

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 GOVERNMENT REFORM  
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,  
INTERGOVERNMENTAL RELATIONS, AND THE CENSUS

REGARDING  
CAN THE USE OF FACTUAL DATA ANALYSIS STRENGTHEN  
NATIONAL SECURITY? -- PART TWO

20 MAY 2003

---

\* 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 2002, it had more than 200,000 individual, foundation, and corporate supporters representing every state in the U.S. Its 2002 contributions came from the following sources: Individuals (61%); Foundations (27%); Corporations (7%); Investment Income (1%); and Publication Sales and Other (3%). 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, especially in the context of data analysis or data mining.

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 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.

My perspective on this matter, then, is that of a lawyer and a prosecutor with a law enforcement background, not that of a 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 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](http://www.heritage.org)). For any who might have read this 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.

\* \* \* \* \*

It is a commonplace for those called to testify before Congress to commend the Representatives or Senators before whom they appear for their wisdom in recognizing the importance of whatever topic is to be discussed – so much so that the platitude is often disregarded as mere puffery. Today, however, when I commend this Subcommittee for its attention to the topic at hand – the difficulty of both protecting individual liberty and enabling our intelligence and law enforcement organizations to combat terror – it is no puffery, but rather a heartfelt view. I have said often since September 11 that 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 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 addressing some theoretical principles that you might consider in structuring your thinking about the problem. I would then like to briefly discuss the nature of the problem posed by terrorist threats – all too often in weighing security and liberty in the balance we focus only

on the liberty side of the ledger without really reminding ourselves of what the true nature of the threat is. Then, in an effort to avoid being too theoretical, I'd like to apply the principles I have offered to the concrete issue of data mining and analysis as it might be used in the Total Information Awareness program (TIA) and the Computer Assisted Passenger Prescreening System (CAPPS II).

But let me first give you a short, pithy answer to the question posed by the title of today's hearing: Can the use of factual data analysis strengthen national security? The answer is "Of course." The more difficult question – the one that is the focus of my testimony – is the challenging one of implementation. How can we use factual data analysis in ways that are effective and useful yet do not unnecessarily or unreasonably trench on fundamental American conceptions of civil liberty and privacy?

### **OVERARCHING PRINCIPLES**

Let begin with some general thoughts about how cautious, yet effective governmental action can, in my view, be implemented. Fundamental legal principles and conceptions of American government should guide the configuration of our intelligence and law enforcement efforts rather than the reverse. 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. As a consequence, the concerns of civil libertarian critics should be fully voiced and considered while any research program is underway.

In general, unlike civil libertarian skeptics, I believe that new intelligence and law enforcement information gathering and information analytical systems can (and should) be constructed in a manner that fosters both civil liberty and public safety. We should not say that the risks of such systems are so great that any effort to construct them should be dispensed with.

Rather in my view, the proper course is to ensure that certain overarching principles animate and control the architecture of any new program and provide guidelines that will govern implementation of the program in the domestic environment.

**The Common Defense** – Let me make one important preliminary point: Most of the debate over new intelligence systems focuses on perceived intrusions on civil liberties, but Americans should keep in mind that the Constitution weighs heavily on both sides of the debate over national security and civil liberties. The President and Congressional policymakers must respect and defend the individual civil liberties guaranteed in the Constitution when they act, but there is also no doubt that they cannot fail to act when we face a serious threat from a foreign enemy.

The Preamble to the Constitution acknowledges that the United States government was established in part to provide for the common defense. The war powers were granted to Congress and the President with the solemn expectation that they would be used. Congress was also granted the power to "punish ... Offenses against the Law of Nations," which include the international law of war, or terrorism. In addition, serving as chief executive and

commander in chief, the President also has the duty to “take Care that the Laws be faithfully executed,” including vigorously enforcing the national security and immigration laws. Thus, as we assess questions of civil liberty I think it important that we not lose sight of the underlying end of government – personal and national security. I do not think that the balance is a zero-sum game, by any means. But it is vital that we not disregard the significant factors weighing on *both* sides of the scales.

