# Protecting America's Freedom in the Information Age

## A Report of the Markle Foundation Task Force

October 2002

*A Project of*

The Markle Foundation,
New York City

*In Alliance with*

Miller Center of Public Affairs,
University of Virginia

The Brookings Institution,
Washington, D.C.

Center for Strategic and International Studies,
Washington, D.C.

# The Markle Foundation
## Task Force on National Security in the Information Age

*Chairmen*

**Zoë Baird**
Markle Foundation

**James L. Barksdale**
The Barksdale Group

*Executive Director*

**Philip Zelikow**
Miller Center of Public Affairs
University of Virginia

*Members*

**Alexander Aleinikoff**
Georgetown University Law Center

**Robert D. Atkinson**
Progressive Policy Institute

**Stewart A. Baker**
Steptoe & Johnson

**Eric Benhamou**
3Com Corp. and Palm, Inc.

**Jerry Berman**
Center for Democracy and Technology

**Robert M. Bryant**
National Insurance Crime Bureau

**Ashton Carter**
Harvard University

**Wesley Clark**
Stephens Group, Inc.

**Wayne Clough**
Georgia Institute of Technology

**William P. Crowell**
Cylink Corporation

**Sidney D. Drell**
Stanford University

**Esther Dyson**
EDventure Holdings

**Amitai Etzioni**
The George Washington University

**David J. Farber**
University of Pennsylvania

**John Gage**
Sun Microsystems, Inc.

**Slade Gorton**
Preston Gates & Ellis

**Morton H. Halperin**
Open Society Institute

**Margaret A. Hamburg**
Nuclear Threat Initiative

**John J. Hamre**
Center for Strategic and International Studies

**Eric Holder**
Covington & Burling

**Arnold Kanter**
The Scowcroft Group

**Robert Kimmitt**
AOL Time Warner, Inc.

**Michael O. Leavitt**
Governor of Utah

**Tara Lemmey**
Project LENS

**Judith A. Miller**
Williams & Connolly

**James H. Morris**
Carnegie Mellon University

**Craig Mundie**
Microsoft

**Jeffrey H. Smith**
Arnold & Porter

**Abraham D. Sofaer**
Hoover Institution
Stanford University

**James B. Steinberg**
The Brookings Institution

**Paul Schott Stevens**
Dechert

**Rick White**
TechNet

*Participating Experts (Non-government)*

**Bruce Berkowitz**
RAND Corporation

**Robert Clerman**
Mitretek

**Mary DeRosa**
Center for Strategic and International Studies

**Lauren Hall**
Microsoft

**James Lewis**
Center for Strategic and International Studies

**Gilman Louie**
In-Q-Tel

**Douglas McDonald**
Abt Associates

**Daniel Ortiz**
University of Virginia
School of Law

**Michael Vatis**
Institute for Security and Technology Studies
Dartmouth College

*Task Force Staff*

**Mary McKinley**
Associate Director

**Ryan Coonerty**
Government Affairs Counsel

**Peter Kerr**
Markle Foundation

**Laura Rozen**
Senior Associate

**Tara Sonenshine**
Advisor

**Stefaan Verhulst**
Markle Foundation

ISBN 0-9725440-0-3

# Table of Contents

# Overview

The geographical boundaries of national security have changed. America has become a potential battlefield for major assaults. Yet, though our military has deeply integrated intelligence and information technology into war fighting, we have not developed a similarly sophisticated use of information and information technology to protect Americans from attacks at home.

Information analysis is the brain of homeland security. Used well, it can guide strategic, timely moves throughout our country and around the world. Done poorly, even armies of guards and analysts will be useless. The Task Force that we had the privilege of chairing has reached some important conclusions to assist our nation in developing its information collection and analysis capabilities.

