The Heritage Foundation
Legal Memorandum
Executive Summary

No. 6 February 05, 2003

THE NEED TO PROTECT CIVIL LIBERTIES WHILE COMBATING TERRORISM: LEGAL PRINCIPLES AND THE TOTAL INFORMATION AWARENESS PROGRAM

PAUL ROSENZWEIG AND MICHAEL SCARDAVILLE

The Total Information Awareness (TIA) project is a research program in its initial stages. Federal agencies eventually could use TIA-developed technology to share information more effectively and to access information already available to law enforcement and intelligence agencies in a less costly manner. If the research is successful, TIA will provide the intelligence and law enforcement agencies with a powerful and safe tool for unearthing suspected terrorists.

Some in Congress have recently expressed concern over the program, fearing that it might be overly intrusive of American liberty. There are understandable and reasonable worries that giving the government data surveillance capabilities to fight terrorism might lead to unacceptable intrusions into the private lives of law-abiding Americans. Congress must, therefore, take some steps to protect Americans from unwarranted and unnecessary intrusions.

But the picture of TIA offered by its most vocal critics is not accurate. Even the legitimate concerns do not warrant the wholesale rejection of TIA's potential benefits, especially before its capacities are realized. Rather, research and development of TIA can and should continue, guided by the fundamental principle that *no information access technology should be implemented in a manner that alters or contravenes existing legal restrictions on the government's ability to access data about private individuals*. More particularly, there should be:

Congressional authorization and strong congressional oversight. Before any program like TIA—with both great potential utility and significant potential for abuse—is implemented, it ought, in the first instance, to be affirmatively approved by the American people's representatives. Moreover, Congress should commit to a strict regime of oversight of the TIA program to prevent mission creep or abuse.

For that to happen, Congress must not strangle the program in the crib by means of an appropriations rider that stops research or development until Congress gets its act together. Such a rider may be well-intended, but it would have the effect of encouraging congressional delay and empowering a committed minority to employ dilatory tactics to kill any eventual authorization. The threat of another horrific attack is simply too grave to

Produced by the
The Center for Legal
and Judicial Studies

Published by
The Heritage Foundation
214 Massachusetts Ave., NE
Washington, D.C.
20002–4999
(202) 546-4400
http://www.heritage.org

This paper, in its entirety, can be found at: *www.heritage.org/research/budget/lm6.cfm*

justify prematurely cutting off such a promising anti-terrorism tool as TIA.

Restricted use of TIA-developed technology. TIA data inquiries to correlate data and uncover potential terrorist activity should be done (whether for law enforcement or intelligence purposes) only to investigate terrorist, foreign intelligence, or national security activities; the TIA technology should never be used for ordinary criminal activity. Congress should require certification of adherence to these limits by Senate-confirmed political appointees and limit access to the results of any analysis derived from applying the TIA search models to a small cadre of analysts. In addition, those developing TIA should be required to construct a system that protects privacy by disaggregating individual identifiers from pattern-based information until after the pattern is independently deemed to be of sufficient interest to warrant further investigation.

No alteration of existing legal restrictions on the government's ability to access data about private individuals. Current laws regarding the issuance of search warrants and subpoenas for domestic information about private individuals should be applied to TIA in equivalent, unchanged form. Congress should also continue existing restrictions on the collection of foreign intelligence data and should not extend any domestic prohibitions on the use of TIA technology to its use on overseas databases containing information on non-citizens.

Absolute protection for fundamental constitutionally protected activity. It is imperative that any implementing legislation contains an absolute prohibition on accessing databases relating to support of political organizations that propagate ideas—even ones favorable to terrorist regimes.

Civil and criminal penalties for abuse. The TIA system must incorporate, as part of its basic structure, an audit trail system that keeps a complete and accurate record of activities that are conducted using the system. Violations of prohibitions enacted by Congress should be punishable by the executive branch through its administrative authority and should be sanctionable both civilly and criminally.

A sunset provision in the authorization. A sunset provision of five years would be ample and would provide a sufficient time for Congress to assemble concrete information on which to base a further reauthorization decision.

Conclusion. The TIA program is no panacea. There is no guarantee that it will prevent further terrorist attacks against America. But neither is it an Orwellian monster whose construction will irretrievably alter the landscape of American liberty and freedom. Rather, as with most innovative proposals, it is a technological development capable of both use and abuse. To view the potential for misuse as the basis for rejection of a new technology is, however, to despair of technological change and improvement. The better approach is a thoughtful and measured one: examining the possibilities of the new technology in the context of existing law and taking steps to ensure that its development is consistent with those limitations. Viewed through this prism, the research into the development of TIA should proceed—with appropriate safeguards.

Prematurely rejecting new technology is no answer to the asymmetric threat of terror. Rather, Congress and the executive branch must work to harness technology's potential benefits and limit its potential abuses. In short, civil liberties and national security need not be traded off in equal measure. Americans deserve essential protections for both and should insist that policymakers engage in the difficult task of ensuring that they get them.

—Paul Rosenzweig is Senior Legal Research Fellow in the Center for Legal and Judicial Studies at The Heritage Foundation and Adjunct Professor of Law at George Mason University. Michael Scardaville is Policy Analyst for Homeland Security in the Kathryn and Shelby Cullom Davis Institute for International Studies at The Heritage Foundation.

The Heritage Foundation
Legal Memorandum

No. 6 February 05, 2003

THE NEED TO PROTECT CIVIL LIBERTIES WHILE COMBATING TERRORISM: LEGAL PRINCIPLES AND THE TOTAL INFORMATION AWARENESS PROGRAM

PAUL ROSENZWEIG AND MICHAEL SCARDAVILLE

Since the September 11, 2001, terrorist attacks on the World Trade Center and the Pentagon, Congress, the media, and the general public have urged the intelligence, counterintelligence, and law enforcement agencies to improve their ability to discover and preempt terrorist plots before additional attacks occur. The criticism is colloquially rendered as the failure of government agencies to "connect the dots."

Yet, when the government begins the development of intelligence programs that would assist in "connecting the dots," Americans naturally also worry that government will overreach and seek to accumulate unwarranted power. This reaction may be in tension with the desire for increased security, but U.S. history shows that it is not unique to the post–September 11 era. The United States has experienced abuses of power in times of war and almost unilateral disarmament in times of seeming calm.

The war on terrorism changes the stakes in fundamental ways. No longer is the United States fighting against adversaries an ocean away—the war has come home to this continent. Yet the war against terrorism is likely to be a long one, and Americans cannot tolerate the long-term substantial degradation of their civil liberties as the price of public safety.

Many see this conundrum as irresolvable: Security must be balanced against civil liberty, and any improvement in one results in a diminution of the other. This is the wrong perspective: America is not limited to a zero-sum game. There are effective ways to limit the ability of the government to intrude into Americans' lives while increasing security. America must adhere to fundamental and firm principles of limited government, and it can do so while also answering the terrorist threat. The challenge is not an easy one, but few worthwhile things are.

Produced by the
The Center for Legal
and Judicial Studies

Published by
The Heritage Foundation
214 Massachusetts Ave., NE
Washington, D.C.
20002–4999
(202) 546-4400
http://www.heritage.org

This paper, in its entirety, can be found at: *www.heritage.org/research/budget/lm6.cfm*

The public controversy over the experimental (and unwisely named) Total Information Awareness (TIA) research program sponsored by the U.S. Department of Defense is an instructive case study of how the challenge might be met. In response to the threat of terrorism, the Defense

Advanced Research Projects Agency (DARPA) in January 2002 opened the Information Awareness Office (IAO), which manages the TIA program. The program is an effort to develop the technological means to "put together the pieces of the puzzle" by (in part) allowing subject- and pattern-based queries of computer databases. Once developed, and if proven effective, technology being researched under TIA eventually could help federal agencies link government information systems together to provide a national intelligence fusion capability and a less costly way to access information already available to law enforcement and intelligence agencies. In other words, if DARPA's research (which is in its initial stages) is successful, a properly implemented TIA will provide intelligence, counterintelligence, and law enforcement agencies with a variety of powerful tools for unearthing suspected terrorists.

