TESTIMONY OF

PAUL ROSENZWEIG

SENIOR LEGAL RESEARCH FELLOW
CENTER FOR LEGAL AND JUDICIAL STUDIES

THE HERITAGE FOUNDATION*

214 MASSACHUSETTS AVENUE, NE
WASHINGTON, DC 20002

BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE

SUBCOMMITTEE ON AVIATION

REGARDING

THE TRANSPORTATION SECURITY ADMINISTRATION'S COMPUTER-ASSISTED PASSENGER PRESCREENING SYSTEM (CAPPS II)

17 MARCH 2004

---

* The Heritage Foundation is a public policy, research, and educational organization operating under Section 501(C)(3). It is privately supported, and receives no funds from any government at any level, nor does it perform any government or other contract work. The Heritage Foundation is the most broadly supported think tank in the United States. During 2003, it had more than 200,000 individual, foundation, and corporate supporters representing every state in the U.S. Its 2003 income came from the following sources: Individuals 52%; Foundations 19%; Corporations 8%; Investment Income 18%; Publication Sales and Other 3%. The top five corporate givers provided The Heritage Foundation with 5% of its 2003 income. The national accounting firm of Deloitte & Touche audits the Heritage Foundation's books annually. A list of major donors is available from The Heritage Foundation upon request. Members of The Heritage Foundation staff testify as individuals discussing their own independent research. The views expressed are their own, and do not reflect an institutional position for The Heritage Foundation or its board of trustees.

Good morning Mr. Chairman and Members of the Subcommittee. Thank you for the opportunity to testify before you today on the challenge of maintaining the balance between security and constitutionally protected freedoms inherent in responding to the threat of terror, in the particular context of the Transportation Security Administration's (TSA's) proposed Computer-Assisted Passenger Prescreening System, known as CAPPS II.

For the record, I am a Senior Legal Research Fellow in the Center for Legal and Judicial Studies at The Heritage Foundation, a nonpartisan research and educational organization. I am also an Adjunct Professor of Law at George Mason University where I teach Criminal Procedure and an advanced seminar on White Collar and Corporate Crime. I am a graduate of the University of Chicago Law School and a former law clerk to Judge R. Lanier Anderson of the U.S. Court of Appeals for the Eleventh Circuit. For much of the past 15 years I have served as a prosecutor in the Department of Justice and elsewhere, prosecuting white-collar offenses. During the two years immediately prior to joining The Heritage Foundation, I was in private practice representing principally white-collar criminal defendants. I have been a Senior Fellow at The Heritage Foundation since April 2002.

I note, as well, (with some degree of pride) that I formerly served on the staff of this Committee as Counsel (Investigations) under the Chairmanship of the Honorable Bud Shuster. So this is, in a way, a homecoming for me and I am pleased to be back in this room.

My perspective on the question before you is that of a lawyer and a prosecutor with a law enforcement background, not that of technologist or an intelligence officer/analyst. I should hasten to add that much of my testimony today is based upon a series of papers I have written (or co-authored with my colleagues James Carafano and Ha Nugyen) on various aspects of this topic and testimony I have given before other bodies in Congress, all of which are available at The Heritage Foundation website (www.heritage.org). A substantial portion of my testimony today are derived from a forthcoming law review article entitled "Civil Liberty and the Response to Terrorism" which will be published in the Duquesne Law Review Spring 2004 issue.[1] For any who might have read portions of my earlier work, I apologize for the familiarity that will attend this testimony. Repeating myself does have the virtue of maintaining consistency -- I can only hope that any familiarity with my earlier work on the subject does not breed contempt.

* * * * *

The civil liberty/national security question is *the* single most significant domestic legal issue facing America today, bar none. And, as is reflected in my testimony today, in my judgment one of the most important components of a responsible governmental policy addressing this difficult question will be the sustained, thoughtful, non-partisan attention of America's elected leaders in Congress. Nothing is more likely, in my judgment, to allow

[1] *See* Paul Rosenzweig, "Civil Liberty and the Response to Terrorism," 42 Duq. L. Rev. __ (2004) (forthcoming)

America to find the appropriate balance than your engagement in this issue. What I would like to do today is assist your consideration of this question by sharing with you some general principles regarding the nature of the threat and then nature of the liberty interest at stake, which underlie my analysis of the CAPPS II program. Then I'd like to apply those principles to the concrete issues raised by the CAPPS II program. Finally, I will offer some thoughts on aspects of CAPPS II where innovative technological solutions may answer some of the challenges the program confronts and ways in which the technological programs that underlie CAPPS II can aid security even if CAPPS II is not implemented in its current proposed configuration.

I. The Threat of Terrorism – Type I and Type II Errors

The full extent of the terrorist threat to America cannot be fully known. Consider, as an example, one domestic aspect of that threat—an effort to determine precisely how many al-Qaeda operatives are in the United States at this time and to identify those who may seek to fly on domestic airplanes in the future. This is the problem to which CAPPS II is directed.

Terrorism remains a potent threat to international security – as the events of last week all too tragically demonstrate. The list of terrorist targets now includes Madrid, Bali, Baghdad, Najaf, Karachi, Istanbul, Mombassa, Jerusalem, Riyadh, Casablanca and of course New York and Washington. The attacks in Spain demonstrate that we cannot return to the "law enforcement" mindset for handling terrorism that existed prior to September 11. Terrorism is not a crime, to be prosecuted after the fact, like murder. We have, in recent months, been tempted to forget this fact – but we cannot.

Let's examine the scope of the problem: The U.S. State Department has a list of over 100,000 names worldwide of suspected terrorists or people with contact with terrorists.[2] Before their camps in Afghanistan were shut down, Al Qaeda trained at least 70,000 people and possibly tens of thousands more.[3] Al Qaeda linked Jemaah Islamiyah in Indonesia is estimated to have 3,000 members across Southeast Asia and is still growing larger.[4] Although the estimates of the number of al-Qaeda terrorists in the United States have varied since the initial attack on September 11, the figure provided by the government in supposedly confidential briefings to policymakers is 5,000.[5] This 5,000-person estimate may include many who are engaged in fundraising for terrorist organizations and others who were trained in some fashion to engage in jihad, whether or not they are actively engaged in a terrorist cell at this time. But these and other publicly available statistics support two conclusions: (1) no one can say with much certainty how many terrorists are living in the

---

[2] Lichtblau, Eric. "Administration Creates Center for Master Terror 'Watch List'." *New York Times*, Sept. 17, 2003.