**Civil Liberty --** Of course, just because the Congress and the President have a constitutional obligation to act forcefully to safeguard Americans against attacks by foreign powers does not mean that every means by which they might attempt to act is necessarily prudent or within their power. Core American principles require that any new counter-terrorism technology deployed domestically) should be developed only within the following bounds:

- No fundamental liberty guaranteed by the Constitution can be breached or infringed upon.
- Any increased intrusion on American privacy interests must be justified through an understanding of the particular nature, significance, and severity of the threat being addressed by the program. The less significant the threat, the less justified the intrusion.
- Any new intrusion must be justified by a demonstration of its effectiveness in diminishing the threat. If the new system works poorly by, for example, creating a large number of false positives, it is suspect. Conversely, if there is a close “fit” between the technology and the threat (that is, for example, if it is accurate and useful in predicting or thwarting terror), the technology should be more willingly embraced.
- The full extent and nature of the intrusion worked by the system must be understood and appropriately limited. Not all intrusions are justified simply because they are effective. Strip searches at airports would prevent people from boarding planes with weapons, but at too high a cost.
- Whatever the justification for the intrusion, if there are less intrusive means of achieving the same end at a reasonably comparable cost, the less intrusive means ought to be preferred. There is no reason to erode Americans’ privacy when equivalent results can be achieved without doing so.
- Any new system developed and implemented must be designed to be tolerable in the long term. The war against terror, uniquely, is one with no immediately foreseeable end. Thus, excessive intrusions may not be justified as emergency measures that will lapse upon the termination of hostilities. Policymakers must be restrained in their actions; Americans might have to live with their consequences for a long time.

From these general principles can be derived certain other more concrete conclusions regarding the development and construction of any new technology:

- No new system should alter or contravene existing legal restrictions on the government’s ability to access data about private individuals. Any new system should

mirror and implement existing legal limitations on domestic or foreign activity, depending upon its sphere of operation.

- Similarly, no new system should alter or contravene existing operational system limitations. Development of new technology is not a basis for authorizing new government powers or new government capabilities. Any such expansion should be independently justified.
- No new system that materially affects citizens' privacy should be developed without specific authorization by the American people's representatives in Congress and without provisions for their oversight of the operation of the system.
- Any new system should be, to the maximum extent practical, tamper-proof. To the extent the prevention of abuse is impossible, any new system should have built-in safeguards to ensure that abuse is both evident and traceable.
- Similarly, any new system should, to the maximum extent practical, be developed in a manner that incorporates technological improvements in the protection of American civil liberties.
- Finally, no new system should be implemented without the full panoply of protections against its abuse. As James Madison told the Virginia ratifying convention, "There are more instances of the abridgment of the freedom of the people by gradual and silent encroachments of those in power than by violent and sudden usurpations."

### **THE SCOPE OF THE TERRORIST THREAT**

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 enter in the future – a question plainly of relevance to any consideration of CAPPs II or TIA.

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 recent, supposedly confidential briefings to policymakers is 5,000. 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 United States, and (2) many who want to enter in the foreseeable future will be able to do so.

Understanding the scope of the problem demonstrates the difficulty of assessing the true extent of the risk to the United States. Consider this revealing statistic: "[M]ore than 500 million people [are] admitted into the United States [annually], of which 330 million are non-citizens." Of these:

- Tens of millions arrive by plane and pass through immigration control stations, often with little or no examination.

- 11.2 million trucks enter the United States each year. Many more cars do so as well: More than 8.5 million cars cross the Buffalo–Niagara bridges each year alone, and only about 1 percent of them are inspected.
- According to the Department of Commerce, approximately 51 million foreigners vacationed in the United States last year, and this figure is expected to increase to 61 million in three years.
- There are currently approximately 11 million illegal aliens living in the United States. Roughly 5 million entered legally and simply overstayed their lawful visit.
- Over half a million foreign students are enrolled in American colleges, representing roughly 3.9 percent of total enrollment, including:
  1. 8,644 students from Pakistan.
  2. A total of 38,545 students from the Middle East, including 2,216 from Iran, 5,579 from Saudi Arabia, and 2,435 from Lebanon, where Hezbollah and other terrorist organizations train.
  3. About 40,000 additional students from North African, Central and Southeast Asian nations where al-Qaeda and other radical Islamic organizations have a strong presence.