However, the concept of TIA has been criticized, most prominently by *New York Times* columnist William Safire.[1] Since Safire's critique first ran, privacy advocates have voiced determined opposition to the program. It has been labeled "a big, scary Orwellian thing,"[2] while Safire describes it as a "computerized dossier"[3] on every American's private life. Other critics cite the potential for government misuse as a reason to forgo any effort to develop TIA.[4] Questions about the program have begun to emerge on Capitol Hill.[5] Some lawmakers have already offered amendments to kill the program[6] and have called for its review by the Inspector General of the Department of Defense.[7]

The criticisms of the nascent TIA programs sound two distinct themes:

1. That TIA will, by making access to data easier and more efficient, inappropriately magnify and enhance the government's power, and
2. That TIA, when implemented, will (beyond increasing government power) allow the government access to data to which it does not currently have access and/or lower existing legal barriers to such access.

These concerns should be taken seriously. Indeed, we and many of our respected colleagues within The Heritage Foundation share these concerns. They stem from an understanding of America's founding history and recent unfortunate examples of government excess.[8] In our consid-

1. William Safire, "You Are a Suspect," *The New York Times*, November 14, 2002.
2. Susan Baer, "Broader U.S. Spy Initiative Debated," *The Baltimore Sun*, January 5, 2003.
3. Safire, "You Are a Suspect."
4. "High-tech U.S. Govt. Spying Threatens Americans' Privacy: Lawmakers," Agence France-Presse, January 16, 2003. The Electronic Privacy Information Center, American Civil Liberties Union (ACLU), American Conservative Union, Americans for Tax Reform, Center for Democracy and Technology, Center for National Security Studies, Eagle Forum, Free Congress Foundation, and Electronic Frontier Foundation have formed a coalition and launched a lobbying campaign to halt the program. The coalition's letter to the House and Senate leadership can be found at *http://www.epic.org/privacy/profiling/TIA_coalition_letter.pdf*.
5. Senators Bill Nelson (D–FL) and Dianne Feinstein (D–CA) have vowed to hold hearings on TIA. Senator Russell Feingold (D–WI) has already offered the Data-Mining Moratorium Act of 2003 (S. 188) to halt DARPA's research. See *http://thomas.loc.gov/cgi-bin/query/D?c108:1:./temp/~c108F8RHrG*.
6. Senators Chuck Grassley (R–IA) and Ron Wyden (D–OR) offered amendments (SA 53 and SA 59, respectively) to the appropriations omnibus (H. J. Res. 2) that would limit funding for the project. The Wyden amendment would halt funding of TIA research in 60 days unless DARPA reports to Congress on the scope of the program and would prohibit deployment of any domestic TIA component absent express authorization from Congress. It was adopted as part of the Senate version of H.J. Res. 2 on January 23, 2002, and will be considered during the House–Senate conference on the bill. See Adam Clymer, "Senate Blocks Privacy Project," *The New York Times*, January 24, 2003. On the overly broad scope of the Wyden amendment, see Paul Rosenzweig, "Congress Should Not Prematurely Short-Circuit the Total Information Awareness Program," Heritage Foundation *Executive Memorandum* No. 853, January 28, 2003.
7. See *http://www.fas.org/sgp/news/2002/11/gr112202.html*.
8. 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. See, e.g., *Hobson* v. *Wilson*, 737 F.3d 1 (D.C. Cir. 1984).

ered judgment, however, these legitimate concerns are outweighed by the potential benefits of the TIA program under development, which may be implemented within existing legal and policy constraints that can prevent abuse of the program during criminal or national security investigations. Indeed, if TIA were the program its most vocal critics describe, we would join them, without reservation, in opposing it.

To an extent that is rare even in Beltway debates, however, the description of TIA offered by most of its critics is not accurate.[9] DARPA certainly invited some of the criticism by adopting a name, symbol, and motto that have an Orwellian ring.[10] It is a natural outgrowth of a healthy military culture that leaders label their operations with titles that convey overwhelming power.[11] Regrettably, when military research projects are given those names—especially when they have potential civilian applications—it strikes many as naive or politically inept. The name does not, however, say very much about what the research project really attempts to achieve.

A more complete and accurate picture of TIA is necessary to foster the debate. Our examination has led us to the conclusion that a wholesale rejection of TIA's possibilities before its capacities are realized would be a serious mistake. Rather, the legitimate concerns call for us to devise thoughtful limits and protections against abuse and to understand the distinction between the foreign and domestic uses to which TIA might be put.

Development of TIA can and should continue, based upon the following foundations:

- Strong congressional oversight;
- High-level authorization for use of the technology and limited access to its product;
- Implementation in a manner that does not alter or contravene existing legal restrictions on the government's ability to access data about private individuals;
- Absolute protection for fundamental constitutional liberties;
- Civil and criminal penalties for abuse; and
- A sunset provision to terminate the program after a trial period.

Our analysis begins (as we believe it ought) with a summary of first principles. We then summarize our understanding of the nature and scope of the problem posed by terrorist threats and offer a more comprehensive summary of what the TIA programs are actually doing.[12] We conclude with several policy recommendations that, in our view, address critics' concerns about privacy and government power while advancing continued research into a potentially powerful weapon against terrorism.

AMERICAN PRINCIPLES OF LIBERTY AND LIMITED GOVERNMENT

Some might say that discussion of any development of TIA is premature—that TIA has yet to grow beyond the concept stage and that discussion of the limits to be placed on the use of TIA should await its development. Although TIA is little more than a research project at this juncture, however, it is still prudent to consider appropriate safeguards on its use while in development and implementation.

9. For an informative political analysis of the opposition, see Heather MacDonald, "Total Misrepresentation," *The Weekly Standard*, January 27, 2003; Shane Harris, "The Big Brother Complex," *Government Executive Magazine*, January 2003; "Total Information Unawareness," at *http://www.govexec.com/dailyfed/1102/112002ti.htm*.
10. The logo, based on the Great Seal of the United States, has an eye atop a pyramid scanning the globe. The TIA motto is Francis Bacon's famous aphorism, "Knowledge is Power." Though the logo and the motto thus both stem from historical antecedents, in context they are far too readily construed as symbols of government overreaching.
11. A certain genre of Hollywood movies would have the commander lead his forces in "Operation Total Destruction" or "Operation Complete Annihilation" or "Operation Overwhelming Force." Viewers would laugh at "Operation Tactical Advance by Means of Approved and Humane Rules of Engagement," even though this is what we really expect the American military to accomplish. In this context, the public understands that the military lexicon is meant to inspire confidence and is not to be taken literally.
12. For a technical overview of TIA, see Dr. John Poindexter, Dr. Robert Popp, and Brian Sharkey, "Total Information Awareness," IEEE Aerospace Conference, Big Sky, Montana, March 2003.

Indeed, fundamental legal principles and conceptions of American government should guide the configuration of TIA rather than the reverse. The precise contours of any rules relating to the use of TIA will depend, ultimately, on exactly what TIA is capable of accomplishing—the more powerful the systems, the greater the safeguards necessary. As a consequence, the concerns of critics should be fully voiced and considered while the TIA research program is underway.

In general, TIA can and should be constructed in a manner that fosters both civil liberty and public safety. Certain overarching principles must animate the architecture of TIA and provide guidelines that will govern the implementation of TIA in the domestic environment. These are the same principles that should animate the consideration of any new program to combat global terrorism at home.

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 other 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,"[13] which include the international law of war, or terrorism. Besides serving as chief executive and commander in chief, the President also has the duty to "take Care that the Laws be faithfully executed,"[14] including vigorously enforcing the national security and immigration laws.

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.[15] Core American principles require that TIA (and, indeed, any new counterterrorism technology deployed domestically) should be developed only within the following bounds:[16]

- 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

13. U.S. Constitution, Article I, section 8, clause 10.

14. U.S. Constitution, Article II, section 3.

15. It is not important here to delineate the respective powers of Congress and the President in times of national emergency, except to note that the President's power is greater when the Congress has not acted to limit the President's range of actions though legislation. See *Youngstown Sheet and Tube* v. *Sawyer*, 343 U.S. 579, 637 (1952) (the Steel Seizure Case) (Jackson, J., concurring). This is one of the reasons why we recommend congressional authorization of any intelligence system that substantially affects Americans' privacy or liberty.