[3] On an interview on NBC's "Meet the Press," U.S. Senator Bob Graham was quoted as saying, "…al-Qaeda has trained between 70,000 and 120,000 persons in the skills and arts of terrorism." Meet the Press (July 13, 2003).

[4] Hunt, Terence. "Bush shows resolve by visiting Bali." *Chicago Sun-Times*, Oct. 22, 2003, p. 36.

[5] Bill Gertz, "5,000 in U.S. Suspected of Ties to al Qaeda." *The Washington Times*. July 11, 2002.

United States, and (2) many of those who are in the United States may seek to fly on domestic airlines in the foreseeable future.

And, the scope of the problem is enormous. These comparatively few potential terrorists are hidden is a sea of travelers. For 2003 there were over 8.5 million domestic airplane departures, and more than 1.2 million international departures.[6] These planes carried over 552 million domestic and more than 123 million international passengers[7] – each of whom requires some form of individual screening.

These statistics illustrates the difficulty of the problem. The danger to America posed by terrorists arises from the new and unique nature of potential acts of war. Virtually every terrorism expert in and out of government believes there is a significant risk of another attack – and Madrid proves that point. Unlike during the Cold War, the threat of such an attack is asymmetric. In the Cold War era, U.S. analysts assessed Soviet capabilities, thinking that their limitations bounded the nature of the threat the Soviets posed. Because of the terrorists' skillful use of low-tech capabilities (e.g. box cutters) their capacity for harm is essentially limitless. The United States therefore faces the far more difficult task of discerning their intentions and thwarting them. Where the Soviets created "things" that could be observed, the terrorists create only transactions an events that can be sifted from the noise of everyday activity only with great difficulty. It is a problem of unprecedented scope, and one whose solution is imperative if American lives are to be saved.

As should be clear from the outline of the scope of the problem, the suppression of terrorism will not be accomplished by military means alone. Rather, effective law enforcement and/or intelligence gathering activity are the key to avoiding new terrorist acts. Recent history supports this conclusion.[8] In fact, police have arrested more terrorists than military operations have captured or killed. Police in more than 100 countries have arrested more than 3000 Al Qaeda linked suspects,[9] while the military captured some 650 enemy combatants.[10] Equally important, it is policing of a different form – preventative rather than reactive -- since there is less value in punishing terrorists after the fact when, in some instances, they are willing to perish in the attack.

The foregoing understanding of the nature of the threat from terrorism helps to explain why the traditional law enforcement paradigm needs to be modified (or, in some instances, discarded) in the context of terrorism investigations. The traditional law enforcement model is highly protective of civil liberty in preference to physical security. All lawyers have heard one or another form of the maxim that "it is better that 10 guilty go free

---

[6] Bureau of Transportation Statistics, Domestic Segment – Departures (available at http://www.transtats.bts.gov/DataIndex.asp); *id.* International Segment – Departures.

[7] *Id.* Domestic Market – Passengers; *id.* International Market – Passengers.

[8] *See, e.g.* Dana Dillon, *War on Terrorism in Southeast Asia: Developing Law Enforcement*, Backgrounder No. 1720 (Heritage Foundation Jan. 22, 2004).

[9] Slevin, Peter. "U.S. Pledges Not to Torture Terror Suspects." *The Washington Post*, June 27, 2003, p. A01

[10] Taylor, Francis. "Transcript: State Dept Official Says War Against Terrorism Continues." June 9, 2003, available at http://usembassy.state.gov/tokyo/wwwh20030611a6.html

than that 1 innocent be mistakenly punished."[11] This embodies a fundamentally moral judgment that when it comes to enforcing criminal law American society, in effect, prefers to have many more Type II errors (false negatives) than it does Type I errors (false positives).[12] That preference arises from two interrelated grounds: one is the historical distrust of government that animates many critics of CAPPS II. But the other is, at least implicitly, a comparative valuation of the social costs attending the two types of error. We value liberty sufficiently highly that we see a great cost in any Type I error. And, though we realize that Type II errors free the guilty to return to the general population, thereby imposing additional social costs on society, we have a common sense understanding that those costs, while significant, are not so substantial that they threaten large numbers of citizens or core structural aspects of the American polity.

The post-September 11 world changes this calculus in two ways. First, and most obviously, it changes is the cost of the Type II errors. Whatever the costs of freeing John Gotti or John Muhammed might be, they are substantially less then the potentially horrific costs of failing to stop the next al-Quaeda assault. Thus, the theoretical rights-protective construct under which our law enforcement system operates must, of necessity, be modified to meet the new reality. We simply cannot afford a rule that "better 10 terrorists go free than that 1 innocent be mistakenly screened or delayed."

Second, and less obviously, it changes the nature of the Type I errors that must be considered. In the traditional law enforcement paradigm the liberty interests at stake is personal liberty – that is, freedom from the unjustified application of governmental force. We have as a model, the concept of an arrest, the seizure of physical evidence, or the search of a tangible place. As we move into the information age, and deploy new technology to assist in tracking terrorists, that model is no longer wholly valid.

Rather, we now add related, but distinct conception of liberty to the equation – the liberty that comes from anonymity.[13] Anonymity is a different, and possibly weaker, form of liberty: The American understanding of liberty interests necessarily acknowledges that the personal data of those who have not committed any criminal offense can be collected for legitimate governmental purposes. Typically, outside the criminal context, such collection is done in the aggregate and under a general promise that uniquely identifying individual information will not be disclosed. Think, for example, of the Census data collected in the aggregate and never disclosed, or of the IRS tax data collected on an individual basis,

---

[11] *E.g. Furman v. Georgia*, 408 U.S. 238, 367 n. 158 (1972) (Marshall, J., concurring). The aphorism has its source in 4 Blackstone, Commentaries, ch. 27 at 358 (Wait & Co. 1907).

[12] "In a criminal case ... we do not view the social disutility of convicting an innocent man as equivalent to the disutility of acquitting someone who is guilty .... [T]he reasonable doubt standard is] bottomed on a fundamental value determination of our society that it is far worse to convict an innocent man than to let a guilty man go free." *In re: Winship*, 397 U.S. 357, 372 (1970) (Harlan, J., concurring).