This, of course, is only part of the story. The other aspect of the danger to America is the new and unique nature of the threat posed by terrorists. Virtually every terrorism expert in and out of government believes there is a significant risk of another attack. . As last week’s truck bombing of Western compounds in Saudi Arabia reminds us, 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 and truck bombs) their capacity for harm is essentially limitless. The United States therefore faces the far more difficult task of discerning their intentions. Where the Soviets created “things” that could be observed, the terrorists create only transactions that can be sifted from the noise of everyday activity only with great difficulty. There can, therefore, be little doubt of the importance of research to better understand the value (or lack thereof) of sifting this mass of data. It is a problem of unprecedented scope, and one whose solution is imperative if American lives are to be saved.

As I said at the outset, these considerations of principle and the scope of the threat, while useful in constructing an *ex ante* heuristic for assessing new programs, are only of real value in application to concrete problems and proposed solutions. Whenever I speak on this topic, I always emphasize (as I do here today) that specifics matter. It is not enough to condemn every governmental initiative. Nor is it apt to afford the government a blank check for all actions designed to repel terror. Rather, each program and proposal must be carefully assessed on its own individual merits.

**“DATA MINING” -- TOTAL INFORMATION AWARENESS TODAY**

To that end, let me first discuss the concept of data mining and more particularly the Total Information Awareness program (“TIA”) – a program that has been widely

misunderstood. [For more detail on the program I refer you to a paper I co-authored with my Heritage colleague, Michael Scardaville – “The Need to Protect Civil Liberties While Combating Terrorism: Legal Principles and the Total Information Awareness Program,” The Heritage Foundation, Legal Memorandum No. 6 (February 2003).]

### **DATA ANALYSIS**

First, and foremost, I think that much of the public criticism has obscured the fact that TIA is really not a single program. Virtually all of the attention has focused on the data mining aspects of the research program – but far more of the research effort is being devoted to providing tools for enhanced data analysis. In other words, TIA is not, as I understand it, about bypassing existing legal restrictions and providing governmental agencies with access to new and different domestic information sources. Rather, it is about providing better tools to enable intelligence analysts to more effectively and efficiently analyze the vast pool of data already at their disposal – in other words to make our analysts better analysts. These tools include, for example, a virtual private network linking existing counter-terrorism intelligence agencies. It would also include, for example, research into a machine translation capability to automatically render Arabic into English. While these developments certainly pose some threat to civil liberty because any enhancement of governmental capability is inherently such a threat, they are categorically different than the data mining techniques that most concern civil libertarians. The threat to civil liberty is significantly less and the potential gain from their development is substantial.

Thus, my first concrete recommendation to you is to not paint with too broad a brush – the distinction between collection and analysis is a real and important one that, thus far, Congress has failed to adequately recognize. Earlier this year, Congress passed an amendment, the so-called Wyden amendment, which substantially restricts TIA development and deployment. That restriction applies broadly to all programs under development by DARPA. That’s a mistake. The right answer is not for Congress to adopt a blanket prohibition. Rather, Congress should commit to doing the hard work of digging into the details of TIA and examining its operation against the background of existing laws and the existing terrorist threats at home and abroad.

We have already seen some of the unintended but pernicious effects of painting with such a broad brush. Recently at a forum conducted by the Center for Strategic Policy, DARPA officials discussed how the Wyden amendment had short-circuited plans to sign a Memorandum of Understanding (MOU) with the FBI. The FBI, as this Subcommittee knows, is substantially behind the technological curve and is busily engaged in updating its information technology capabilities. The MOU under consideration would have enabled the FBI to join in the counter-terrorism Virtual Private Network (VPN) being created by the TIA program. Again, the VPN is not a new data collection technology – it is a technology to enhance data analysis by allowing information sharing. Other counter-terrorism agencies with exclusively foreign focus are already part of the VPN – the CIA and DIA for example. Though the Department of Defense has not reached a final interpretation of the Wyden amendment, the lawyers at DoD were sufficiently concerned with its possible scope that they directed DARPA to not sign the MOU with the FBI. As a consequence one of our principal domestic counter-terrorism agencies is being excluded from a potentially valuable

network of information sharing. Extrapolating from this unfortunate precedent, it is likely that the Wyden amendment will have the effect of further balkanizing our already unwieldy domestic counter-intelligence apparatus. The same law will probably be interpreted to prohibit the Department of Homeland Security from joining the network, as well as the counter-terrorism agencies of the various States.