The federal government is preparing to spend nearly $40 billion a year to protect the homeland. While this report takes no position on any pending legislation, the White House has developed the important concept of homeland security, the centerpiece of which is the Department of Homeland Security (DHS). But almost no dollars have been directed to creating the capacity for the sharing of information and integrating the way it is analyzed, so that out of information collection comes enhanced knowledge. Neither the White House nor the current appropriations pipeline for the new Department of Homeland Security have yet identified the money to turn information collection into knowledge.

With even relatively small sums of money, however, tremendous gains can be made. The new Department of Homeland Security can be the central hub for decisions about what information needs to be collected and stored—in the government or in the private sector—and about where the information should be analyzed and how. The DHS can help develop rules for protecting the well-established liberties of our citizens when information is collected and used. And it can support meaningful research and development efforts. This report describes how. To protect our freedoms, our task—as in previous generations—is to craft the national framework that will draw on this generation's and this society's greatest strengths.

To protect freedom, America's physical safety is essential. Protecting freedom also requires securing the values that define America, including the civil liberties and rights to privacy that make our country special. Rights go together with responsibilities in preserving the public order in which our values can flourish. When Americans feel they must start trading fundamental rights in return for more security, we will know our national security policies are failing. The rule of law is our strength.

Fortunately, to paraphrase John Paul Jones, we have not yet begun to fight. We have not taken adequate and thoughtful advantage of the laws and resources that are already available. We have barely begun to create a serious domestic intelligence capability, one that learns from the abuses of the past and uses the powers that can already be brought to hand.

We have not yet begun to mobilize our society's strengths in information, intelligence, and technology. The Task Force agrees that the U.S. government needs the proposed Department of Homeland Security. But, to us, the most compelling argument for the DHS is that it is a necessary foundation for building entirely *new* capacities for national action. We need to train people, sponsor research, and cre-

ate systems that use information in new ways, finding smarter and more cost-effective strategies that provide both real security and real accountability.

Meanwhile, every agency is rushing out to collect information and buy technology for its own stovepiped systems. As they do so, with congressional and citizen watchdogs trying to chase them across the political countryside, one Task Force member spoke for the group when he warned that, "We may end up getting all of the disadvantages of invasion of privacy with none of the national security gains."

Instead of matching unguided power with unfocused oversight, there is a better approach that borrows from best practices in public and private management: telling officials what they *can* do, as well as setting the limits on their power.

Start by spelling out the kind of information and analysis the country really needs. The solutions start in the way people think and work together. This report illustrates the kind of roadmap that can guide them.

Technology is not a panacea. Those who have called for endless mining of vast new government data warehouses to find intricate correlations are not offering the promise of real security. They instead evoke memories of the walls of clippings collected by the paranoid genius, John Nash, in *A Beautiful Mind.*

Knowledge of the world and those who would do us harm is what is needed. Knowledge does not come from the accumulation of random data, but rather it is found in thoughtful and informed inquiries. Great progress can be made just with sensible, straightforward use of relatively simple tools and already-collected data. Inexpensive data checks, strategically planned, should have been able to prevent the 9/11 attacks. Yet, then, the government lacked the capacities to perform them. Now, more than a year later, the government still has not acquired them.

With this improved definition of the analytic task, the President should issue well-crafted operating guidelines for all federal agencies to encourage confident performance. Only the President can establish and be accountable for the proper balance between development of domestic intelligence and preservation of liberty. These guidelines can embed respect for essential values into the very fabric of the institutions—their core training and their routines. Those guidelines should provide transparent focal points for strong, constructive oversight and proper accountability, both within the agencies and from outside.

America will make a mistake, however, if we create a centralized, "mainframe" information architecture in Washington, D.C., rather than the networked, decentralized system that is needed to defeat the challenge of decentralized, sometimes networked adversaries. The problem is not just information sharing among federal agencies in Washington, D.C. Most of the people, information, and action will be in the field—in regional or local federal offices, in state, regional, and local governments, and in private firms. The federal approach and guidelines can inform and support these local efforts, but information needs to be available widely and should not be required to flow through a central hub.