[13] *See* Phillip Kurland, "The private I," *The University of Chicago Magazine*, Autumn 1976, p. 8 (characterizing three facets of privacy, broadly characterized as anonymity, secrecy, and autonomy), *quoted in Whalen v. Roe*, 429 U.S. 589, 599 n.24 (1977).

reported publicly in the aggregate, and only disclosed outside of the IRS with the approval of a federal judge based upon a showing of need.[14]

What these examples demonstrate is not so much that our conception of liberty is based upon absolute privacy expectations, but rather that government impingement on our liberty will occur only with good cause. In the context of a criminal or terror investigation, we expect that the spotlight of scrutiny will not turn upon us individually without some very good reason.

This conception of the liberty interest at stake (the interest that will be lost when Type I errors occur) also emphasizes one other point about privacy – in many ways the implementation of new laws and systems to combat terror are not an unalloyed diminution of privacy. Rather the laws and practices can substitute one privacy intrusion (for example, a search of electronic data about an individual) for another privacy intrusion (the physical intrusiveness of body searches at airports).

Let me record, here, an anecdote that illustrates the point – I've obscured the identifying details a bit to protect my traveling companions' anonymity, but I assure you the incident is true: Recently I was traveling through a small airport in the West that was quite a distance from any border and not an origination point (or arrival point) for any international travel. Thus, the airport was a "low risk" for terrorist infiltration. One of my traveling companions was a female federal judge of adult years – completely outside the profile for a terrorist. Nonetheless, the TSA complement, as part of its routine searches, selected her for a complete screen of her luggage. They proceeded to publicly examine all of her clothing, including the dirty laundry she had accumulated at the conference we had attended, literally displaying her lingerie to anyone who cared to view it. My companion was mortified and hastily urged all of us to go on to the gate and not wait for her, as we had been. I have absolutely no doubt that at that moment, if she had been asked, she would have gladly traded a small amount of electronic privacy that would have verified her identity as a federal judge for the significant physical intrusion she suffered.

But this means that legal analysts cannot make broad value judgments – each person weighs the utility of their own privacy by a different metric. For many Americans, the price of a little less electronic privacy might not be too great if it resulted in a little more physical privacy – for others the opposite result might hold. This suggests little in resolving the tension, save that it cautions against allowing the tension to be resolved by unrepresentative institutions like the courts and in favor of allowing more representative institutions, like the Congress, to do their best at evaluating the multi-variable privacy preferences of the population. I would urge you not, therefore, to be categorical in your condemnation of any form of privacy intrusion – for you are not eliminating all intrusions, merely trading one form for another.

Finally, it bears noting that not all solutions necessarily trade off Type I and Type II errors, and certainly not in equal measure. Some novel approaches to combating terrorism

[14] *E.g.* 26 U.S.C. § 7213 (prohibiting disclosure of tax information except as authorized for criminal or civil investigations).

might, through technology, actually reduce the incidence of both types of error.[15] More commonly, we will alter both values but the comparative changes will be the important factor. Where many critics of governmental initiatives go wrong is, it seems to me, in their absolutism – they refuse to admit of the possibility that we might need to accept an increase in the number of a limited sort of Type I errors. But that simply cannot be right – liberty is not an absolute value, it depends on security (both personal and national) for its exercise. As Thomas Powers has written: "In a liberal republic, liberty presupposes security; the point of security is liberty."[16] The growth in danger from Type II errors necessitates altering our tolerance for Type I errors. More fundamentally, our goal should be to minimize both sorts of errors.

II. CAPPS II

One common critique offered by skeptics of new initiatives to combat terrorism is the concern that advances in information technology will unreasonably erode the privacy and anonymity to which American citizens are entitled. They fear, in effect, the creation of an "electronic dossier" on every American. Attention to this issue has particularly focused on TSA's proposal to use an enhanced information technology program to screen airplane passengers. That program, known as CAPPS II, would effectively conduct a computerized screen of every passenger to assess his or her potential threat as a terrorist.

Since September 11th, the aviation industry has undergone many changes to strengthen airport security. The TSA was created and placed in charge of passenger and baggage screeners (who are now federal employees). It has been using explosives detection systems on 90 percent of checked baggage and substantially expanded the Federal Air Marshal Service. However, little has been done to determine whether a person seeking to board an aircraft belongs to a terrorist organization or otherwise poses a threat. In order to meet this objective, the Transportation Security Administration is developing the Computer Assisted Passenger Prescreening System II (CAPPS II).

Most of the changes made in airport security have focused on looking for potential weapons (better examination of luggage, more alert screeners) and creating obstacles to the use of a weapon on an aircraft (reinforced cockpit doors, armed pilots, etc). A computer-aided system would improve the TSA's ability to assess the risk a passenger may pose to air safety.

A Bit Of History – CAPPS I: The current, limited CAPPS I system was first deployed in 1996 by Northwest Airlines. Other airlines began to use CAPPS I in 1998, as recommended by the White House Commission on Aviation Safety and Security (also known as the Gore Commission).[17] In 1999, responding to public criticism, the FAA limited the use of CAPPS I – using it only to determine risk assessments for checked luggage screening. In other words, between 1999 and September 2001 CAPPS I information was not used as a basis for subjecting passengers to personal searches and questioning – only for

---

[15] *See* K. A. Taipale, "Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data," 5 Colum. Sci. & Tech. L. Rev. 2, 31 (December 2003) (arguing for utility of strong audit technology) (available at http://www.stlr.org/cite.cgi?volume=5&article=2).

[16] Thomas Powers, "Can We Be Secure and Free?" *The Public Interest* (Spring 2003)

[17] *See* White House Commission on Aviation Safety and Security (Feb. 12, 1997) (available at http//www.airportnet.org/depts/regulatory/gorefinal.htm).

screening checked bags. As a consequence even if CAPPS I flagged a high-risk passenger he could not be singled out for more intensive searches.