In short, as Senator Shelby has written of TIA:

The TIA approach thus has much to recommend it as a potential solution to the imperative of deep data-access and analyst empowerment within a 21st-century Intelligence Community. If pursued with care and determination, it has the potential to break down the parochial agency information “stovepipes” and permit nearly pure *all* source analysis for the first time – yet without unmanageable security difficulties. If done right, moreover, TIA would be infinitely scalable: expandable to as many databases as our lawyers and policymakers deem to be appropriate.

TIA promises to be an enormously useful tool that can be applied to whatever data we feel comfortable permitting it to access. How broadly it will ultimately be used is a matter for policymakers to decide if and when the program bears fruit. It is worth emphasizing, however, that TIA would provide unprecedented value-added even if applied exclusively *within* the current Intelligence Community – as a means of finally providing analysts deep but controlled and accountable access to the databases of collection and analytical agencies alike. It would also be useful if applied to broader U.S. Government information holdings, subject to laws restricting the use of tax return information, census data, and other information. Ultimately, we might choose to permit TIA to work against some of the civilian “transactional space” in commercially-available databases that are already publicly and legally available today to marketers, credit card companies, criminals, and terrorists alike. The point for civil libertarians to remember is that policymakers can choose to restrict TIA’s application however they see fit: it will be applied only against the data-streams that our policymakers and our laws permit.

Put more prosaically, it remains for this Congress to decide how widely the analytical tools to be provided by TIA are used – but it is imperative that Congress understand that the tools themselves are distinct from the databases to which they might have access.

#### **DATA COLLECTION – STRUCTURAL LIMITATIONS**

As for concerns that the use of new data collection technologies could intrude on civil liberties by affording the government access to new databases, I certainly share those concerns. The question then is how best to ensure that any domestic use of TIA (or, frankly, any other intelligence gathering program) does not unreasonably intrude on American domestic civil liberties. There are several operational principles that will effectively allow the use of TIA while not substantially diminishing American freedom. Amongst these are the following requirements:

**Require congressional authorization.** In light of the underlying concerns over the extent of government power, it is of paramount importance that there be formal congressional consideration and authorization of the TIA program, following a full public debate, before the system is deployed. Some of the proposed data-querying methods (for example, the possibility for access to non-government, private databases, which is discussed in the next section) would require congressional authorization in any event. But, more fundamentally, before any program like TIA—with both great potential utility and significant potential for abuse—is implemented, it ought to be affirmatively approved by the American people’s representatives. Only through the legislative process can many of the restrictions and limitations suggested later in this testimony be implemented in an effective manner. The questions are of such significance that they should not be left to executive branch discretion alone.

**Maintain stringent congressional oversight.** In connection with the congressional authorization of TIA, Congress should also commit at the outset to a strict regime of oversight of the TIA program. This would include periodic reports on TIA’s use once developed and implemented, frequent examination by the U.S. General Accounting Office, and, as necessary, public hearings on the use of TIA. Congressional oversight is precisely the sort of check on executive power that is necessary to insure that TIA-based programs are implemented in a manner consistent with the appropriate limitations and restrictions. Without effective oversight, these restrictions are mere parchment barriers. While potentially problematic, one can be hopeful that congressional oversight in this key area of national concern will be bipartisan, constructive, and thoughtful. Congress has an interest in preventing any dangerous encroachment on civil liberties by an executive who might misuse TIA.

My colleagues at The Heritage Foundation have written extensively on the need for reorganization of the congressional committee structure to meet the altered circumstances posed by the war on terrorism and the formation of the Department of Homeland Security. Oversight of any program developed by TIA would most appropriately be given either to the committee which, after reorganization, had principal responsibility for oversight of that Department or, if TIA is limited to foreign intelligence applications, to the two existing intelligence committees.

**Construct TIA to permit review of its activities.** To foster the requisite oversight and provide the American public with assurances that TIA is not being used for inappropriate purposes, the TIA program must incorporate, as part of its basic structure, an audit trail system that keeps a complete and accurate record of activities conducted using the technology. To the maximum extent practical, the audit system should be tamper-proof. To the extent it cannot be made tamper-proof, it should be structured in a way that makes it evident whenever anyone has tampered with the audit system. Only by providing users, overseers, and critics with a concrete record of its activity can TIA-developed technology reassure all concerned that it is not being misused.

