PAUL ROSENZWEIG

Paul Rosenzweig is Senior Legal Research Fellow in the Center for Legal and Judicial Studies at The Heritage Foundation, where he his research interests focus on issues of civil liberties and national security, criminal law, law enforcement, and legal ethics. Mr. Rosenzweig is also an Adjunct Professor of Law at George Mason University School of Law, teaching Criminal Procedure and an advanced seminar on White Collar Crime. In addition Mr. Rosenzweig serves on the District of Columbia Bar Legal Ethics Committee.

Mr. Rosenzweig has served as a Trial Attorney in the Environmental Crimes Section of the Department of Justice, as Investigative Counsel to the House Committee on Transportation and Infrastructure and, most recently, as Senior Litigation Counsel in the Office of the Independent Counsel (In re: Madison Guaranty Savings & Loan Assn.). Immediately prior to joining The Heritage Foundation Mr. Rosenzweig was in private practice.

Mr. Rosenzweig is a *cum laude* graduate of the University of Chicago Law School. He has an M.S. in Chemical Oceanography from the Scripps Institution of Oceanography, University of California at San Diego and a B.A from Haverford College. Following graduation from law school he served as a law clerk to the Honorable R. Lanier Anderson, III of the United States Court of Appeals for the Eleventh Circuit.

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

PERMANENT SELECT COMMITTEE ON INTELLIGENCE

REGARDING

SECURING FREEDOM AND THE NATION: COLLECTING INTELLIGENCE UNDER THE LAW

9 APRIL 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 afternoon 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.

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 Chief 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 an intelligence officer or 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, all of which are available at The Heritage Foundation website (www.heritage.org). For any who might have read this earlier work, I apologize for the familiarity that will attend this testimony. I can only hope it 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 Committee 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 first providing some historical context and addressing some theoretical principles that you might consider in structuring your thinking about the problem. Then, in an effort to avoid being too theoretical, I'd like to apply those principles to the concrete issues of data mining and the Total Information awareness program. Finally, I will offer some briefer thoughts about the issue of information sharing and reflect on the lessons of the recent indictment of Sami Al-Arian.

HISTORICAL CONTEXT

Let me begin by briefly putting the question posed by today's hearing in historical context. I do so because all too often we see our current situation as unique, when in fact it is part of a recurring pattern in American history. The tension between civil liberty and national security is but one example of how we return to the same fundamental issues over and over again. Consider the following history: [My learning in this area was greatly aided by a lecture Professor Geoffrey Stone of the University of Chicago recently gave to the Supreme Court Historical Society. I have borrowed liberally from his work for my understanding of these historical events]:

In 1798, the Napoleonic wars raged in Europe. President John Adams, a Federalist, effectively brought the United States into a state of undeclared war with France, on the side of the British. Thomas Jefferson and the Democratic Republican party opposed these measures as likely to provoke an unnecessary war. The Federalists, in turn, accused the Jeffersonians of treason.

To exacerbate the situation, the Federalist Congress enacted the Alien and Sedition Acts of 1798. The Alien Act authorized the president to deport any non-citizen he judged dangerous to the peace and safety of the United States, without a hearing or the right to present evidence. The Sedition Act prohibited the publication of false, scandalous and malicious writings against the government, the Congress or the president with intent to bring them into contempt or disrepute. These were, in effect, aggressive efforts to suppress political criticism of Adams, his policies, and his administration. The Act expired by its terms, and after Jefferson replaced Adams as President, he pardoned all those who were convicted under the act. Though never tested in the Supreme Court, these acts are widely regarded as having been unconstitutional and a stain on American liberty.

During the Civil War, President Abraham Lincoln suspended the writ of habeas corpus on eight occasions. The broadest such suspension declared that "all persons . . . guilty of any disloyal practice . . . shall be subject to court martial." As many as 38,000 civilians were imprisoned by the military, in reliance on this authority. In 1866, a year after the war ended, the Supreme Court ruled that the president was not constitutionally empowered to suspend the writ of habeas corpus, even in time of war, if the ordinary civil courts were functioning. Here, again, the suspension is remembered as an excessive response to a wartime crisis and has come to be regarded as Lincoln's most unfortunate wartime error.