After September 11 CAPPS I returned to its original conception and is now again used to screen all passengers along with their carry-on and checked luggage. However, the criteria used to select passengers, such as last-minute reservations, cash payment, and short trips are over inclusive. This is a very crude form of pattern-recognition analysis. So crude that it can flag up to 50% of passengers in some instances, mainly in short haul markets.[18] These criteria are also widely known and thus readily avoided by any concerted terrorist effort. Nor does CAPPS I attempt to determine whether or not the federal government has information that may connect a specific perspective passenger with terrorism or criminal activity that may indicate they are a threat to the flight. And it is costly – I've heard informal estimates as high as $150 million per year for domestic airlines to operate the system. As a result, we are wasting resources: it's likely that if Osama bin Laden tried to board a plane today CAPPS would not identify him for arrest or further inspection.[19]

Changing The System -- CAPPS II: The TSA believes that screening what a passenger is carrying is only part of the equation and is developing CAPPS II as a successor to CAPPS I in order to determine whether the individual poses a threat to aviation security. CAPPS II will use government intelligence and law enforcement information in order to assign risk levels to passengers based on real information not arbitrary models. The TSA will then be able to devote more of its resources to those with a higher score (indicating they pose a greater risk), than those deemed to be a lesser concern (although some degree of randomness will need to be retained).

In January 2003, TSA released a Privacy Act notice for CAPPS II, the successor to CAPPS I.[20] Since then, many critics have raised substantial concerns. Some thought that CAPPS II, as originally proposed, was too broad in scope and could infringe on passengers' privacy. Others were concerned that the government should not rely on potentially flawed commercial data to prevent individuals from traveling by air. Some asserted that the use of knowledge discovery technologies on a wide variety of personal data could pose privacy and civil liberty violations. Finally, many wondered if individuals would be able to challenge their score.

---

[18] *See* Robert W. Poole, Jr. & George Passatino, "A Risk-Based Airport Security Policy" Reason Public Policy Institute at 11 (May 2003).

[19] It has been reported that the CAPPS I system was partially effective, flagging nine of the 19 September 11 terrorists for additional screening. *See* National Commission on Terrorist Attacks Upon the United States, "The Aviation Security System and the 9/11 Attacks: Staff Statement No. 3" (Jan. 27, 2004) (available at http://www.9-11commission.gov/hearings/hearing7/staff_statement_3.pdf]); *see also* Sara Goo and Dan Eggen, "9/11 Hijackers Used Mace and Knives, Panel Reports," Wa. Post at A1 (Jan. 28, 2004) (summarizing report). To the extent that is true it emphasizes both that some form of screening can be effective, that the limitation to bag-only screening was unwise, and that however effective electronic screening might be, the human element will always be a factor in insuring the success of any system.

[20] *See* 68 Fed. Reg. 2101 (Jan. 15, 2003).

In August 2003, TSA made available an Interim Final Privacy Notice on CAPPS II, which includes substantial modifications to the initial proposal based on many of the concerns voiced in response to the first Privacy Notice.[21]

Under the Interim Notice, TSA will not keep any significant amount of information after the completion of a passenger's itinerary. Furthermore, TSA anticipates that it will delete all records of travel for U.S. citizens and lawful permanent residents a certain number of days after the safe completion of the passenger's travels (7 days is the current anticipation). TSA has also committed to developing a mechanism by which a passenger targeted for more thorough screening can seek to set the record straight if they think they have been identified in error.

More importantly, the CAPPS II system has addressed privacy concerns by severely limiting the types of private information collected and the way in which commercial data will be examined. The proposed CAPPS II system will access only a "passenger name record" (PNR), which will include information collected at the time the passenger makes the reservations, prior to the flight. Selected PNR information (including name, address, date of birth, and telephone number) will be transmitted to commercial data providers for the sole purpose of authenticating the passenger's identity. This process is similar to the credit card application procedure used to check for fraudulent information.

The way this works is relatively straightforward, and is in common use today in the commercial world. A requesting party, whether TSA or a commercial user, submits information (*e.g.* name, address, phone number and date of birth) about an individual. That identification information is then compared to information held in numerous commercial databases. A numeric score, reflecting the confidence with which an identity is authenticated is then generated for each of the four pieces of information – that score itself is based upon both the quality of the databases queried and the frequency with which matches within the database are found. The scores for each independent data field are then combined for a cumulative score. Commercial data providers will then transmit back to TSA a numeric score indicating the degree of match between commercial data and TSA data, giving TSA a good idea if the person is who they say they are.[22] No commercial data will be retained by the TSA and the commercial companies will retain no travel data.

After the authentication phase, the CAPPS II system will conduct a further risk assessment by comparing that identification information to intelligence and law enforcement data. The thresholds for action can be adjusted generically based upon existing external threat intelligence. If we have information that some form of attack is imminent, the threshold score for enhanced screening can be lowered – and vice versa. Passengers whose identity is confirmed with a high degree of confidence and have no matches with intelligence or law enforcement data will be less likely to receive additional scrutiny, whereas those on the opposite end of the spectrum will likely be searched more thoroughly or arrested as

---

[21] *See* 68 Fed. Reg. 45265 (Aug. 1, 2003).

[22] Absolute certainty of identification is impossible. In practice, all identification will be expressed as a "confidence interval" reflecting an estimate of the degree of certainty in an identification. For most travelers, this confidence interval will be quite high. For a few, who will be subject to greater screening, it will not.

appropriate. This will allow TSA to focus its prevention resources on those passengers who, through a qualitative analysis, are determined to more dangerous.

Assessing The Risks of Type I and Type II Errors: The CAPPS II program poses some interesting and challenging problems in adapting the law to new technology and the realities of new technology to the law. First, if CAPPS II is to be effective its hallmark will be the idea that some form of "result" will necessarily be immediately available to TSA screeners on a "real-time" basis so that they can make near-instantaneous decisions regarding whom to screen or not screen prior to allowing passengers to board the aircraft. If CAPPS II were designed so that detailed personal information on each passenger were transmitted to every TSA screener, all would agree that the architecture of the system did not adequately protect individual privacy. The analysis passed by the CAPPS II system to TSA employees at the airport must be (and under current plans, will be) limited to a reported color code – red, yellow or green – and should not generally identify the basis for the assignment of the code.

Thus, CAPPS II proposes to precisely reverse the privacy protection equation being developed in other contexts. To protect privacy, other information technology program disaggregate analysis from identity by making the data available to the analyst while concealing the identity of the subject of the inquiry unless and until disclosure is warranted. In the reverse of this paradigm, CAPPS II will disclose the identity of the potential threat (through a red/yellow/green system displayed to the screener, warning of a particular individual) but will conceal from the screener the data underlying the analysis – at least until such time as a determination is made that the two pieces of information should be combined. The privacy protection built into CAPPS II is therefore the mirror image of the more common system. It is by no means clear which method of protecting privacy is *ex ante* preferable – but it is clear that the two systems operate differently and if we are to have any sort of CAPPS II system at all, it can only have privacy protections of the second kind.