16. See Paul Rosenzweig, "A Watchful America," *The Responsive Community*, Fall 2002, p. 89, and "Principles for Safeguarding Civil Liberties in an Age of Terrorism," Heritage Foundation *Executive Memorandum* No. 854, January 31, 2003.

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 terrorism, 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 that 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 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."[17]

SCOPE OF THE TERRORIST THREAT AND TIA'S POTENTIAL PROMISE

With those principles in mind, the discussion of TIA will also be well-served by a thorough understanding of the threat it is intended to address and the precise means by which it would address that threat.

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.

Although 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.[18] 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

17. Speech to the Virginia Ratifying Convention, June 16, 1788, reprinted in Matthew Spalding, ed., *The Founders' Almanac* (Washington, D.C.: The Heritage Foundation, 2002), p. 133. Thomas Jefferson was of much the same view: "The natural progress of things is for liberty to yield and government to gain ground." Letter to E. Carrington, May 27, 1788, reprinted in *The Founders' Almanac*, p. 157.

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

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."[19] Of these:

- Tens of millions arrive by plane and pass through immigration control stations, often with little or no examination.[20]
- 11.2 million trucks enter the United States each year.[21] 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.[22]
- According to the U.S. 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.[23]
- There are currently approximately 11 million illegal aliens living in the United States. Roughly 5 million entered legally and simply overstayed their lawful visit.[24]
- 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 Hezballah and other terrorist organizations train; and
  3. About 40,000 additional students from North African, Central Asian, and Southeast Asian nations where al-Qaeda and other radical Islamic organizations have a strong presence.[25]

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. Moreover, the threat of such an attack, unlike the threat posed by the Soviet Union during the Cold War, is asymmetric.

In the Cold War era, U.S. analysts assessed Soviet capabilities, thinking that their limitations bounded the nature of the threat the Soviets posed. Because of the terrorists' skillful use of low-tech capabilities (e.g., box cutters), their capacity for harm is essentially limitless. The United States therefore faces the far more difficult task of discerning their intentions. Where the Soviets created "things" that could be observed, the terrorists create 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.

19. White House, "Securing America's Borders Fact Sheet," at *www.whitehouse.gov* (accessed January 14, 2003).
20. U.S. Department of Commerce, Office of Travel and Tourism Industries, "Inbound Travel to the U.S.," at *http://tinet.ita.doc.gov/outreachpages/inbound.general_information.inbound_overview.html?ti_cart_cookie=20030127.125013.04230*.
21. White House, "Securing America's Borders."
22. Michelle Malkin, *Invasion: How America Still Welcomes Terrorists, Criminals, and Other Foreign Menaces to Our Shore* (Washington, D.C.: Regnery Publishing Inc., 2002) p. 8.
23. Office of Travel and Tourism Industries, "Inbound Travel."
24. Malkin, *Invasion*, pp. xii and 197.
25. Institute of International Education, Open Doors, at *http://opendoors.iienetwork.org*. This is not, of course, to suggest that all of these students or even a substantial fraction of them are likely terrorists, but merely to point out that the size of the group within which a terrorist may hide is quite large.

The Total Information Awareness Program. The Department of Defense is experimenting with a number of possible technological approaches to solving this problem, collectively known as TIA.[26] It is a research project to develop a variety of new software and hardware tools to improve the way the intelligence, counterintelligence, and law enforcement communities share information on suspected terrorist plans in order to prevent future attacks.

TIA can be a powerful collaborative network for agencies that have a counterterrorism mission. By fostering the sharing of information in existing databases, TIA can close the seams between organizations that have prevented early detection of foreign terrorists in the past. The program conducts research in issues relating to data search, pattern recognition, and information security. It is a multi-year feasibility study and development effort consisting of numerous related research initiatives that first began awarding contracts in 1997.[27] A prototype of the more controversial technology is at least five years away.

This research has two intended uses: gathering foreign intelligence on non-Americans and gathering domestic information for intelligence and law enforcement purposes. The research also has two potential government applications: the relatively uncontroversial goal of establishing a much-needed intelligence fusion capability by permitting data integration from a variety of government-owned databases[28] and the more controversial creation of a more efficient means of querying non-government databases holding information relevant to domestic terrorism investigations.[29]

The more controversial aspects of TIA relate to the second of these development projects insofar as it would operate domestically[30]—the effort to create technology to link databases and permit queries of those databases based upon models of potential terrorist behavior. As the accompanying appendix describes in substantially more detail, there are two aspects of this project: the development of the technological means for querying databases with widely varying data formats and the development of the technological means for conducting such queries while enhancing the privacy of the data being retrieved.

Terrorists preparing for an attack will leave an electronic trail of interactions with the government both outside (e.g., travel from Yemen to Germany) and within the United States (e.g., Customs decla-

26. The following summary is intended only as an introduction to a thorough understanding of the various TIA programs under development. A more thorough summary is contained in the appendix to this Legal Memorandum. More detailed technical information is publicly available at the DARPA Web site. See, e.g., the IAO presentations at *http://www.darpa.mil/darpatech2002/presentation.html*. A review of this information will convince a fair-minded observer that, to paraphrase Mark Twain, reports of TIA's capabilities are greatly exaggerated.

27. TIA's various component projects are in varying stages of development: IAO's earliest efforts to establish a collaborative information-sharing environment are already undergoing field-testing at the United States Army's Intelligence and Security Command (INSCOM) in coordination with the Army's Information Dominance Center (IDC) and the Joint Counter-Terrorism Assessment Group (JCAG), where they are being used to allow better sharing of intelligence between the participants. By contrast, other research programs, including the development of a mechanism to link governmental databases and public non-government databases, have barely begun and represent some of the greatest technological challenges the TIA program faces. As a result, these latter programs will require at least five years of development before they will be ready for field-testing or use by federal agencies.

28. Larry M. Wortzel, "Creating an Intelligent Department of Homeland Security," Heritage Foundation *Executive Memorandum* No. 828, August 23, 2002.

29. At this early stage of development, which, if any, domestic non-government databases might be queried by TIA-developed technology has yet to be determined. Fears that *all* non-government databases will be subject to access are inconsistent with IAO's public description of the TIA development program and appear to be without any factual foundation. Should such a plan be contemplated, it should be opposed.

30. As discussed below, both the law and policy strongly counsel for a clear distinction between use of any TIA-developed technology in a domestic context and use of that technology overseas in the war against terrorism. The recent Senate amendment adopted as part of H.J. Res. 2 wisely recognizes this distinction and makes no prohibition on any TIA program related to "lawful foreign intelligence activities conducted wholly overseas, or wholly against non-United States persons." See SA 59, at *http://www.fas.org/irp/congress/2003_cr/s011703.html*.

rations upon entry) through purchases, travel, and other activities, just as anybody else living in the modern world does. Through a subject-oriented query of databases containing this information, technology being developed by the IAO could be used to gain a more complete understanding of a suspect, his activities, and his relationships with others through an examination of this trail. Through a pattern-oriented query, TIA solutions linked to this information could be used to identify a terrorist based on intelligence data and detailed models of potential terrorist activities.[31]

Thus, for example, imagine if credible intelligence sources reported that the precursor components of Sarin gas were being smuggled into the United States by al-Qaeda operatives via flights originating in Germany during the month of February 2003. If TIA-based technologies were available today, a pattern-based inquiry of existing government databases might produce a list of non-resident aliens entering the United States during that period on flights meeting those specifications. This information might be cross-checked against other government databases identifying known or suspected terrorists. A subject-based data query might then be used to develop additional information about those identified as warranting further investigation. Their purchase, for example, of additional materials that might assist in the deployment of Sarin gas (canisters and the like) could conceivably be sifted from the information in non-government databases and used as a predicate for further investigation.

