99] In Europe, officials prepared legal action against carriers that shared passenger information with the U.S. because it violated Europe's own strict data privacy laws.[100] With the implementation of the U.S.-EU agreement, the airlines will now be able to help the U.S. combat terrorism and still be in compliance with the EU laws.

International airlines will turn over data about their U.S. bound passengers including name, email address, telephone and credit card numbers to DHS's Customs and Border Protection Unit. The U.S. will then screen the data and use it for terrorist investigations and other international probes into crimes such as drug-trafficking and money laundering.[101]

CONCLUSION

The fiscal 2004 DHS Appropriations Act (the "Act"),[102] outlines the requirements for implementation of CAPPS II. The Act includes provisions for testing CAPPS II, the establishment of an internal oversight board and operational safeguards, and a requirement for the GAO to submit a report on CAPPS II by February 15, 2004. The Act, however, does not address the absence of specific federal privacy rules for the travel industry and the overall lack of public awareness concerning the significance of travel data in the wrong hands or used for the wrong purposes.[103] CAPPS II has the potential to make passenger screening more effective because it has the capacity to analyze a broad range of data in real time. The combination of commercial and national security sources and dynamic intelligence data will allow for a timely and appropriate response to security threats.[104] Nevertheless, Congress should provide oversight to guide the development of CAPPS II to prevent the system from infringing on citizens' privacy and civil liberties.[105]

ENDNOTES

[1] Gilmore, John. *Gilmore v. Ashcroft* - FAA ID Challenge Frequently Asked Questions. July 20, 2002 (for more information pertaining to Gilmore's challenge see http://cryptome.org/gilmore-v-usa-faq.htm).

[2] Treverton, Gregory F., *Terrorism, Intelligence and Law Enforcement: Learning the Right Lessons*, June 3, 2003, at 15.

[3] Schulhofer, Stephen J., *The Enemy Within: Intelligence Gathering, Law Enforcement and Civil Liberties in the Wake of September 11*, (New York: The Century Foundation ed., 2002), at 46.

[4] Kehaulani Goo, Sara, *U.S. to Push Airlines for Passenger Records Travel Database to Rate Security Risk Factors*, The Washington Post, Jan. 12, 2004.

5 Federal Register, Vol. 68, No. 10. Jan. 15, 2003, at http://www.access.gpo.gov/su_docs/aces/fr-cont.html.

[6] See http://privacyactivism.org/Item/48.

[7] Rosenzweig, Paul, *CAPPS II Should Be Tested & Deployed, Backgrounder*, No.1683, Aug. 28, 2003, available at www.heritage.org/research/homelandsecurity/bg1683.cfm.

[8] Id.

[9] See http://www.epic.org/privacy/airtravel/.

[10] See http://www.epic.org/privacy/airtravel/profiling.html.

[11] See http://www.eff.org/Privacy/cappsii/.

[12] See http:www.eff.org./Privacy/cappsii/20030930_comments.php.

[13] See http://www.eff.org/Privacy/cappsii/.

[14] See http://www.tsa.gov/public/display?content=708.

[15] U.S. Department of Homeland Security, TSA, Docket No. DHS/TSA-2003-1, *Privacy Act of 1974: System of Records*, at www.eff.org/Privacy/cappsii/20030930_comments.php.

[16] See http://www.tsa.gov/public/display?content=708.

[17] Electronic Frontier Foundation, *Comments on CAPPS II*, at www.eff.org/Privacy/cappsii/20030930_comments.php.

[18] Privacy Office, U.S. Department of Homeland Security, Docket No. DHS/TSA-2003-1, at www.eff.org/Privacy/cappsii/20030930_comments.php.

[19] Id.

[20] Id.

[21] Id.

[22] Id.

[23] Chemerinsky, Erwin. *Constitutional Law, Principles and Policies* (Aspen Law and Business ed., 2002) at 826.

[24] Saenz v. Roe, 526 U.S. 489 (1999).

[25] Id. at 490.

[26] Shapiro v. Thompson, 383 U.S. 745, 757 (1969).

[27] Id.

[28] Id. at 492.

[29] Id.