That is why the information management challenge is also organizational. Our country's leaders should set up the new Department so that it will empower local efforts, nationally coordinated. Promising, innovative local efforts are already springing up across America. To use the power of a net-

work, rather than rely on a mainframe, the federal government must build an operating system that can harness the distributed power of local, state, and federal officials and analysts across the nation. And it needs to be able to integrate information developed from around the world through our foreign intelligence capabilities. This report outlines the organization and the network architecture to do the job.

One aspect of the organizational problem is to sort out the roles of key federal agencies, especially the Department of Homeland Security and the FBI. Our Task Force's basic conception is that the Department of Justice and its FBI should be the lead agencies for law enforcement, exercising the power to investigate crimes, charge people with crimes, perhaps take away their liberty, and prepare cases for trial and appeal. The DHS should be the lead agency for shaping domestic intelligence products to inform policymakers, especially on the analytical side, so that there is some separation between the attitudes and priorities of intelligence analysis and the different, more concentrated, focus of law enforcement personnel authorized to use force on the street to make arrests and pursue or detain citizens.

We understand that criminal investigation (and counterintelligence) often overlaps with intelligence work. Some overlap is natural and good. But the case for a fundamental separation is strong. Intelligence has much broader purposes than criminal investigation. The operational objectives are different. The training is different. The rules about how to collect, retain, and share information are different. The relationships with sources of information are different.

Therefore the DHS should take the lead in collecting information that is publicly available or voluntarily obtained and in analyzing domestic information and intelligence from all sources and setting overall priorities for new collection efforts, working within an interagency process that will include the FBI and other relevant agencies in the intelligence community. It should coordinate the national organization of homeland security task forces in states, regions, and metropolitan areas across the country. But the FBI should continue to have the responsibility for managing clandestine collection operations, like FISA wiretaps or the recruitment of undercover agents, under the supervision of the Attorney General.

The DHS must also develop science and engineering strengths to be able to incorporate advanced technologies that are available in the private sector. This will require procurement practices and private sector expertise that facilitate knowledgeable evaluation of promising capabilities. In addition, the DHS should be able to stimulate progress in IT areas where national needs are great, yet not well served by market forces.

We commend this report to those in government, business, and non-profit communities who feel responsibility for protecting America and to all of our citizens, who play such a key role in ensuring the strength of our nation.

Zoë Baird

James Barksdale

# Acknowledgments

This Task Force commenced its work with a plenary meeting in April 2002. In our six months of work, we have been greatly encouraged by the priority and resources that the federal government and many state and local authorities have devoted to tackling the challenge of improving the potential of information and information technology to enhance our national security. We have therefore tried to develop a truly national framework, fusing this energetic outpouring of patriotic effort into a broad plan of action.

Our Task Force addressed the following questions, to develop a new national framework:

1. What information and which analytic methods do we need most in order to protect Americans at home?

2. How can government better employ the best private sector practices in managing information and developing technology?

3. How should the U.S. government task its agencies to more effectively gather, analyze, and use the national security information it needs, working with the private sector? And what new boundaries to such deployment of information are needed to protect essential liberties?

We organized three working groups to help develop our analysis of these questions, led respectively by Task Force members James Steinberg, Abraham Sofaer, and John Hamre. John received particular help in his working group from Mary DeRosa. These working groups then refined and presented their views at another plenary meeting of the Task Force, held in July 2002. (Their final working group papers are in Part Two of this Report.)

As the report then took shape, we created two additional working groups to take on even more specific tasks. One, on "Connecting for Security," was led by Tara Lemmey; the other, developing illustrative guidelines on "Collection, Use, and Analysis," was led by William Crowell. The efforts of those two working groups are incorporated directly into the Task Force report itself, as readers will see.