To reiterate a point made earlier, CAPPS II is not necessarily a decrease in privacy. Rather, it requires trade-offs in different types of privacy. It substitutes one privacy intrusion (into electronic data) for another privacy intrusion (the physical intrusiveness of body searches at airports). It will allow us to target screening resources, while actually *reducing* the number of intrusive searches: Currently 14% of the traveling public are subject to some form of secondary screening. CAPPS II will likely reduce that to 4% for additional screening.[23] CAPPS II may also have the salutary effect of reducing the need for random searches and eliminate the temptation for screeners to use objectionable characteristics of race, religion, or national origin as a proxy for threat indicators.[24] For many Americans, the

---

[23] *See* Transcript of Media Roundtable with DHS Under Secretary Asa Hutchinson (Feb. 12, 2004) (available at www.tsa.gov).

[24] Some purely random searches will need to be retained in order to maintain the integrity of the inspection system and defeat so-called "Carnival Booth" attacks (named after a student algorithm proposing a method of defeating CAPPS). Adding a random factor to the inspection regime answers the problem. *See* Samidh Chakrabati & Aaron Strauss, "Carnival Booth: An Algorithm for Defeating the Computer-assisted Passenger Screening," (available at http://www.swiss.ai.mit.edu/6805/student-papers/spring02-papers/caps.htm) (describing program); Taipale, "Data Mining and Domestic Security," at n. 285 (explaining how addition of random screening guards against such attacks).

price of a little less electronic privacy might not be too great if it resulted in a little more physical privacy, fewer random searches, and a reduction in invidious racial profiling.

Finally, the subject matter of the CAPPS II system calls for heightened sensitivity to the potential for an infringement on protected constitutional liberties. While the Constitution affords no additional protection to information that an individual has made available to other individuals or institutions and while CAPPS II will not directly affect personal physical liberty, which lies at the core of constitutional protections, CAPPS II does implicate at least one fundamental liberty interest guaranteed by the Constitution. Since the 1960s the Supreme Court has recognized a fundamental right to travel[25] – indeed, one might reasonably say that one purpose of the Federal union was to insure the freedom of commerce and travel within the United States.

Thus, there is a risk that a poorly designed system will unreasonably impinge upon a fundamental constitutional liberty. The risk of such impingement should not result in abandonment of the program – especially not in light of the potentially disastrous consequences of Type II error if there is another terrorist attack in the United States. However, we will need stringent oversight to provide the requisite safeguards for minimizing infringements of civil liberty in the first instance and correcting them as expeditiously as possible.

CAPPS II is therefore a paradigm for answering the question of whether or not we can conceive of a suitable oversight mechanism that would appropriately constrain executive authority while allowing its application to circumstances we consider necessary. In my view, the use of CAPPS II should be subject to significant Congressional oversight, including spot checks (in a classified means, if necessary) to insure that the CAPPS II methodology is not being misused. Though the details would need, of course, to be further developed, the outline of such an oversight system might include some or all of the following components:

- CAPPS II should be constructed to include an audit trail so that its use and/or abuse can be reviewed;
- It should not be expanded beyond its current use in identifying suspected terrorists and threats to national security – it should not be used as a means, for example, of identifying drug couriers or deadbeat dads.[26] Thus, the pending proposal to screen for outstanding criminal warrants should be modified;
- The program should sunset after a fixed period of time, thereby ensuring adequate Congressional review;
- CAPPS II should have significant civil and criminal penalties for abuse;
- The "algorithms" used to screen for potential danger must, necessarily, be maintained in secret, as there disclosure would frustrate the purpose of CAPPS II. They must, however, also be subject to appropriate congressional

[25] *Shapiro v. Thompson*, 398 U.S. 618 (1969)

[26] *Cf.* William Stuntz, "Local Policing After the Terror," 111 Yale L. J. 2137, 2183-84 (2002) (use of expanded surveillance authority to prosecute only terrorists and other serious offenses).

scrutiny in a classified setting and, if necessary, independent (possibly classified) technical scrutiny;

- An individual listed for additional screening or prohibited from flying should be entitled to know the basis for his or her listing and should have a mechanism for challenging the listing before a neutral arbiter or tribunal. To the extent practicable the review should be as prompt as possible;
- Because commercial databases may be error-ridden, no American should be totally denied a right to travel (i.e. red-carded) and subject to likely arrest as a suspected terrorist solely on the basis of public, commercial data. An indication of threat sufficient to warrant denial of that right should (except in extraordinarily compelling circumstances) be based only upon significant intelligence from non-commercial sources.
- The CAPPS II system should be designed so that the No-Fly/Red Card designation, though initially made as the product of a computer algorithm, is never transmitted to the "retail" TSA screening system until it has been reviewed and approved by an official of sufficiently high authority within TSA to insure accountability for the system.[27] Nor is there any reason for the underlying data ever to be transmitted to the TSA screener.

To a large degree, the pending CAPPS II proposal is already structured to meet many of these criteria. For example, the software platform under which CAPPS II will operate already incorporates strong audit trail systems to uncover abuse and a use-permission system that limits the potential. The software, known as Radiant Trust, is derived from legacy technology certified by the National Security Agency. It may not be perfect, but it certainly is the best we can produce today. Similarly, current plans are to never impose anything more than enhanced screening on passengers on the basis of commercial data – only governmental data will be used to list a passenger as a "No Fly" risk.

Thoughtful critics have identified at least three potentially significant problems in the current proposed system – the possibility of mission creep, the need for a redress system and the possibility that it will be thwarted by identity theft. Let me address each of these.

Regarding mission creep, I remain a friendly critic of TSA. Given my understanding of the nature of the balance of harms – that is, the nature of the Type I and Type II errors involved – I am one who is willing to alter the scope of permitted government powers, to combat the threat of terror. The closely related point, of course, is that we must guard against "mission creep." Since the justification for altering the traditional assessment of comparative risks is in part based upon the altered nature of the terrorist threat, we cannot alter that assessment and then apply it in the traditional contexts.[28] But this problem is

---

[27] This would mirror the view of the European Union which styles it as a "right" to have human checking of adverse automated decisions. The EU Directives may be found at http://www.dataprivacy.ie/6aii-2.htm#15.