In 1917, the United States entered World War I. During the war federal authorities acting under the aegis of the Espionage Act prosecuted more than 2,000 people for their opposition to the war. As a result, virtually all dissent with respect to the war was suppressed. Though the Supreme Court initially approved most federal actions in support of the war, over the next half-century, the Court overruled every one of its World War I decisions, effectively repudiating the excess of that war-time era.

Finally, and most notoriously, on Feb. 19, 1942, Roosevelt signed Executive Order 9066, which authorized the Army to "designate military areas" from which "any persons may

be excluded." Over the next eight months, more than 110,000 people of Japanese descent were forced to leave their homes in California, Washington, Oregon and Arizona. Though the Supreme Court upheld the president's action it has come to be recognized as a grave error. In 1988, President Ronald Reagan offered an official presidential apology and reparations to each of the Japanese-American internees.

I call your attention to this history for the lessons it provides. Some see in this history a cautionary note: As Professor Stone has noted: "In time of war or national emergency, we respond too harshly in our restriction of civil liberties, and then, later, when it is too late, we regret our behavior." And we should not disregard that caution.

But I also believe we may take a more optimistic lesson from history as well. Whatever one may think of the steps that the domestic law enforcement and intelligence agencies are taking to combat terror during today's crisis, I think it is undeniable that the actions today are more moderate and restrained than those of the past. Let me be clear – that comparison does not justify any current actions. But it does counsel restraint in accepting apocalyptic claims of the imminent demise of American liberty.

This history also should give us some comfort. Many who are concerned with current activities think that we are on a downward spiral towards diminished civil liberties. But to my way of thinking what this history shows is that the balance between liberty and security is more like a pendulum that gets pushed off-center by significant events (such as those of September 11) than a spiral. Over time, after Americans have recovered from the understandable human reaction to catastrophe and after the threat recedes, the pendulum returns to center. As Chief Justice Rhenquist wrote in his book *All the Laws but One: Civil Liberties in Wartime*:

> In any civilized society the most important task is achieving a proper balance between freedom and order. In wartime, reason and history both suggest that this balance shifts in favor of order – in favor of the government's ability to deal with conditions that threaten the national well-being.

We should acknowledge the historical reality that the opposite is true as well. When the wartime crisis passes, the balance swings back in favor of freedom and liberty. And since World War II, our society has, we hope, matured such that the scope of the swings in the pendulum are not nearly as great as they have been in the past. To quote Chief Justice Rhenquist again:

> [T]here is every reason to think that the historic trend against the least justified of the curtailments of civil liberty in wartime will continue in the future. It is neither desirable nor is it remotely likely that civil liberty will occupy as favored a position in wartime as it does in peacetime. But it is both desirable and likely that more careful attention will be paid by the courts to the basis for the government's claims of necessity as a basis for curtailing civil liberty.

And to the courts we may add Congress, the press and the American public. Thus, we should not, I think, be utterly unwilling to adjust the balance between liberty and security in today's crisis of terrorism. Cautious, to be sure, but not immobilized by our fear of government excess, for there are any number of mechanisms by which governmental excess may be curbed.

OVERARCHING PRINCIPLES

Let me now turn to some thoughts about how the cautious, yet effective actions of government should, in my view, be effectuated. 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."

As I said at the outset, these theoretical considerations and operational guidelines, 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 Committee 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 will 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 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, 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. As discussed below, 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.

SHARING INFORMATION – THE CASE OF SAMI AL-ARIAN

Let me now turn briefly to a different aspect of the question this hearing poses today – the question the sharing of intelligence information among domestic and foreign intelligence and law enforcement organizations. Here, I think the answer is much clearer – ***any information lawfully gathered during a foreign or domestic counter-intelligence investigation or lawfully gathered during a domestic law enforcement investigation should be capable of being shared with other federal agencies.*** The artificial limitations we have imposed on such information sharing are a relic of a bygone era and are of substantially diminished value today.