Because of the evident challenges to civil liberties that such capabilities would present, the TIA development program has built into its research agenda various measures designed to protect privacy by keeping personal data and irrelevant information out of government's hands. To insure this privacy protection, as part of its research, the IAO is developing technologies intended to prevent the examination of personal information and general misuse. These include, for example, information partitioning and selective revelation technology (that is, separating individual identification information from the underlying data). It also includes the increased use of filters and software to analyze data and remove information unrelated to the investigation.

The combined components of the TIA program would present the intelligence community with a powerful means to electronically intercept and process electronically stored data. Because of the potential power of these tools, the IAO is investing resources in technology that "can allow us to make substantial progress toward supporting both privacy and national security."[32]

OVERSIGHT AND LAW CAN SAFEGUARD CIVIL LIBERTIES

The first argument against the use of intrusive software and easier data collection technology in general—and TIA in particular—is the argument against expanding powers of the state. This argument has substantial historical foundation. The principal concern of many critics of TIA is not that the government is gaining access to more information than it previously had, but rather that the government's enhanced ability to quickly and effectively correlate disparate databases to which it already lawfully has access will increase the government's control and power over Americans' lives.

This concern is not unwarranted. One of the fundamental bulwarks of American liberty is the notion of a federal government of limited powers. The constitutional system of checks and balances is, in part, a recognition that individual liberty is advanced by structures that purposefully render government less efficient and thus more measured. Any enhancement of the government's ability to act is in tension with this venerable American tradition.

At the same time, however, one must also acknowledge the potential value of the increased efficiency in anti-terrorism investigations that would come from the ability to pose directed pat-

31. As discussed more fully below, in both cases, it can and should be mandatory that such queries follow established legal and policy guidelines for querying private, non-government domestic data and that this non-public information be accorded the same level of protection it currently enjoys.

32. Defense Advanced Research Projects Agency, Information Science and Technology Panel, "Security with Privacy," December 13, 2002.

tern queries to government databases. Consider, for example, the recent sniper attacks in the Washington, D.C., area—attacks that initially were thought to be linked to terrorism. There was ample information about the two killers in government databases that had been lawfully collected: the court order issued in Washington State; the fingerprints on the bullet in Alabama; and the traffic stop information collected on more than a dozen occasions by several law enforcement agencies in the Washington metropolitan area, to name but a few. Yet even these data (which nobody can doubt were appropriately collected in the government databases) were not accessible or integrated in a useable manner. Had, for example, the federal government had the capacity to make a simple query of local law enforcement databases—identify all cars about which more than five local data queries had been made since the attacks began—the snipers' car would have been identified as suspicious well before their capture actually occurred.

It is this sort of failure (typified by the inability to coordinate information gathered in Montgomery, Alabama, with that gathered in Montgomery County, Maryland) that TIA is intended to address.[33] Perhaps this new tool will prove to be ineffective, but at its inception, it holds out significant promise.

How, then, can the fears of increased government efficiency and authority be addressed? Ultimately, it is not persuasive to argue that the prospect of increased efficiency and increased governmental power is so great a threat to civil liberties that all efforts toward an enhanced capacity for information fusion should be abandoned. The potential benefits are too substantial and the threat of further terrorist attacks on the United States too real and horrific to forsake all such effort. Even if the use of TIA were confined to examination of overseas databases containing information on non-Americans, it would offer significant benefits. Thus, the better response is to embrace the challenge of constructing a useful system to combat terrorism that has strong safeguards to protect against abuse. Among the safeguards:

- **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 paper be implemented in an effective manner. The questions are of such significance that they should not be left to executive branch discretion alone.

  For that to happen, Congress must not strangle the program in the crib by means of an appropriations rider that stops research or development until Congress gets its act together. Such a rider may be well-intentioned, but it would have the effect of encouraging congressional delay and empowering a committed minority to employ various dilatory tactics to kill any eventual authorization. The threat of another horrific attack on America is simply too grave to justify prematurely cutting off such a promising anti-terrorism tool as TIA.[34]
- **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 imple-

33. One of the arguments advanced by critics of the development of TIA is that it will be ineffective in its mission of identifying terrorist activity if it does not have access to both private and governmental databases and that the prospect of access to private databases is so troubling that TIA should be abandoned. As should be evident from the example discussed in the text, this ground for opposition to TIA is a red herring: more fanciful and political than practical. Even if the TIA data coordination and query system were restricted exclusively to existing government databases, it would represent a substantial increase in the ability of the government to combat terrorism.

mented, 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.

The Heritage Foundation has 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.[35] 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.[36] 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 qualitatively poses a 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.[37] 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.

34. The Wyden amendment, SA 59, makes any domestic use of TIA-developed technology contingent upon congressional authorization. Although the intent behind the amendment is commendable, as written, it will disable domestic agencies with foreign counterintelligence missions (such as the FBI and portions of the new Department of Homeland Security) from participation in counterintelligence activities with incidental domestic effects. It also prohibits coordination of existing government databases in a way that will erode the government's ability to fight domestic terrorism. The amendment should be modified to allow more measured consideration of the question. See Rosenzweig, "Congress Should Not Prematurely Short-Circuit the Total Information Awareness Program" (cited in note 6, *supra*).

35. See, e.g., Michael Scardaville, "The New Congress Must Reform Its Committee Structure to Meet Homeland Security Needs," Heritage Foundation *Backgrounder* No. 1612, November 12, 2002, and "Congress Must Reform Its Committee Structure to Meet Homeland Security Needs," Heritage Foundation *Executive Memorandum* No. 832, July 12, 2002.

36. As discussed in the appendix, the TIA program is already developing technology to achieve this objective.

37. As outlined more fully in the next section, intelligence fusion linking existing government databases and permitting ready data queries across government jurisdictional lines is legally far less problematic and to a large degree is the greatest promise of TIA technology.

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 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 inquiry 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 is unacceptable 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 substantiates the utility of the information, it can 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.[38]
- **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.

38. As noted earlier, the Senate has already adopted the Wyden amendment (SA 59) forbidding the potential use of TIA in domestic contexts absent authorization. However, even that amendment recognizes the potential utility of TIA in foreign intelligence contexts and provides that its limitations do not apply to TIA components used to support "lawful military operations of the United States conducted outside the United States" or "lawful foreign intelligence activities conducted wholly overseas, or wholly against non-United States persons." Although the Senate amendment should be modified, the distinction drawn by the amendment between "Domestic TIA" and "Foreign TIA" is a good one. See Rosenzweig, "Congress Should Not Prematurely Short-Circuit the Total Information Awareness Program."

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.[39]

- **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.

LIMIT GOVERNMENT ACCESS TO DOMESTIC INFORMATION DATABASES

The second root of public concerns about the development of TIA lies in the fear that the government will gain access to data to which it does not now have access. TIA should not be a vehicle for expanding the government's storehouse of information about individuals. Rather, appropriately conceived, TIA should mirror existing legal limitations. It should neither expand nor contract the corpus of data available for analysis.

Existing Legal Limitations on the Collection of Data

Fourth Amendment Principles. Under settled modern Fourth Amendment jurisprudence, law enforcement may secure without a warrant (through a subpoena) an individual's bank records, telephone toll records, and credit card records, to name just three of many sources of data. Other information in government databases (e.g., arrest records, entries to and exits from the country, and driver's licenses) may be accessed directly without even the need for a subpoena.

In 1967, the Supreme Court said that the Fourth Amendment protects only those things in which someone has a "reasonable expectation of privacy" and, concurrently, that anything one exposes to the public (i.e., places in public view or gives to others outside of his own personal domain) is not something in which he has a "reasonable" expectation of privacy—that is, a legally enforceable right to prohibit others from accessing or using what one has exposed.[40] So, for example, federal agents need no warrant, no subpoena, and no court authorization to:

- Have a cooperating witness tape a conversation with a third party (because the third party has exposed his words to the public);[41]
- Attach a beeper to someone's car to track it (because the car's movements are exposed to the public);[42]
- Fly a helicopter over a house to see what can be seen;[43] or

39. One model for enhanced sanctions would be section 224 of the USA PATRIOT Act, Pub. L. No. 107–56, which provided for the administrative discipline of federal officers and employees who violate prohibitions against unauthorized disclosures of information and allowed for civil actions against the United States for damages. With TIA, Congress should go beyond that statute and include provisions for individual civil and, in the case of deliberate misconduct, criminal liability.