[28] *See* Paul Rosenzweig and Michael Scardaville, The Need to Protect Civil Liberties While Combating Terrorism: Legal Principles and the Total Information Awareness Program, Legal Memorandum No. 6, at 10-11 (The Heritage Foundation February 2003); (arguing for use of new technology only to combat terrorism); Stuntz, "Local Policing After the Terror," 111 Yale L. J. at 2183-84 (arguing for use of information sharing only to combat most serious offenses).

soluble. Congress can and should implement policy limitations regarding this aspect of the CAPPS II implementation. I think that "slippery slope" arguments are basically an appeal to abandoned rationality – we can and should draw rational lines with the expectation that we can adhere to them.

The concerns with regard to redress are also well taken – though not without solution. At this juncture, all we have is a commitment for such a system. Unlike some critics, I certainly anticipate that TSA will honor that commitment and provide a viable redress system – and it is no basis for rejecting a proposal that it has yet to be fully fleshed out. Any system for redress must meet the following criteria:

- It must be administratively nimble and quick, so that false positives who are delayed in travel are corrected as rapidly as possible;
- It must be supple enough to ensure against repetition – that is, the system must accommodate correction in a way that allows an individual to travel in the future without being again mistakenly singled out; and
- There must be independent review of any adverse resolution where the administrative process denies correction.

But these are not impossible criteria. They can be readily met.[29] To be sure, the Congress should oversee the process, but it, too, can be accomplished.[30]

The identity theft problem is somewhat more intractable.[31] Thus, while the technology will allow the resolution of an identity – that is determining whether the identity is a false, created one or not – it cannot resolve the theft of a true identity.[32] Given the limited amount of information being requested in the PNR (name, address, date of birth, and telephone number) it is possible that individuals could pose as people other than themselves readily. The only ways to enhance CAPPS II to fight this prospect are to strengthen it -- by collecting additional information about an individual; to return additional information (for example, gender, height, weight and hair color) to the TSA screener so that the screener could confirm the identity of the individual before him; or by requiring travelers

---

[29] I outlined in more detail an appropriate system of administrative and judicial review for false positives in Paul Rosenzweig, "Proposals for Implementing the Terrorism Information Awareness System," Legal Memorandum No. 8 (The Heritage Foundation August 2003).

[30] One challenge for designing such a process will be the competing impulses of critics who both want CAPPS II to purge individual information rapidly and who want a redress system that must, fundamentally, conduct a review of the individual information. Thus, the presentation of a challenge to a screening decision will need to trigger the retention of data about the individual until the challenge is resolved.

[31] Identity theft – stealing a real identity – should be distinguished from identity fraud – creating a new, fraudulent identity. Identity fraud is a far less difficult problem and is, essentially, solved.

[32] *See* GAO, Aviation Security: Computer Assisted Passenger Prescreening System Faces Significant Implementation Challenges at 29-30 (GAO-04-385) (Feb. 2004) (available at http://www.gao.gov/new.items/d04385.pdf).

to use some verified token or identification with clearance incorporated in it.[33] These are neither technologically easy nor necessarily desirable results – yet the conundrum of identity theft must be solved if CAPPS II is to prove at all useful.[34]

The current architecture of the system offers the best prospect for combating the identity theft problem. CAPPS II will rely on the same structure that commercial users employ using their "best practices." And those commercial users have a significant financial incentive to insuring that the algorithms prevent identify theft. We are thus doing the wise thing in harnessing the discipline of the market place as a means of enabling improvement and change. Also, the use of readily available commercial systems weakens, somewhat, any privacy objection – it is at least a little odd to say that the same system we use daily to verify a credit card application somehow becomes an horrific intrusion when it is used to identify potential terrorist risks.

Of equal significance, the criticism that the CAPPS II system is subject to potential defeat through identity theft misses one of the most significant and important points about enhanced security. We know that ***no*** security system is perfect – thus, instead of relying on a single system of security without backup (a "brittle" system) we prefer to use layered security systems of as many different forms as reasonable, so that the overall security system is flexible – it bends but it doesn't break. The "reasonableness" of a new system depends, of course, on its costs, the level of its intrusiveness, and the ease or difficulty with which it may be defeated. But the mere possibility of defeat is not enough to warrant rejections – and given what we know of how identity verification works in the commercial world (it is highly successful, for example, in Las Vegas identifying gambling cheaters),[35] there is every reason to anticipate that CAPPS II will meet the cost-benefit threshold of utility.

Which brings us to the final question of effectiveness. Of course, before full deployment, CAPPS II needs to demonstrate that it can work.[36] It holds great promise – but

---

[33] *See* K. A. Taipale, "Identification Systems and Domestic Security: Who's Who in Whoville," Potomac Institute for Policy Studies (Jan. 28, 2003) (available at http://www.stilwell.org/presentations/CAS-IDsystems-012804.pdf)

[34] One could also take steps to harden identification cards to ensure they are less readily falsifiable and more certainly government products. *See* Markle Foundation, "Task Force on National Security in the Information Age," App. A "Reliable Identification for Homeland Protection and Collateral Gains" (Dec. 2003) (recommending hardened drivers license identification). Such hardening will not, however, be of great utility unless we also strengthen the authentication process to insure that those seeking identification are who they say they are. Colorado's recent adoption of a biometric face identification mechanism offers some promise of a technological solution to that question. *See* State of Colorado Deploys Facial Recognition Technology to Fight Identity Theft (Digimarc 2003) (reporting detection of 20 attempted frauds per month through facial recognition technology).

[35] *See* Don Clark, "Entrepreneur Offers Solution for Security-Privacy Clash," Wall St. J. at B1 (March 11, 2004).

[36] Thus, I agree with the GAO that CAPPS II must prove its utility. *See* GAO, "Aviation Security" at 13-20. What I find problematic is GAO's critique that the absence of such proof is evidence of problems within the program. Of course CAPPS II needs to be tested and refined – and it should be. *See* James Jay Carafano, Paul Rosenzweig & Ha Nuygen, "Passenger Screening Program is Vital – And Vital to Get Right," Web Memo No. 428 (The Heritage Foundation, Feb. 18, 2004)

promise is far different from reality. Thus, the ultimate efficacy of the technology developed is a vital antecedent question. If the technology proves not to work—if, for example, it produces 95 percent false positives in a test environment—than all questions of implementation may be moot. For no one favors deploying a new technology—especially one that impinges on liberty—if it is ineffective. Thus, CAPPS II must be thoroughly tested. Conversely, we are unwise to reject it before knowing whether the effectiveness problem can be solved.