**Limit the scope of activities for which queries of domestic non-government databases may be used.** TIA is a technological response to the new, significant threat of terrorism at home and abroad. After September 11, no one can doubt that domestic law

enforcement and foreign intelligence agencies face a new challenge that poses a qualitatively greater threat to the American public than any other criminal activity.

U.S. foreign counterintelligence efforts are responding to a new and different form of terrorism and espionage. It is appropriate, therefore, that the use of TIA to query non-government databases be limited to the exigent circumstances that caused it to be necessary. Technology being developed for TIA to build models, query and correlate data, and uncover potential terrorist activity should be used (whether for law enforcement or intelligence purposes) only to investigate terrorist, foreign intelligence, or national security activities, and the TIA technology should never be used for other criminal activity that does not rise to this level.

It is important to be especially wary of “mission creep,” lest this new technology become a routine tool in domestic law enforcement. It should not be used to fight the improperly named “war on drugs,” combat violent crime, or address other sundry problems. While certainly issues of significant concern, none of these are so grave or important as the war on terrorism. Given the *bona fide* fears of increased government power, any systems that might be derived from TIA should be used only for investigations where there is substantial reason to believe that terrorist-related activity is being perpetrated by organizations whose core purpose is domestic terrorism.

The legislation authorizing TIA should enact this limitation. Congress should, therefore, specify that use of the TIA system is limited to non-government data inquiries that are certified at a sufficiently high and responsible level of government to be necessary to accomplish the anti-terrorism objectives of the United States. Only if, for example, a Senate-confirmed officer of the Department of Justice, Homeland Security, FBI, or CIA (such as an Assistant Attorney General or the FBI Director) certifies the objectives of the query based upon a showing of need should one be made.

**Limit access to the results of the search.** A corollary to the need to limit authority to initiate an analysis using TIA is an equivalent necessity to limit access to the findings of any resulting analysis. It would be unacceptable, for example, for the data and analysis derived from a TIA query (or, for that matter, a CAPPs II query), and linked to an individual identity, to be available to every Transportation Security Administration screener at every airport. Assuredly, after high-level analysis substantiated the utility of the information, it could be used to create watch lists and other information that can be shared appropriately within the responsible agencies. Until that time, however, access to the results of a TIA search should be limited by the authorizing legislation to a narrow group of analysts and high-level officials in those intelligence, counterintelligence, and law enforcement agencies.

**Distinguish between use of TIA in examining domestic and foreign activities.** In practice, it will be possible to use whatever technology the TIA program develops to unearth terrorist activity or conduct counterintelligence activity both abroad and domestically. Existing law places significant restrictions on intelligence and law enforcement activity that addresses the conduct of American citizens or occurs on American soil. Conversely, fewer restrictions exist for the examination of the conduct of non-Americans abroad.

The development of TIA is not a basis for disturbing this balance and changing existing law. Thus, even if Congress ultimately chooses to prohibit the implementation of TIA for any domestic law enforcement purpose whatsoever (a decision that would be unwise), it would be a substantial *expansion* of existing restrictions on the collection of foreign intelligence data were it to extend that prohibition to use of the technology with respect to overseas databases containing information on non-citizens. At a minimum, in considering TIA, Congress should ensure that, consistent with existing law, any program developed under TIA will be used in an appropriate manner for foreign intelligence and counterintelligence purposes.

**Impose civil and criminal penalties for abuse.** Most important, all of these various prohibitions must be enforceable. Violations of whatever prohibitions Congress enacts should be punishable by the executive branch through its administrative authority. Knowing and willful violations should be punishable as crimes. These forms of strong punishment are a necessary corollary of any TIA authorization.

In addition, Congress should enlist the third branch of government—the courts—to serve as a further check on potential abuse of TIA. As is detailed below, the courts will be involved in challenges to TIA information requests. To insure effective oversight of the use of TIA by the courts, Congress should also authorize a private right of civil action for injunctive relief, attorneys' fees, and (perhaps) monetary damages by individuals aggrieved by a violation of the restrictions Congress imposes.

**Sunset the authorization.** Any new law enforcement or intelligence system must withstand the test of time; it must be something that the American public can live with, since the end of the war on terrorism is not immediately in sight. Congress should be cautious, therefore, in implementing a new system of unlimited duration. It is far better for the initial authorization of TIA to expire after a fixed period of time so that Congress may evaluate the results of the research program, its costs (both public and private), and its long-term suitability for use in America. A sunset provision of five years would be ample time for Congress to gather concrete information on the program. With such information, Congress will be in a position to continue, modify, or terminate the program, as it deems appropriate.