40. *Katz* v. *United States*, 389 U.S. 347 (1967).

41. *United States* v. *White*, 401 U.S. 745 (1971). A few states have consent laws that restrict the ability of state law enforcement officials to conduct taping of telephone conversations without consent.

42. *United States* v. *Karo*, 468 U.S. 705 (1984).

43. *Florida* v. *Riley*, 488 U.S. 445 (1989) (plurality opinion).

- Search someone's garbage.[44]

Thus, an individual's banking activity, credit card purchases, flight itineraries, and charitable donations are information that the government may access because the individual has voluntarily provided it to a third party.[45] According to the Supreme Court, no one has any constitutionally based enforceable expectation of privacy in such data. The individual who is the original source of this information cannot complain when another entity gives it to the government. Some thoughtful scholars have criticized this line of cases, but it has been fairly well settled for decades.

Congress, of course, may augment the protections that the Constitution provides, and it has done so with respect to certain information. There are privacy laws restricting the dissemination of data held by banks, credit companies, and the like.[46] But in almost all of these laws (the Census being a notable exception),[47]the privacy protections are good only as against other private parties; they yield to criminal, national security, and foreign intelligence investigations.[48]

Access to Data Concerning an Individual and the Distinction Between Government and Private Domestic Databases. Despite the lack of Fourth Amendment protections for data provided by an individual to others, the law still draws a clear and sharp distinction governing access to such information based upon the nature of the entity to which the information has been given. Information that an individual gives to the government (whether federal, state, or local) may be much more readily accessed than that given to private third parties.

With respect to information given to the government, if TIA-based technology accesses the data, it will be accessing information about the disclosure of which individuals have already (as a matter of law) forgone any right to complain: They provided the data to the government in the first instance. So if the government implements a TIA network to query only information from existing government databases, there is no barrier in law. To be sure, some government databases (e.g., the Census and the IRS) are off-limits, and critics can make a plausible case that others should be as well. In the main, however, developing technology to allow querying government databases would, by itself, be a significant improvement. It is precisely the "connecting the dots" that many complain the government did not do prior to September 11.

A similar analysis will apply to what might be termed public, non-government domestic databases. Many non-government databases are readily accessible to the government (as they are to members of the public) either as a matter of course or

44. *California* v. *Greenwood*, 486 U.S. 35 (1988).

45. The same is true of the physical characteristics that one exposes to the public every day. Many have ridiculed IAO's research proposal to develop a means of identifying people from their physical characteristics, deriding it as the "Ministry of Silly Walks." Others fear such a capacity. But the government already has the authority and the capacity to identify an individual by surveillance photographs whenever he or she walks out the front door. (It may not, however, use technology to penetrate that door. See *Kyllo* v. *United States*, 533 U.S. 27 (2001).) From a legal perspective, the "better telephoto lens" proposed by IAO is not off-limits.

46. E.g., 12 U.S.C. §§ 3402, 3403 (bank disclosure); *id.* § 3407 (subpoenas to bank).

47. E.g., 13 U.S.C. §§ 8, 9 (prohibition on disclosure of Census data); *id.* § 214 (penalties for disclosure).

48. Important restrictions on the authority of foreign intelligence agencies to conduct surveillance or examine the conduct of American citizens continue to exist. E.g., Exec. Order No. 12333, 3 C.F.R. 200 (1982), reprinted at 50 U.S.C. § 401 note; Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (April 1983), at *http://cryptome.org/fbi-fic-fci.htm*; see generally National Academy of Science, "Legal Standards for the Intelligence Community in Conducting Electronic Surveillance, February 2000, at *http://www.fas.org/irp/nsa/standards.html*. Conversely, however, the courts have recognized that in the national security context, the requirements of the Fourth Amendment apply somewhat differently than they do in the context of domestic law enforcement. See *United States* v. *United States District Court (Keith)*, 407 U.S. 297 (1972) (applying Fourth Amendment in context of domestic national security surveillance); *In re Sealed* Case, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002) (applying Fourth Amendment in context of foreign intelligence surveillance). None of these limitations should be changed as a consequence of TIA research. Their utility can and should be independently examined as appropriate.

on commercial terms that would apply to the government or any member of the public. Examples of these sorts of databases would include the Yellow Pages and the Associated Press news service. These private entities collect, organize, and disseminate data publicly, and the government is legally free to access these databases just as any member of the general public might.

This makes clear the necessity of drawing a sharp line between government and public, non-government databases on the one hand and private domestic databases on the other. The distinction, which already exists in law, embodies certain protections against government access to private domestic databases. If one provides information of any sort to anyone else (e.g., the bank, the credit card company, or the phone company), the government may secure that information from the private database holder of the information without any notice to the original source of the data.

But the government may not secure this information without notice to the third-party holder of the information; it must issue a subpoena requiring its production. The recipient of the subpoena (i.e., the bank, and not the individual who originally provided the data) can oppose the subpoena after it is issued but before a response is made, and judges adjudicate those cases where there is opposition.[49]

Opposition to subpoenas is comparatively rare, and the grounds upon which a subpoena may be resisted are narrow. One may, for example, oppose a subpoena on the ground that it seeks information that is not germane to the government's ongoing investigative inquiry. But the burden for making such a challenge is high: A subpoena may be quashed only if "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject matter of the…investigation."[50] In practice, this test is infrequently met, perhaps in part because of the self-restraint of government investigators mindful of the existence of a process by which possible abuse can be challenged.[51]

Implications for the Structure of TIA

The existing legal structure and the overarching principles that have been discussed lead to a singular 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

49. There is one exception to the rule that only the data holder and not the original source of the data may object to a subpoena: When a common law evidentiary privilege is asserted, the holder of the privilege who is the original source of the information may appear to assert his right to restrict access to the information being disclosed. Thus, for example, when the government subpoenas an attorney to provide information he received from his client, the client may appear to assert that the request transgresses the attorney–client privilege. See *In re Sealed Case Nos. 96-3085, 96-3086*, 107 F.3d 46, 48 n.1 (D.C. Cir. 1997). But this process is a rarity. No mechanism exists whereby, for example, a bank account holder may protest the disclosure of his bank records to the government. To the contrary, the government may, in the interests of the security of its investigation, impose a gag rule on the bank prohibiting it from disclosing the existence of a government inquiry to the account holder. E.g., 12 U.S.C. § 3409 (delay of notice of subpoena).

50. *United States* v. *R. Enterprises*, 498 U.S. 292 (1991).

51. The second basis for opposing a subpoena—and the far more common one advanced by subpoena recipients—is that the scope of the subpoena is overly broad and it would be unduly burdensome to respond. In practice, since many (though not all; see Timothy Lynch, "The Paper Chase," *Forbes*, January 20, 2003, p. 36) requests are not particularly burdensome (it takes, for example, very little time for the bank to provide copies of the bank transactions of an individual), a bank or other company will routinely respond to requests about an individual rather than advance any opposition. Most telecommunications companies have a subpoena compliance office whose principal function is the routine response to subpoenas requesting information from the company.