Some critics are skeptical that CAPPS II can ever work, characterizing it as the search for a "silver bullet" that cannot function because of Bayesian probability problems.[37] That broad statistical criticism is rejected by researchers in the field who believe that because of the high correlation of data variables that are indicative of terrorist activity, a sufficient number of variables can be used in any model to create relational inferences and substantially reduce the incidence of false positives.[38] And, in other environments, enhanced technology allowing the correlation of disparate databases and information has proven to have potentially significant positive uses. American troops in Iraq, for example, use the same sorts of link and pattern analysis, prediction algorithms and enhanced database technology that would form a part of CAPPS II to successfully track the guerrilla insurgency.[39]

It is also important to realize that there may be potentially divergent definitions of "effectiveness." Such a definition requires *both* an evaluation of the consequences of a false positive *and* an evaluation of the consequences of failing to implement the technology. If the consequences of a false positive are relatively modest (e.g. enhanced screening), and if the mechanisms to correct false positives are robust (as recommended herein), then we might accept a higher false positive rate precisely because the consequences of failing to use CAPPS II technology (if it proves effective) could be so catastrophic. In other words, we might accept 1,000 false positives if the only consequence is heightened surveillance and the benefit gained is a 50 percent chance of preventing the next terrorist flight attack. The vital

---

(available at http://www.heritage.org/Research/HomelandDefense/wm428.cfm). But to critique a developmental program for incomplete testing puts the cart before the horse.

[37] *E.g.* Jeffrey Rosen, The Naked Crowd 105-06 (Random House 2004).

[38] *See* Remarks, David Jensen, "Data Mining in the Private Sector," Center for Strategic and International Studies, July 23, 2003; David Jensen, Matthew Rattigan, Hannah Blau, "Information Awareness: A Prospective Technical Assessment," SIGKDD '03 (August 2003) (ACM 1-58113-737-0/03/0008).

[39] *See* AP, "Computer-sleuthing aids troops in Iraq," (Dec. 23, 2003). Any who doubt that, in some form, enhanced information search technology can work need only contemplate the recent arrest of LaShawn Pettus-Brown, whose date identified him as a fugitive when she "Googled" him. *See* Dan Horn, "Fugitive Done in by Savvy Date and Google," USA Today (Jan. 29, 2004) (available at http://www.usatoday.com/tech/news/2004-01-29-google-bust_x.htm). Compare that with the pre-September 11 prohibition (eliminated by the new FBI guidelines) on the FBI's use of Google. *See* L. Gordon Crovitz, "Info@FBI.gov," Wall St. J. (June 5, 2002). At some fundamental level the ultimate question is how to reconcile readily available technology in commercial and public use, with the broad governmental monopoly on the authorized use of force. Whatever the proper resolution, we cannot achieve it by hiding our heads in the sand and pretending that data integration technology does not exist.

research question, as yet unanswered, is the actual utility of the system and the precise probabilities of its error rates.[40]

III. Some Speculative Thoughts and Analysis

Innovation – Since my goal here is to do more than address the status quo let me briefly talk about two innovative ideas that have yet to become part of the discussion of CAPPS II generally and that may offer additional technological or programmatic means of improving the system. I offer them here in outline form – they are by no means fully developed.

The first of these is something that K. A. Taipale of the Center for Advanced Studies has called "verified pseudonymity."[41] In effect, verified pseudonymity, is a form of "traceable anonymity." It would allow the disclosure of relevant and important information while concealing that which is not necessary to disclose. In the credit card context, for example, a merchant doesn't need to know the name of the person carrying the card, he only needs to know that the person is entitled to carry the card and that the card can pay the fee. A card with no name, but with a thumbprint, for example, would work. Similarly, in the air transportation context, the traveler might carry a token with a unique, anonymized identifier and that identifier (rather than his name) could be compared to a database of prohibited travelers. The result would produce the answer that TSA wants – whether the person in question is "safe to travel" – without necessarily requiring disclosure of the individuals identity or other attributes. And the virtue of the "traceable" portion of the anonymity is that if a match is made – if, for example, a traveler is identified as a terrorist threat then (and *only* then) could the government (through legal procedures to be determined by Congress) break the anonymity barrier and identify the individual. To be sure, the technology for this sort of solution to the problem is still in its infancy, but I commend it to the Subcommittee's attention as a possible technological answer to some of the privacy concerns relating to CAPPS II – if only for implementation at a later date.[42]

The second suggestion is an idea of my own, inspired by some consideration of a "Trusted Traveler" program. Let me return to the paradigm that governs my thinking on CAPPS II – as with the federal judge whose dilemma I described, the problem is not one of a privacy invasion. We have long since passed the point where, for example, one could colorably claim a right to travel anonymously (i.e. pay cash, no identification, no name). So some aspects of a travelers' privacy will have to be foregone – the question really is which

---

[40] One final note – though privacy advocates are concerned about the false positives, the existence of an available system also may create civil tort liability for the failure to deploy. It is not fanciful to imagine tort suits against airlines that either do not implement CAPPS II or refuse to cooperate with TSA if by doing so the give rise to a false negative.

[41] The concept I outline here is discussed in more detail in K. A. Taipale, "Technology, Security, and Privacy: The Legend of Frankenstein, the Mythology of Privacy, and the Lessons of King Ludd," Yale J. Law and Technology (forthcoming) (a discussion draft is available at http://www.taipale.org/papers/tsp-yls.htm).

[42] Substantially more information on data anonymization mechanisms (as well as privacy permissioning technology and immutable audits) will be available soon in a forthcoming paper being jointly produced by The Heritage Foundation and the Center for Democracy and Technology. *See* James X. Dempsey & Paul Rosenzweig, "Privacy-Preserving Data Sharing: Technologies That Can Protect Privacy as Information Is Shared for Counterterrorism Purposes" (forthcoming).

aspects an individual is asked to give up. In other words: how much privacy must we give up and in what mixture?

The precise amount of privacy one gives up must, of course, be calibrated to the level of the threat we experience. One could imagine, as a thought experiment, systems in which one were required to give up *all* physical or electronic privacy in order to fly. Thus, we could require all passengers to fly naked, or let nobody fly who had not passed a full Top Secret security background check. Of course, to suggest either course is to recognize how absurd the proposals are.