#### **DATA COLLECTION – LEGAL LIMITATIONS**

As I noted earlier, the existing legal structure and the overarching principles that I see in American law lead to a singular legal recommendation for the structure and operation of TIA:

*TIA should be implemented only in a manner that mirrors existing legal restrictions on the government's ability to access data about private individuals—nothing more and nothing less.*

This recommendation may be particularized in the following ways:

**TIA should not have access to protected governmental databases.** Most government databases (e.g., arrest records and driver's licenses) contain information about an individual that is accessible to the government and in which the individual has no reasonable expectation of privacy. Linking such information through TIA technology should

not be subject to any greater restriction than that applied to its initial inclusion in the local, state, or federal government database from which the information is retrieved. By contrast, some existing governmental databases (like the Census database) cannot be used for purposes other than those for which they were created. Others (like the IRS database on taxpayer returns) can be accessed only with a special court order.

In authorizing the development of TIA technology, Congress should make it clear that information from existing government databases may be queried using TIA structured query programs only to the extent that the government already lawfully has access to the data. The creation of TIA-based networks should not be viewed as an excuse or opportunity to remove existing restrictions on the use of particularly sensitive individual data.

**Information from private domestic databases should be accessed only after notice to the data holder.** A similar limitation should also apply to queries made of private, non-government databases from which the government seeks information. Where predication for an investigation (whether criminal or foreign intelligence) exists, law enforcement or intelligence authorities should have the ability to secure data about an individual or pattern of conduct from private databases just as they do under current law.

Thus, with appropriate predication and/or court authorization (if the law requires), the government should be able to secure data from banks, credit card companies, and telephone companies about the conduct of specified individuals or about specified classes of transactions. But existing warrant and subpoena requirements should not be changed. Such data gathering should be done only at the “retail” level when a particularized basis for investigation exists.

More important, in each instance where data is sought from a private database, the holder of the data should be notified prior to securing the data and (as in the context of a subpoena today) have the capacity to interpose an objection to the data query to the same extent the law currently permits. The law today does not provide a mechanism by which such information requests may be made other than by subpoena. Thus, in authorizing a TIA-based investigative system, Congress should require that any aspects of TIA seeking data from private databases should operate in a manner similar to that in contemporary subpoena practice.

As this analysis makes evident, one should strongly oppose any effort to incorporate in TIA the ability to gather private database information at the “wholesale” level (e.g., all bank transactions processed by Citibank). One should also strongly oppose any TIA-based system that allows access to privately held data without notice to (and the opportunity to object by) the data holder. In short, the development of TIA technology and the war on terrorism is not a justification for the routine incorporation of all private data and information in a single government database.

**TIA is not a justification for creating new government databases.** Given the clear distinction that the law enacts between access to government and access to private, non-government databases, a further cautionary note is in order. In order to evade the legal strictures limiting access to information in private databases, the government might be tempted, in effect, to “institutionalize” the information it deems relevant by enacting new

data-reporting requirements to capture in government databases information that now exists only in private databases to which access is less ready. The first such proposal may already have been made: that Americans flying abroad be required to provide their travel itineraries to the Transportation Security Administration upon their departure from America.

The expansion of existing government databases should be resisted except upon a showing of extraordinary need. The government already collects too much information about Americans on a day-to-day basis. While many government programs require the collection of such data to permit them to operate, one should not create databases where no program requiring their creation exists—otherwise, there is the risk of wholesale evasion of existing legal restrictions on the use of information in private databases. Initiatives such as the new itinerary-collection program should be evaluated independently to determine their necessity and utility.

**There must be absolute protection for fundamental constitutionally protected activity.** The gravest fear that most Americans have about TIA is that it might be used to transmit queries about and assemble dossiers of information on political opponents. One should not discount these fears as they rest on all-too-recent abuses of governmental power. If a system developed based on TIA technology is used to enable an effort to harass anti-war demonstrators or gather information on those who are politically opposed to the government's policies (as the FBI used its investigative powers to do in the 1960s and 1970s), such abuse should be terminated immediately.