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.[52] 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 data-

52. One can envision unusual circumstances where access to the data without notice to the data holder might be necessary in order to protect the integrity of the law enforcement or intelligence investigation. Those circumstances should, however, be rare; telephone companies and banks routinely provide data without compromising ongoing investigative activities. In any event, the law already provides for limited circumstances in which the authorization of a neutral court officer can substitute for the consent of the individual from whom the data are being taken—e.g., the so-called sneak and peek warrants; see, e.g., *United States* v. *Villegas*, 700 F.Supp. 954 (N.D.N.Y 1988), *aff'd*, 899 F.2d 1324 (2d Cir. 1990); Kevin Corr, "Sneaky but Lawful: Use of Sneak and Peek Search Warrants," 43 U. Kan. L. Rev 1103 (1995). A similar legal regime would, in special circumstances, be appropriately applied to TIA data queries.

bases 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.[53]

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), it 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.[54] 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, one aspect of TIA, the Genisys Privacy Protection program, is to be welcomed by everyone on both sides of the discussion. 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

53. See 68 Fed. Reg. 2101–03 (Jan. 15, 2003).

54. Again, the technology under development at IAO to accomplish this objective is more fully described in the accompanying appendix.

administrator control these protections. This methodology would ensure that the privacy protections are not being circumvented.[55]

APPLYING THESE PRINCIPLES: A POTENTIAL REAL-WORLD EXAMPLE

The foregoing discussion has, at times, perhaps been overly theoretical, but it provides an important grounding for a discussion of the real-world application of TIA when, and if, it is ever successfully developed. To make this discussion concrete, consider the real-world example alluded to earlier: Imagine, again, the receipt of credible intelligence information that the precursor components of Sarin gas were being smuggled into the United States by al-Qaeda operatives via flights originating in Germany during the month of February 2003.

Certain information relevant to this intelligence would exist in foreign databases to which U.S. officials might have access either by treaty or, in the case of enemies, through non-consensual means. A query of those databases might assist in identifying the potential terrorists. Other information might already exist in U.S. government databases. TIA-based software might pose a pattern-based inquiry to these government databases in an effort to produce a list of non-resident aliens entering the United States during that period on flights meeting those specifications. It might also pose a query to other government databases identifying known or suspected terrorists. Finally, after authorization from a sufficiently high-level official and notice to the airlines in question (which would have an opportunity to object in court), TIA might query the airline databases for flight manifests of those who traveled to the United States during the relevant period.

From these various queries, the federal government could develop a list of subjects for further investigation. As it stands right now, little of this is possible, and that which is possible is cumbersome and inefficient. By the time the appropriate correlations were made, it might well be too late.

If TIA works as intended, by contrast, the development of a subject list could occur rapidly enough to make it possible to preempt terrorist activity. Meanwhile, privacy protection technology would insure that the data regarding those who were deemed not to warrant investigation were never examined by human agents or, if examined, were partitioned so that identifying personal information was segregated from travel data.

With a list of investigative subjects in hand, TIA could then make subject-based data queries to develop additional information about those identified as warranting further investigation. Again, after notice to the appropriate data holders and their consent, the list of subjects could be correlated with, for example, purchases of canisters necessary for the deployment of Sarin gas (which might have occurred domestically or abroad). If the data queries enabled the government to identify a limited number of suspects, a high-ranking official could authorize a full examination of their activity. This fuller examination might enable the government to identify co-conspirators, sources of funding, and the like.

After September 11, it took hundreds of federal agents several months to backtrack the money trail, travel itineraries, and personal interactions of the 19 terrorists—far too long for the effort to be effective at preempting the next terrorist attack. With TIA, there is at least the prospect of more quickly and effectively identifying and disrupting terrorist activity before it occurs. The government might be able both to identify the "dots" and to put them together in a manner that allows it to short-circuit terrorist efforts to kill Americans—certainly a salutary goal if it can be accomplished without sacrificing fundamental American liberties.

CONCLUSION

The Total Information Awareness program is no panacea. It will not, by its operation, ensure that no further terrorist attacks against America occur. But neither is it an Orwellian monster whose construction will irretrievably alter the landscape of American liberty and freedom. Rather, as with most innovative proposals, it is a technological development capable of both use and abuse in equal measure.

55. See also Markle Foundation "Protecting America's Freedom in the Information Age," October 2002.

The potential for misuse requires constant vigilance—by Congress, the courts, and the public; but a balanced and measured approach, examining the possibilities of the new technology in the context of existing law and taking steps to ensure that its development is consistent with those limitations, is wiser than blanket condemnation. We should be mindful and respectful of the potential for abuse, but we should not let that potential immobilize our response to terrorism. Research into the development of TIA should proceed. Strangling this new technology in its crib is no answer to the threat of terrorism.

—Paul Rosenzweig is Senior Legal Research Fellow in the Center for Legal and Judicial Studies at The Heritage Foundation and Adjunct Professor of Law at George Mason University. Michael Scardaville is Policy Analyst for Homeland Security in the Kathryn and Shelby Cullom Davis Institute for International Studies at The Heritage Foundation.

APPENDIX

TECHNICAL SPECIFICATIONS OF THE TOTAL INFORMATION AWARNESS PROGRAM

In this appendix, we provide a more detailed and technical summary of the Total Information Awareness program and its related components. Our summary is derived, to a large degree, from publicly available information from the Information Awareness Office as released to the research community in the IAO's call for research assistance.[56]

Overview of the Technology

TIA's overall goal is to promote the more efficient transfer and analysis of information in a secure, collaborative, virtual community in order to advance more effective and rapid decisionmaking. Despite information in recent press reports, the aim is not to give government access to any information to which it does not already have legal access, but rather to promote the more efficient use of the information that it already possesses or has the authority to receive. To increase efficiency, research efforts are focused on developing (1) a means of data integration that does not require the physical transfer of data from one repository to another and (2) advanced analytical models that will conduct much of the initial processing of scanned and extracted data.

Technology being developed through the TIA program would be crucial to developing an intelligence fusion capability to remedy the intelligence failures exhibited prior to September 11, 2001. An intelligence fusion center[57] would focus on integrating information from many sources in order to break down the bureaucratic cultures that have prevented effective information sharing in the past. Such a facility should utilizing advanced data-integration and automated data-mining technology to speed the process and make sense of otherwise disparate bits of information. Specifically, a successful fusion capability must (1) include access to and the ability to explore all government databases, including intelligence, regulatory, and law enforcement as described in the body of this paper; (2) integrate the information found in those databases to be usable by individual analysts; (3) make automated independent judgments about that information; and (4) and allow analysts to provide more complete and accurate warning.[58]

One area on which DARPA is focusing significant effort is more advanced techniques for data mining. Data mining or knowledge discovery, according to David Jensen of the University of Massachusetts, uses "algorithms [to] discover useful, previously unknown knowledge by analyzing large databases."[59] The health care industry uses data mining to predict a patient's chances of survival as an aid to better prioritization. Likewise, for intelligence purposes, data-mining technology can allow an intelligence analyst to focus his or her attention on the most relevant information. However, current data-mining systems are insufficient for countering terrorism because they assume that data sets are made of unrelated cases, whereas uncovering existing relationships is crucial to terrorism investigations.[60] The TIA program is working to develop data-mining or knowledge discovery programs to uncover relationships.

Contrary to recent media reports, one of the TIA program's primary goals is to develop a method of

56. See *http://www.darpa.mil/darpatech2002/presentation.html*; see also Poindexter, Popp, and Sharkey, "Total Information Awareness" (providing a technical overview of the program).

57. For a more complete discussion of how an intelligence fusion center should operate, see Wortzel, "Creating an Intelligent Department of Homeland Security."

58. For a discussion of how technology being developed under TIA can contribute to such a capability, see David Jensen, "Data Mining in Networks," at *http://kdl.cs.umass.edu/people/jensen/papers/nrcdbsse02/slide01.html*.

59. *Ibid*.

60. For more on the differences between these two assumptions, see *ibid.*

making information stored electronically in a database available to users linked to that database without having to download it into a central repository or distributed data warehouses that would function as a single entity. Investigating terrorism with the goal of preventing future attacks will require intense sharing of data among agencies in an efficient and rapid fashion.

Attempting to consolidate the terrorism-related information held in a variety of government and commercial databases through existing technology would create a number of problems. Specifically:

- **Adding new interfaces to link existing databases limits scalability,** as every database will require that new interfaces be added for it to be able to communicate. Eventually, the network is likely to become incredibly complex and cumbersome.
- **Development of software that can translate a query into a format that multiple databases can understand is possible.** This removes the need to modify existing systems. However, it does not reduce the complication associated with adding interfaces; instead, it transfers the same problems to the linking software.
- **The final option is to reformat data into a re-engineered database—**a process that is both excruciatingly slow and cumbersome.[61]

To overcome these limitations, the IAO is attempting to develop a means of integrating information without removing it from its original sources. This will depend in part on the IAO's ability to develop query methods that do not need either to know where the data are located or to reference specific fields.[62]

Merely giving an analyst access to numerous sources of data offers little value, however, as it offers no way to determine what information should be looked at and what should be ignored. The IAO is attempting to develop models that software can use to analyze raw data for relevance. The models the IAO envisions will be baskets of detailed information about terrorist activities, the patterns they follow, and their methods of operation.