[30] Privacy Office, U.S. Department of Homeland Security, Docket No. DHS/TSA-2003-1, at http://eff.org/Privacy/cappsii/20030930_comments.php.

[31] See http://freetotravel.org/capps-2.1-comments.txt.

[32] Privacy Office, U.S. Department of Homeland Security, Docket No. DHS/TSA-2003-1, at http://eff.org/Privacy/cappsii/20030930_comments.php.

[33] Id.

[34] Privacy Office, U.S. Department of Homeland Security, Docket No. DHS/TSA-2003-1, at http://eff.org/Privacy/cappsii/20030930_comments.php.

[35] See http://www.aclu.org/news/NewsPrint.cfm?ID=9532&c=133.

[36] Id.

[37] See http://www.aclu.org/news/NewsPrint.cfm?ID=9532&c=133.

[38] *Wrong Then, Wrong Now. Racial Profiling Before & After September 11, 2001,* at www.civilrights.org/publications/reports/racial_profiling/racial_profiling_report.pdf.

[39] Id.

[40] *Gilmore v. Ashcroft*, Pl's Complaint, United States District Court for the Northern District of California, Case No. C-02-3444 SI, filed July 18, 2002.

[41] Id.

[42] See http://www.aclu.org/news/NewsPrint.cfm?ID=9532&c=133.

[43] See http://www.aclu.org/news/NewsPrint.cfm?ID13849&c=206.

[44] See www.aclu.org/news/NewsPrint.cfm?ID=13847&c=206.

[45] Steinhardt, Barry, *Airline Security and Civil Rights*, The Washington Post, Sep. 10, 2003, available at www.washingtonpost.com/ac2/wp-dyn?page-name=article&node=&contentId=A47665

[46] Ibrahim, Nabeel, *The Ethics of Airport Profiling*, Mar. 8, 1999, at http://www.stanford.edu/~ibrahim/writings/sts/profiling.html.

[47] Id.

[48] Alexander, Keith L., *Profiling of Fliers Raises Racial Issue*, USA Today, Sep. 26, 1997, at 1A.

[49] Harden, Blaine, *Two on 'No Fly List' Arrested at Airport*, The Washington Post, Aug. 14 2003, at A2.

[50] Id.

[51] See http://freetotravel.org/capps-2.1-comments.txt.

[52] *U.S. v. Davis*, 482 F.2d 893 (1973).

[53] Id. at 910.

[54] *Torbet v. U.S. Airlines*, 298 F.3d 1087 (Cal. App. 9th 2002).

[55] Id. at 1089.

[56] Id.

[57] Schachter, Madeleine, *Informational & Decisional Privacy* (Carolina Academic Press ed., 2003), at 3.

[58] Id. at 25.

[59] *Doe v. City of New York*, 15 F.3d 264, 268 (1993).

[60] *Nader v. General Motors Corp*., 255 N.E.2d 765 (1970).

[61] See http://www.cato.org//testimony/ct-rp090800.html.

[62] The Privacy Act of 1974, 5 U.S.C. §552 (the "Privacy Act").

[63] Id.

[64] Id.

[65] Pierce, Deborah, *Law & Technology: CAPPS II*, The Seattle Press, Mar. 11, 2003, available at http://www.seattlepress.com/print-10116.html.

[66] See http://hasbrouck.org/articles/travelprivacy.html.

[67] Id.

[68] See http://hasbrouck.org/articles/travelprivacy.html.

[69] Id.

[70] See http://www.access.gpo.gov/su_docs/aces/fr-cont.html.

[71] Id.

[72] Id.

[73] See http://www.access.gpo.gov/su_docs/aces/fr-cont.html.

[74] See http://www.privacyactivism.org/Item/48.

[75] See http://freetotravel.org/capps-2.1-comments.txt.

[76] See http://freetotravel.org.capps-2.1-comments.txt.

[77] Id.

[78] Id.

[79] Id.

[80] Privacy Office, U.S. Department of Homeland Security, Docket No. DHS/TSA-2003-1, at http://eff.org/Privacy/cappsii/20030930_comments.php.

[81] 49 U.S.C. §44901, available at http://freetotravel.org/capps-2.1-comments.txt.

[82] Id.