This prospect is not, however, sufficient to warrant a categorical rejection of all of the benefits to the war on terrorism that TIA technology might provide. TIA can be developed without these abuses, and aspects of the technology under investigation in fact hold the promise of enhancing civil liberties. Still, it is imperative that any implementing legislation has concrete, verifiable safeguards against the misuses of TIA. These should include, for example, an absolute prohibition on accessing databases relating to support of political organizations that propagate ideas—even ones favorable to terrorist regimes—absent compelling evidence that the organizations also aid terrorist conspirators with monetary, organizational, and other support not protected by the First Amendment. There must be an absolute prohibition on accessing databases relating solely to political activity or protest.

**TIA should build privacy protections into its architecture.** Finally, it should be recognized that access to data is not necessarily equated with a loss of privacy. To be sure, it may in many instances amount to the same thing, but it need not. There is, for example, a sense in which the automated screening of personal data by computer enhances privacy: It reduces the arbitrariness or bias of human screening and insures that an individual's privacy will be disrupted by human intervention only in suspicious cases.

In addition, those developing TIA can be required to construct a system that initially disaggregates individual identifiers from pattern-based information. Only after the pattern is independently deemed to warrant further investigation should the individual identity be disclosed. So, for example, only after a query on the bulk purchase of the precursors of Ricin poison turned up a qualifying series of purchases linked to a single individual would the individual's name be disclosed to terrorism analysts.

Thus, everyone on both sides of the discussion should welcome one aspect of TIA, the Genisys Privacy Protection program. The Genisys program is developing filters and other protections to keep a person's identity separate from the data being evaluated for potential terrorist threats. In authorizing TIA, Congress should mandate that a trusted third party rather than an organization's database administrator control these protections.

## **CAPPS II**

Virtually all of what I have said about TIA, is equally valid in any consideration of the Computer Assisted Passenger Prescreening System (CAPPS II), which has, of course, already been authorized by Congress. In particular, the TSA's new program should be:

- Constructed to include an audit trail so that its use and/or abuse can be reviewed;
- 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;
- Sunset after a fixed period of time, thereby ensuring adequate Congressional review;
- Prohibited from having access to any protected government databases, like the Census; and
- Have significant civil and criminal penalties for abuse.

The basis for these recommendations is, essentially, the same analysis I have already laid out with respect to TIA, and I will not burden the record by repeating it here.

There are, however, several aspects of the CAPPS II program that warrant additional commentary because they pose issues of concern:

**Access to Data.** First, if CAPPS II is to be effective, my recommendation that access to the results of a data inquiry be limited will need to be revisited. The very hallmark of CAPPS II is 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, I would think that the architecture of the system did not adequately protect individual privacy. Thus, in my view, the analysis passed by the CAPPS II system to TSA employees at the airport must be limited to a reported color code – red, yellow or green – and should not generally identify the basis for the assignment of the code. My understanding is that this is the current intent of those developing CAPPS II and that intent should be implemented.

**Privacy.** It is worth noting that CAPPS II precisely reverses the privacy protection equation being developed in the context of TIA. To protect privacy, the TIA program plans

to 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 – again, 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 system contemplated for TIA. 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.

One other brief point should be made about privacy – in many ways the implementation of CAPPS II is not an unalloyed diminution of privacy. Rather it is the substitution of one privacy intrusion (into electronic data) for another privacy intrusion (the physical intrusiveness of body searches at airports). Similarly, the use of CAPPS II may reduce 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.

Here one cannot make broad value judgments – each person weighs the utility of their own privacy by a different metric. But I do venture to say that 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, fewer random searches, and a reduction in invidious racial profiling.

**Domestic Use of CAPPS II.** The distinction earlier drawn between foreign and domestic applications of TIA is simply inapposite to any consideration of CAPPS II. By its nature, if it is to be at all effective, CAPPS II must at least operate domestically – that is where the gravest threat exists. Permitting the domestic use of factual data analysis systems requires, of course, a value judgment – one that Congress is uniquely capable of making. For my own part, I do not perceive the necessity of domestic operation as precluding the implementation of a suitably narrow inquiry system – but I do note the issue so that you may form your own judgments.