TIA technology is being tested by the IAO using synthetic data based on past experience and simulated terrorist activities. These tests will allow analysts to determine the specific information encapsulated in each model. If applied in the real world, models would be based on law enforcement data and intelligence information related to past investigations of terrorism. In addition, the IAO is attempting to develop a way for models to evolve continually as new knowledge becomes accessible. For example, if new patterns of activity were uncovered during the course of an investigation, the computer's models would be updated as appropriate.

The models being researched under TIA are intended to be much more comprehensive than the limited profiles that are used today and frequently discussed in the press, such as the invidious use of race or national origin as a proxy for terrorist threats. Ultimately, more sophisticated models will be used to determine what information to extract from databases through queries and to evaluate the relationships among people, organizations, and activities that may be indicated by that information.[63]

The IAO is attempting, through these advanced analytical models, to improve the way the information is queried so that analysts see only data relevant to the terrorism investigation they are conducting. This will allow for more rapid understanding and analysis by reducing the amount of unrelated material that each analyst must analyze. TIA is being designed to allow an analyst to conduct two kinds of queries: subject-oriented, which focus on an individual suspect, and pattern-oriented, which look at suspected activities. Both types of searches will utilize models to provide more detailed results by providing information that is within the context of modeled terrorism

61. For a discussion of these options, see remarks of Lt. Col. Doug Dyer during DARPATech 2002 symposium, at *http://www.darpa.mil/darpatech2002/presentation.html*.

62. *Ibid*.

63. For a discussion of one component of TIA's research, see Information Awareness Office, "Total Information Awareness Program (TIA) System Description Document (SDD) Version 1.1," July 19, 2002, p. 81.

profiles and limited to data that are directly related to the investigation.

The IAO is also researching ways to include credentialing when an analyst submits a query. Inclusion of this information could be used to limit access to government information to those who have a specific need to know and conceivably to ensure that appropriate legal authority has been granted to search commercial data. By developing more advanced query methods, the IAO is seeking to move beyond the current limitations in data profiling that have been criticized since September 11 (i.e., providing additional scrutiny to airline passengers who purchase tickets with cash at the last minute) and to replace them with detailed, complex queries based on actual intelligence through modeling and other sets of conditions.

A crucial distinction needs to be made between what TIA is designed to do and what its opponents have described as its purpose. Critics have claimed that TIA-based networks will look for unusual relationships or patterns in order to identify terrorists without reason to initiate an investigation. Both the public and private sectors frequently use existing technology, including data-mining technology, to identify potential targets (whether for investigation, advertising, or other purposes). These efforts are limited to looking for specific actions such as purchasing airline tickets at the last minute, past criminal activity, and racial profiling.

This option, however, was rejected by the IAO, which is attempting to replace today's limited electronic profiling methods that frequently result in false positives with more detailed analysis of transactional relationships. During the DARPATech 2002 symposium, Evidence Extraction and Link Discovery (EELD) program director Ted Senator discussed the different means that could be used to analyze transactional information:

> Much technology exists to implement the first approach [searching for unusual relationships]. While it can find groups of people who appear to be linked together, it tells us nothing about whether their activities are legitimate or suspicious. It also requires us to make many assumptions about the prior joint probability distributions, such as the likelihood that two people will happen to be at a particular airport together. And there are important and legitimate legal and policy constraints that prohibit its [the technique of looking for these kinds of relationships] widespread use.
>
> Monitoring data streams for indicators of activity can suffer from the limitations of traditional fraud detection techniques and also can be limited to finding instances of previously known or suspected types of threatening behavior. Criteria for new types of threatening behavior can be incorporated after they are discovered, typically after a small but significant number of instances of that behavior surface. This reaction time, of allowing for a small number of new types of incidents before updating the automated system, may work for domains where the goal is preventing most illicit behavior most of the time, such as credit card fraud, but is not acceptable for the one-time rare events of such magnitude that we experienced on September 11.[64]

Instead, the IAO intends to use the models it is developing to sort through information. While DARPA is testing the feasibility of the concept, these models will be based on synthetic data and "red team"[65] simulations of terrorist activity. If applied in the real world, models would be based on law enforcement data and intelligence information related to past investigations of terrorism.

Since the modeling programs will be based on known intelligence, lessons learned from past investigations, and detailed simulations, they should overcome many of these limitations. Doing so will improve the effectiveness of an investigation by reducing the number of innocent people

64. For a discussion of these options, see remarks of Ted Senator during DARPATech 2002 symposium, at *http://www.darpa.mil/darpatech2002/presentation.html*.

65. Red Team exercises utilize a group of people simulating an enemy in order to test defense against an actual enemy attack.

targeted during an investigation—a fact that is also more friendly to a free society than are today's limited generalizations.

TIA's Efforts to Promote Intelligence Sharing

In the past year and a half, it has become abundantly clear that better intelligence sharing might have helped to prevent the terrorist attacks on the World Trade Center and the Pentagon on September 11, 2001. Multiple FBI field offices were conducting investigations related to Arab students at U.S. flight schools; the CIA was monitoring the foreign activities of two of the perpetrators; five were on other government lookout lists; and three had even been stopped by police for traffic violations shortly before the attack. None of these agencies, however, was aware of related activities occurring elsewhere. Even information that should have been shared, such as the names of the terrorists the CIA was tracking, was hoarded. The most effective way to promote information sharing would be to automate the process through the establishment of an intelligence fusion center.[66]

In response, the IAO is continuing over six years of DARPA research on how to use highly advanced information technology solutions to better share and analyze intelligence in order to provide tools to combat terrorism more effectively. Currently, analysts spend hours reading intelligence reports, potentially only to digest a small amount of information relevant to an ongoing investigation. Instead of relying on the electronic or physical transmission of intelligence reports, which analysts will then have to read in order to discover what could be only a small bit of information, the TIA program seeks to provide a quicker mechanism for providing analysts with information specifically related to their needs.[67]

The goal is to use the advanced data integration and analysis tools the IAO is researching to ensure that an analyst has access to the full scope of information the federal government is holding related to their case, to form a virtual network of analysts studying the same issue across agency lines, and to take some of the analytical burden off of the analyst by conducting some of the initial research and data collection. With these services provided, intelligence analysts will be able to focus more on assessing threats and developing recommendations for policymakers.

The first step in this process was to create a virtual environment in which information can be exchanged within ad hoc electronic interagency teams that emerge to study an issue. This was the purpose of project Genoa, launched six years ago and completed by the IAO last year. The knowledge gained under project Genoa is what is currently being integrated into operational computer systems and subjected to field-testing with the Army intelligence community.

This program still requires an individual analyst to provide information to the virtual community. but it also establishes a situation in which they are more likely to realize that such information should be shared and allows information to be shared among a virtual team with the approval of the person or agency holding the information. Genoa technology is being used today in a fashion that falls short of full intelligence fusion; but if used throughout the counter-terrorism community, it would solve some of the most pressing communication problems that occurred before September 11.[68]

The ultimate goal of DARPA's ongoing research in its TIA program is to automate much of this process. In particular, the IAO's Genoa II project is researching ways to automate the excavating and initial analysis of relevant information from that

66. See Wortzel, "Creating an Intelligent Department of Homeland Security."

67. For a discussion of these options, see remarks of Tom Armour during DARPATech 2002 symposium, at *http://www.darpa.mil/darpatech2002/presentation.html*.