[83] 49 U.S.C. §44903, available at http://freetotravel.org/capps-2.1-comments.txt.

[84] Id.

[85] Id.

[86] See http://www.aclu.org/news/NewPrint.cfm?ID=12108&c=39.

[87] Direct written requests to: CAPPS II Passenger Advocate, at PO Box 597, Annapolis Junction, MD, 20701-0597.

[88] Id.

[89] Dept. of Homeland Security, TSA, Docket No. DHS/TSA-2003-1, Privacy Act of 1974: System of Record at www.eff.org/Privacy/cappsii/20030930_comments.php.

[90] *Wrong Then, Wrong Now.Racial Profiling Before & After September 11, 2001*, at www.civilrights.org/publications/reports/racial_profiling/racial_profiling_report.pdf.

[91] See http://www.aclu.org/news/NewsPrint.cfm?ID=13847&c=206.

[92] Id.

[93] Id.

[94] Editorial Desk, *Betraying One's Passengers*, N.Y. Times, Sept. 23, 2003, at A30, available at http://query.nytimes.com/gst/abstract.html? res= FBOC1 2F6345EO C708EDDA00894DB404482.

[95] *Northwest Shared Passenger Data with NASA for Research Project, EPIC Complaint Alleges*. The Bureau of National Affairs, Inc. Vol. 72, No. 27, Jan. 27, 2004.

[96] Id.

[97] Id.

[98] *Will Europe Stop CAPPS II?*, available at http://www.dontspyonus.us/europe.html.

[99] Kehaulani, Sara, *EU Agrees to Share Airline Passenger Data*, The Washington Post, Dec. 17, 2003, available at http://www.washingtonpost .com/ac2/wp-dyn/A6526-2003Dec16.

[100] Id.

[101] Id.

[102] The fiscal 2004 DHS Appropriations Act, Public Law 108-90.

[103] Department of Homeland Security Appropriations Act of 2004, Pub. L. No. 108-90, available at http://hasbrouck.org/articles/travelprivacy.html.

On 24 September 2003, Congress enacted H.R. 2555, the "Department of Homeland Security Appropriations Act 2004", which was signed into law by the President on 1 October 2003 and became Public Law 108-90. §519 included the following provisions on CAPPS I, CAPPS II and the "selectee" and "no fly" lists:

(a) None of the funds provided by this or previous appropriations Acts may be obligated for deployment or implementation, on other than a test basis, of CAPPS II that the Transportation Security Administration (TSA) plans to utilize to screen aviation passengers, until the General Accounting Office (GAO) has reported to the Committees on Appropriations of the Senate and the House of Representatives that –

1. A system of due process exists whereby aviation passengers determined to pose a threat and either delayed or prohibited from boarding their scheduled flights by the TSA may appeal such decision and correct erroneous information contained in the CAPPS II system;

2. The underlying error rate of the government and private data bases that will be used both to establish identity and assign a risk level to a passenger will not produce a large number of false positives that will result in a significant number of passengers being treated mistakenly or security resources being diverted;

3. The TSA has stress tested and demonstrated the efficacy and accuracy of all search tools in CAPSS II and has demonstrated that CAPPS II can make an accurate predictive assessment of those passengers who may constitute a threat to aviation;

4. The Secretary of Homeland Security has established an internal oversight board to monitor the manner in which CAPPS II is being developed and prepared;

5. The TSA has built in sufficient operational safeguards to reduce opportunities for abuse;

6. Substantial security measures are in place to protect CAPPS II from unauthorized access by hackers or other intruders;

7. The TSA has adopted policies establishing effective oversight of the use and operation of the system; and

8. There are no specific privacy concerns with the technological architecture of the system.

(b) During the testing phase permitted by paragraph (a) of this section, no information gathered from passengers, foreign or domestic air carriers, or reservation systems may be used to screen aviation passengers, or delay or deny boarding to such passengers.

(c) The GAO shall submit the report required under paragraph (a) of this section no later than 15 February 2004.

[104] Rosenzweig, Paul. "CAPPS II Should Be Tested & Deployed." Backgrounder, No. 1683, Aug. 28, 2003, available at www.heritage.org/research/homelandsecurity/bg1683.cfm.

[105] Id.