**Government Databases.** I mention this issue not because any particular aspect of the CAPPS II program presents an immediate concern – TSA has made it clear that it will not use CAPPS II to create a new government database – but simply as a cautionary note. Though such plans do not exist now, the creation of a government database of domestic travelers might, in the future, prove tempting. We should acknowledge that temptation at the outset and consciously and firmly reject it. The only information the government should ever retain about individuals who are screened and permitted to proceed under “green” or “yellow” cards is information sufficient to respond to an individual challenge to an analysis listing that individual as a potential risk.

**Non-Government Databases.** Next, we must consider the issue of access to non-government commercial databases. In general, the non-government databases to which CAPPS II will have access are databases whose holders make their data generally

available to all members of the public (sometimes, as in the Yellow Pages, for free; in other circumstances, for a fee). As a general matter, rules for new programs like CAPPs II relating to government access to data should mirror existing legal restrictions on the government's ability to access data about private individuals -- nothing more and nothing less. Thus, since the government may now have access to such public, non-government databases without any notice to or approval of either the data holder or the subject of the data inquiry, I see no significant privacy concern in affording access to that information through the CAPPs II system.

I should hasten to add, however, that some of the databases to which CAPPs II might seek access are *private* non-government databases, to which the public does not have general access -- for example, credit card use information. In some instances access to this information may be the lynchpin of the system, enabling identification of an individual with a high degree of certainty. As with my recommendations regarding TIA, CAPPs II should not generally be allowed to query such databases without first providing notice to the data holder and mechanism by which the data holder may object to the query and seek a judicial determination of the objection. If it is concluded that CAPPs II will routinely require access to a specific class of such private data, it may be appropriate for Congress to consider a blanket authorization of such access -- but only after it deems the utility of CAPPs II sufficiently great to warrant that step. In addition there is one obvious exception to this rule -- and one that is necessary if CAPPs II is to function at all: It is a tautological necessity that, in order to function, CAPPs II will need access to the normally private data contained in airline reservation systems themselves.

**Protection of Constitutional Liberties.** Finally, the unique subject matter of the CAPPs II system calls for heightened sensitivity to the potential for an infringement on protected constitutional liberties. I have generally been supportive of the potential inherent in the development of the TIA system. In part, that reflects my belief in the benefits of technology. But it also reflects my conviction that existing Supreme Court precedent, dating back to the 1960s, accurately captures the scope of the Constitutional privacy protection embodied in the Fourth Amendment: The Constitution affords no additional protection to information that an individual has made available to other individuals or institutions. Privacy concerns relating to the further distribution of such information are matters of policy and legislative concern, not constitutional law.

By contrast, CAPPs II implicates at least two fundamental liberty interests guaranteed by the Constitution. Most obviously, since the 1960s the Constitution has recognized a fundamental right to travel -- indeed, one might reasonably say that one significant purpose of the Federal union was to insure the freedom of commerce and travel within the United States. Second, many of the indicators that *might* be used to identify potential terrorists are also indicators that, in other circumstances, are potentially the products of protected First Amendment activity -- in other words, though CAPPs II is not intended to impinge upon free political speech, it may have the collateral effect of doing so.

Thus, there is a significant risk that a mal-administered system will impinge upon fundamental constitutional liberties. I am not, however, one to say that the risk of such impingement should result in abandonment of the program -- especially not in light of the

potentially disastrous consequences of another terrorist attack in the United States. I do, however, believe that some fairly stringent steps are necessary to provide the requisite safeguards for minimizing inadvertent infringements of civil liberty in the first instance and correcting them as expeditiously as possible. Those steps would include some or all of the following:

- The use of CAPPs II should be subject to extensive, continuous Congressional oversight. By this I do not mean the mere reporting of raw data and numbers – I mean that, at least as a spot check, Congress should examine individual cases (if necessary using confidential procedures to maintain classified status) to assure itself that the CAPPs II methodology is not being misused. In other words, the database contemplated by the CAPPs II system for “positives” (i.e. red cards) should, under classified circumstances, be subject to Congressional scrutiny;
- The “algorithm” used to screen for potential danger must, necessarily, be maintained in secret, as its disclosure would frustrate the purpose of CAPPs II. It must, however, also be subject to appropriate congressional scrutiny in a classified setting;
- 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. Nor, as I’ve said, is there any reason for the underlying data ever to be transmitted to the TSA screener.

\* \* \* \* \*

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