This is not to say that we disregard the past. We cannot, and should not, ignore recent unfortunate examples of government excess: For example, the abuses of the FBI's COINTELPRO (counterintelligence program) in the 1960s and 1970s, when investigative authority was used to conduct surveillance of anti-war activists and civil rights groups. Similarly, as the Church Committee investigation disclosed, our intelligence agencies have in several instances acted beyond the bounds of the law. The limitations that restrained our activity prior to September 11 grew out of those revelations and were an appropriate, understandable reaction to excess.

But we can no longer afford to hamstring our counter-terrorism efforts in that way. As with TIA, the right answer is oversight and control, not complete rejection of enhanced government capacity to combat terror. The latter answer is one of despair – that we cannot possibly both ensure domestic safety and protect liberty. We should reject that view because, as should by now be evident, we can repose confidence in the genius of the Constitution and the ability of our system of checks and balances to insure against excessive Executive power. We need not belabor the point here – virtually all of the recommendations I have made regarding TIA are, in one form or another, susceptible of modification and application to enhanced information sharing regimes.

We have already had at least one test case demonstrating the potential utility of enhanced information sharing between intelligence and law enforcement organizations: the indictment of Sami Al-Arian. Since the case has yet to be tried, and since Mr. Al-Arian is by law innocent until proven guilty, the truth of the government's assertions about him remain unproven and have yet to be tested. Indeed I have no knowledge of the facts beyond that provided in the indictment.

But let us consider a hypothetical case and indulge the hypothesis that the allegations are true. Let us imagine that, six months from now, the trial is over. If the allegations made in the indictment are substantiated what will we have learned?

Most pressingly, we will have learned that the charges against Mr. Al-Arian were delayed for at least 5 years by self-imposed legal obstacles barring the sharing of information between foreign counter-intelligence and domestic law enforcement organizations.

The government's case against Mr. Al-Arian is apparently based upon foreign counter-intelligence wiretap intercepts that date back as far as 1993. According to the information in those wiretaps, Mr. Al-Arian is charged with having knowingly provided financing to a terrorist organization with the awareness that the funds he provided would be used to commit terrorist acts. And that information has been in the possession of our intelligence organizations for at least the past 7 years.

According to the Department of Justice, however, it was not until the passage of the USA Patriot Act, and the ruling of the Foreign Intelligence Surveillance Court of Review last November that the intelligence community felt it was lawfully in a position to provide that information to law enforcement officials at DOJ and the FBI. According to the Attorney General, only those changes enabled the government to bring the charges pending against Mr. Al-Arian.

If this is true, then we have truly been foolish. No one, not even Mr. Al-Arian, has publicly argued that the original foreign intelligence scrutiny of Mr. Al-Arian was unlawful or unwarranted. If it really is the case that one branch of our government lawfully had in its possession information about the criminal activity of a foreign national on American soil and that that branch was (or believed it was) obliged by law not to disclose that information to other branches of the government, then that fact alone will make some of the changes wrought by the USA Patriot Act worthwhile. To the extent that the law removed longstanding legal barriers to brining information gathered in national security investigations into federal criminal courts, it is to be welcomed.

This is not, of course, to say that all information sharing is appropriate or necessary. Important restrictions on the authority of foreign intelligence agencies to conduct surveillance or examine the conduct of American citizens can and should continue to exist. Conversely, however, the government should, in this time of terror, take full advantage of the authority they have. Courts have recognized that, the requirements of the Fourth Amendment apply somewhat differently in the national security context than they do in the context of domestic law enforcement. And, as with TIA, none of the substantive limitations should be changed as a consequence of success. Their utility can and should be independently examined as appropriate.

* * * * *

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