Or is it? In my view, we should recognize the reality of a privacy trade-off, and also recognize that different people might make different choices. I was struck, for example, by the fact that there already *was* an airline flight known as "Naked Air." (albeit a bit of a lark).[43] Similarly, though the proposed "Trusted Traveler" program will require something equivalent to a security background check for entrants, it has been reported that many business travelers have expressed an interest in the program.[44] By their choices, Americans are already voicing their preferences.

And that suggests the germ of a further idea – allowing choice for the less frequent traveler of other, more moderate options. We might, for example, envision a system in which a traveler could opt among three possibilities – a "Trusted Traveler" program, a limited electronic screening as embodied in CAPPS II that had on-site electronic screening, and a baggage and personal screening system akin to that which is now randomly applied. Imagine if Americans were empowered to choose – you would be able to either allow an in-depth examination of your personal background (and receive the benefit of no physical screening); a modest examination of your electronic records to verify your identity electronically; or agree to forgo some physical privacy to permit examination of your person and effects. Of course, we would need to know if CAPPS II can work in "real time" at the airport or allow passengers to make the choice at the time they book their trips. Perhaps, given the various values that differing individuals place on different aspects of their privacy, the availability of choice would answer many of the concerns. Again, this is merely a notion, but I offer it for the Subcommittee's consideration.

Risk Assessment and Resource Allocation – I want to close with one other point that I think is worth your consideration – one that is often not remarked upon. I refer to the distinction between the risk assessment and risk avoidance or reduction. This distinction acknowledges the difference between the analysis aspects of CAPPS II and the screening process itself.

Risk assessment – attempting to determine what risks there are and the likelihood of the threat – is an inexact science. But it is a science -- one that we use in rating risks throughout our experience in the commercial world. It is also, at least in theory, completely distinct from the question of risk avoidance/reduction – that is, how we address the risks

---

[43] Inasmuch as this testimony will be posted to the House web site, I will provide the link for this citation in a modified form to preclude a direct access link. You may view the Naked Air web site at www "dot" naked-air "dot" com.

[44] Travelocity reports, for example, that 43% of frequent travelers (with more than 5 trips per year) favor the program. *See* Travel Security Update (Feb. 2002) (available at http://media.corporate-ir.net/media_files/NSD/TVLY/presentations/tvly_022502/sld001.htm).

identified. Risk assessment may inform resource allocation but it does not specify how those resources are employed. In the CAPPS II context, the process of determining which airports are at greater risk is theoretically distinct from the manner proposed for addressing those risks (i.e. screening the individuals who are assessed as more risky).

We could, at least in theory, adopt a system where the CAPPS II screening system did not result in an individual screening determination. Rather, we could use it on a pure resource allocation basis, surging additional TSA screening resources to areas where the threat is perceived and then using those resources to conduct a greater number of random screenings. It could also be used to target at risk flights to allow for the better allocation of limited Federal Air Marshal resources. Even these uses, though less precise than the targeted use envisioned, would be a vast improvement over the current situation. Today, for example, TSA screeners are distributed throughout the system based not upon an assessment of risk but rather on the volume of traffic at an airport. Implicit in this assignment is either the assumption that risk is directly proportional to the volume of traffic or a conscious decision to disregard risk assessment – the former is a gross over-generalization and the latter is simply unwise and ineffective.

CAPPS II promises a change – we can envision the day when TSA inspectors (and other resources such as Air Marshals), are allocated in the way we think best addresses actual risks of harm, increasing the chances of catching terrorists and minimizing the unnecessary intrusion into people's lives at times and places where there is no risk at all. Should Congress have any concerns at all about the intrusiveness of individual screening it should, at a minimum, recognize the utility of enhanced risk assessment technology. To fail to do so would be even worse than our current system.

* * * * *

In short, CAPPS II has some significant issues that need to be addressed. But it also is a system of great promise. Failing to make the effort to use new technology wisely poses grave risks and is an irresponsible abdication of responsibility.

As six former top-ranking professionals in America's security services recently observed, we face two problems—both a need for better analysis and, more critically, "improved espionage, to provide the essential missing intelligence." In their view, while there was "certainly a lack of dot-connecting before September 11," the more critical failure was that "[t]here were too few useful dots."[45] CAPPS II technology can help to answer both of these needs. Indeed, resistance to new technology poses practical dangers. As the Congressional Joint Inquiry into the events of September 11 pointed out in noting systemic failures that played a role in the inability to prevent the terrorist attacks:

> 4. Finding: While technology remains one of this nation's greatest advantages, it has not been fully and most effectively applied in support of U.S. counterterrorism efforts. Persistent problems in this area included a lack of collaboration between

[45] Robert Bryant, John Hamre, John Lawn, John MacGaffin, Howard Shapiro & Jeffrey Smith, "America Needs More Spies," *The Economist*, July 12, 2003, p. 30.

> Intelligence Community agencies [and] *a reluctance to develop and implement new technical capabilities aggressively* . . . .[46]

Or, as one commentator has noted, the reflexive opposition to speculative research by some is "downright un-American."[47] Though CAPPS II technology might prove unavailing, the only certainty at this point is that no one knows. It would be particularly unfortunate if Congress opposed basic scientific research without recognizing that in doing so it was demonstrating a "lack [of] the essential American willingness to take risks, to propose outlandish ideas and, on occasion, to fail."[48] That flaw is the way to stifle bold and creative ideas—a "play it safe" mindset that, in the end, is a disservice to American interests.

Mr. Chairman, thank you for the opportunity to testify before the Subcommittee. I look forward to answering any questions you might have.

---

[46] *Report of the Joint Inquiry Into the Terrorist Attacks of September 11, 2001*, House Permanent Select Committee on Intelligence and Senate Select Committee on Intelligence, 107th Cong., 2nd Sess., S. Rept. No. 107–351 and H. Rept. No. 107–792, Dec. 2002, p. xvi (available at *http://www.fas.org/irp/congress/2002_rpt/911rept.pdf*) (emphasis supplied). The Joint Inquiry also critiqued the lack of adequate analytical tools, *id.* Finding 5, and the lack of a single means of coordinating disparate counterterrorism databases, *id.* Findings 9 & 10. Again, aspects of the CAPPS II program are intended to address these inadequacies and limitations on the research program are inconsistent with the Joint Inquiry's findings.

[47] *See* David Ignatius, "Back in the Safe Zone," *The Washington Post,* August 1, 2003, p. A19.

[48] *Id.*