This report is not the final work of the Task Force. As governments and citizens around the country create new institutions and guidelines, perhaps along some of the lines we suggest, a series of new challenges will arise calling for more specialized technical, political, and legal assistance. The Task Force will continue to facilitate that phase of construction, helping build structures to use information to protect our freedom in the 21st century.

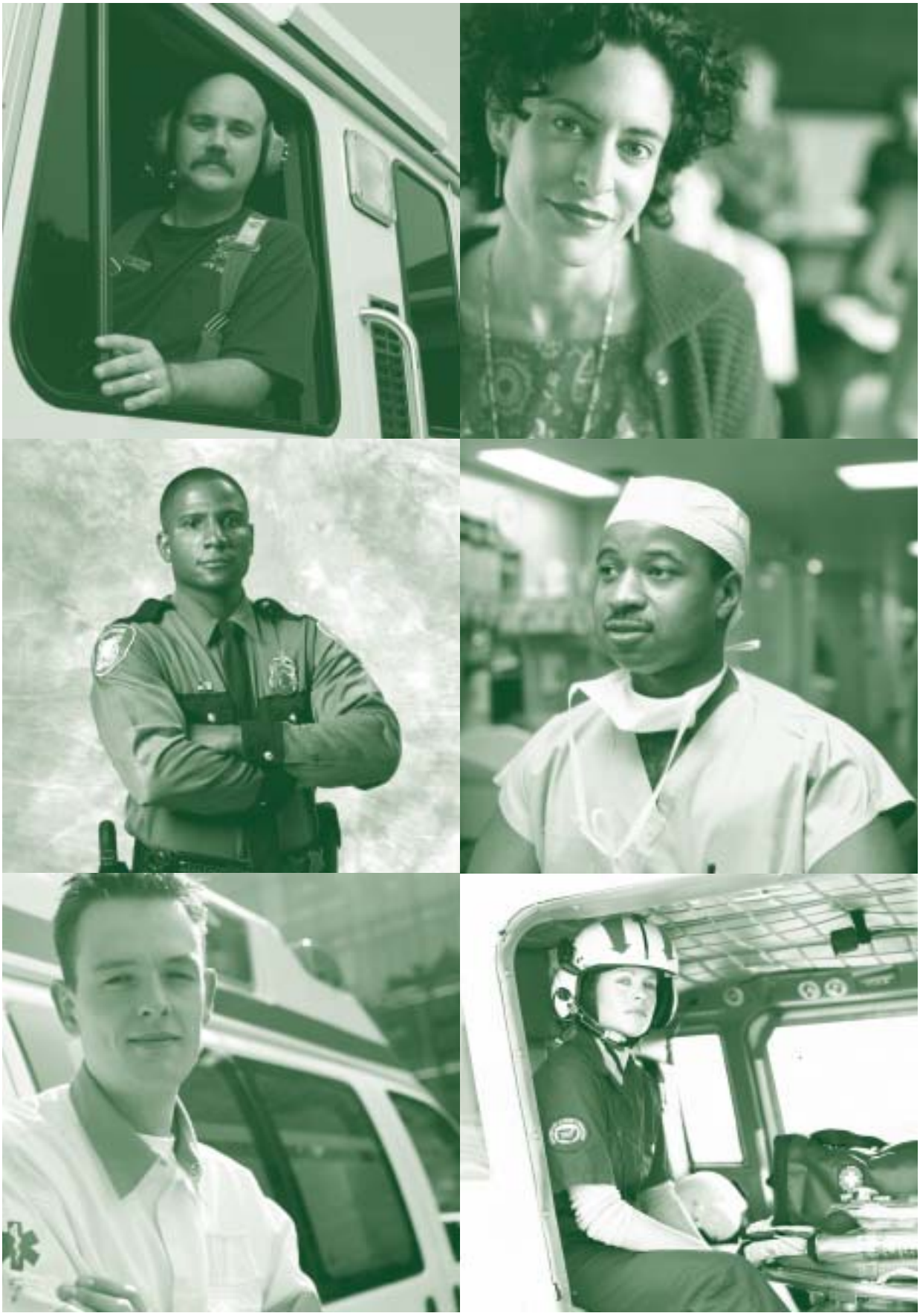
Our executive director, Philip Zelikow, provides exceptional drive and intellect. He joins us in acknowledging the contributions of an extraordinary staff. Mary McKinley runs the operation. Ryan Coonerty and Laura Rozen handle government relations and provide key substantive research and analytical support to the working groups. Wistar Morris oversees the project for the Miller Center Foundation.