68. For example, both the Central Intelligence Agency and the National Security Agency had information on Nawaf al-Hazmi that illustrated his link to al-Qaeda. Prior to September 11, 2001, these agencies had enough information to add his name to State Department, INS, and Customs Service terrorist watch lists. Although adding his name to these lists could have resulted in his entry to the United States being denied, this step was never taken. For more details, see *http://intelligence.senate.gov/0209hrg/020920/hill.pdf*.

held by the linked community and then to capture the knowledge gained by an analyst to support future study. Under the IAO's vision processes, such as the translation and finding of stored data, checks for relevance and the development linkages would occur electronically, allowing an analyst to focus on studying the meaning of the data to establish whether or not a threat exists and then formulate recommendations for policymakers. Research being conducted on modeling, data linking, and other analytical tools will be crucial to this effort.

USING TIA to Query Government and Non-Government Databases

Most of the controversy that has emerged over TIA in the past three months has been related to possible use of the technology being developed by the IAO as a new investigative tool to search commercial transactional data such as, for example, credit card purchases, airline reservations, and Internet activities. Terrorists preparing for an attack will leave an electronic trail of purchases, travel, and other activities just as anybody else living in the modern world does.

Currently, law enforcement agencies can obtain this information legally through the subpoena process. However, without a real-time connection, the information may not be as up-to-date as possible. Improving law enforcement's access to the most current and accurate data could prove a valuable tool for investigating terrorism.

Technology being developed by the IAO to allow subject-oriented queries of data could be used to gain a more complete understanding of a suspect, the suspect's activities, and his or her relationships with others through a search of this trail. Through a pattern-oriented query, TIA solutions linked to this information could be used to identify a terrorist based on intelligence data and the detailed models discussed above. In both cases, established legal and policy guidelines for viewing commercially held data would still have to be followed.

This aspect of TIA would rely on the integration of information held in non-government private databases through a technique similar to but more capable than (and more respectful of individual privacy than) the data-integration and data-mining technology commonly used in the private sector. Data integration and data mining generally refers to the process of extracting, analyzing, and categorizing information from large quantities of stored data. These data can include facts, numbers, or text that is processed by a computer and then typically accumulated and stored in a separate database warehouse. The analysts or users of such a computer can then identify correlations, relationships, or patterns within the large amounts of data.

In the commercial world, data mining can serve many functions: It allows, for example, Amazon to pitch a particular book to you as one you are likely to enjoy based on your past purchases. But it also allows your credit card company to combat fraud by noting anomalous large purchases that may well be the product of stolen credit card data.

TIA, in contrast with commercial data-mining systems, is not being developed to download and centrally store raw data. The accumulation and storage of vast amounts of information runs contrary to the basic purpose of TIA, which is to facilitate an analyst's access to *relevant* information by insuring that pertinent data are not buried under mounds of useless records. Similarly, traditional data-integration methods would be of little value because the information extracted under these techniques would be outdated as quickly as it could be downloaded, reformatted, and made accessible to an analyst.

TIA will also differ from existing data-mining technology by relieving the user of the need to assess the raw data for relevance. It will do this by using electronic modeling and filters to provide analysts only with specific, detailed information related to their requests: a development that could contribute significantly to the protection of personal data by insuring that human agents review only data that exhibit substantial indicia of relevance to terrorist activity.

The IAO intends to establish this link by developing an "appliance" consisting of software and hardware to analyze the information stored in a data warehouse for relevance and—after any private information is filtered out—make that information electronically accessible to the analyst initiating a query. The appliance would be responsible for confirming the credentials of the user attempting to access it; applying the appropriate

rules for its use (based on existing legal and policy constraints and such additional constraints as Congress may see fit to impose); searching the data; determining what may and may not be released; removing private information; and beginning an audit trail.

This process will allow for the greater protection of irrelevant personal information than is provided by the way in which government currently accesses such information through a subpoena. While this is an important component of TIA's research agenda, TIA has barely begun to study its feasibility.

Exactly what databases would be accessed by the technology the IAO is attempting to develop has not yet been determined. Clearly, not every transactional record held by the private sector would contribute to terrorism investigations; but a wide variety, such as financial and travel records, could prove crucial. DARPA has commissioned RAND to study what data should be made available to investigators using TIA technology and the National Academy of Sciences to study the policy implications of such advanced information technology. For research purposes, the IAO plans to create a simulated virtual world made up of imaginary transactional data in which it can test its concepts. DARPA will test the feasibility of the concept and turn it into a working prototype.

As we have set forth more fully in the body of this paper, policymakers and elected officials will have to make a final determination as to what databases may be accessed, what to exclude, and who should have access to TIA technology as an investigative tool.

DARPA's Technical Efforts to Protect Privacy

Protecting individual privacy is an integral part of DARPA and IAO research efforts. Accordingly, the IAO has noted,

> The Information Awareness Office at DARPA is about creating technologies that would permit us to have both security and privacy. More than just making sure that different databases can talk to one another, we need better ways to extract information from those unified databases, and to ensure that the private information on citizens is protected.[69]

Because DARPA is a research and development agency, its efforts in the area of privacy protection are technological and are focused on developing information technology solutions, such as TIA, that can be utilized in a manner that is consistent with American law and respects American civil liberties. As part of its research on privacy solutions, the IAO is developing technologies directly intended to prevent the divulging of personal information and general misuse, including information-partitioning and selective-revelation programs, and filters and software to analyze intercepted data and remove information unrelated to the investigation.

Information partitioning would protect privacy in two ways. First, it would block an analyst from seeing personally identifying information such as names, addresses, and Social Security numbers unless legal authority—such as a Foreign Intelligence Surveillance Act (FISA) warrant—is granted to access it. Indeed, blocking private information collected incidentally is a priority for DARPA generally.

Research on selective revelation recommended by the Information Science and Technology (ISAT) Panel's "Security with Privacy" study and included in TIA would develop barriers between the analyst and the data to prevent access to private information stored in either a government or a commercial repository. The ISAT Panel described how selective revelation could work in practice:

> An analyst might issue a query asking whether there is any individual who has recently bought unusual quantities of certain chemicals, and has rented a large truck. The algorithm could respond by saying yes or no, rather than revealing the identity of an individual. The analyst might then take that information to a judge or other appropriate body, seeking

69. For a discussion of these options, see remarks of Dr. John Poindexter during DARPATech 2002 symposium, at *http://www.darpa.mil/darpatech2002/presentation.html*.

> permission to learn the individual's name, or other information about the individual.[70]

Such a capability would allow federal agencies to use TIA in a manner consistent with existing U.S. privacy laws. The IAO's information-partitioning research could also be used to ensure that those who have access to a network are able to retrieve only information that they have a need to see, providing an added layer of security against misuse.

The Genisys Privacy Protection program is developing filters to record only information allowed by law and other federal guidelines. Filters are commonly used for a variety of purposes to limit information retrieved in response to a query. However, a filter by itself is an insufficient guarantor of civil liberties, as it is only as good as its programming. Simple problems such as a misspelling can inhibit the usefulness of filters while—more important—complex rules may not be readable by both a computer and a person. The ISAT Panel has recommended additional research into rule writing that would be readable by both.

Since a filter may not catch everything, Genisys is also developing a combination of software and hardware that would use models, as discussed earlier, to analyze incoming information for relevance and expunge irrelevant information. This process would occur before an analyst receives a response to a query and would increase both the efficiency of the analyst's search and the protection of individual privacy by providing only relevant information. Using the ISAT Panel's previously described example of a search on individuals purchasing certain chemicals and renting a truck, these solutions could further limit the results produced to those that fit detailed knowledge about terrorist purchasing habits that could be included in the modeling software.

The IAO is researching more tamper-evident and tamper-resistant information repositories to allow for more timely and accurate auditing of use. TIA is being designed to identify users, create an audit trail, and govern the information that is available. These efforts are being designed to monitor not only when users log on and what they do while connected, but also to track how the information is used and where it goes after it is received.

Monitoring how an analyst will use TIA technologies will make it easier to identify potential misuse and quickly take appropriate disciplinary action as required. In many cases, detailed auditing may deter misuse; in others, it will facilitate catching those responsible. Sufficiently secure auditing technologies such as this would contribute greatly to internal and external oversight by either making evident or preventing unauthorized use.

70. Defense Advanced Research Projects Agency, Information Science and Technology Panel, "Security with Privacy," December 13, 2002.