Garth Wermter is a resource on technology issues, and Karen Thomas provided an excellent platform on the Web for the Task Force's work. Ann-Woods Isaacs, Chris Freise, and Courtney Stephens work day-to-day to support the Task Force members and staff.

James Lewis of CSIS has been a great asset to our work. At the Markle Foundation headquarters in New York City, we thank Stefaan Verhulst for his thoughtful research assistance, Peter Kerr for his contribution to ensuring that this report contributes to the public's education on these issues, and Karen Byers for her financial management.

Zoë Baird James Barksdale

# Part One:
# THE TASK FORCE REPORT



## The Task Force Report

Many Americans understandably believe that technology is the source of America's military and economic power. They believe this so much that they often seek technological solutions to essentially human problems. But America's technological achievements—in weaponry, commerce, and science—are merely the reflections of strengths in our society, a society that has evolved and is organized supremely well to unleash and promote human initiative. Though we need technology to secure our nation, a successful domestic intelligence and information strategy should start with the way we organize our people to take advantage of innovation.

The way we obtain and use information will determine how well we can protect freedom while striving to attain the objectives set forth in the President's National Strategy for Homeland Security, to:

- prevent terrorist attacks within the United States;
- reduce America's vulnerability to terrorism; and
- minimize the damage and recover from attacks that do occur.

Our vision starts with development of a networked and national homeland security community in agencies, firms, and neighborhoods. In connecting for security, we outline the elements of a next-generation national security infrastructure. We also discuss the organization of domestic intelligence collection and analysis in Washington, D.C., within a framework that respects our nation's traditions and civil liberties.

The problem is broader than just collecting and sharing information. It is the challenge of using information effectively, linking collection with sound and imaginative analysis derived from multiple perspectives and employing cutting-edge technology to support end-users, from emergency responders to Presidents. In other words, we need to *mobilize* information for the new era of national security we have entered.

Domestic intelligence has a deservedly bad reputation in America. Yet we nonetheless believe the country now needs a serious capability to analyze domestic intelligence. In the past we drifted into such serious undertakings through wartime directives and unchecked agency initiatives. Now we should learn from our history and foreign experiences to move ahead thoughtfully and deliberately. To take our civil rights seriously, right from the start, we can chart a path for protecting freedom. To take domestic intelligence seriously, we must address the specifics of the analytical work that needs to be done. To link analysis to action, we give some illustrations of how information can empower people in the field, while also recommending guidelines to protect American liberties, not just American lives.

We also suggest how governments at all levels can form a more effective partnership with the private sector. Some key government agencies have been demonstrably unable to meet the challenge of securing the best information technology. The new Department of Homeland Security must be able to enlist outside expertise. We can tap the best practices found in our private sector. From basic research to product development to acquisition, there are specific reforms that can leverage the power of information to safeguard our freedom.

## A Networked and Nationwide Analytic Community

At the working level in the federal agencies in Washington, D.C., the problem of information and homeland security has been seen, first of all, as a problem of buying new technology. At least that is where practically all the federal money is being spent, like the $300 million for the Information Technology Initiative in FBI's budget for Fiscal Year 2003, a multiyear $1 billion plan for the new Transportation Security Administration's information technology infrastructure, the five-year $550 million plan for the Immigration and Naturalization Service, the $6.9 billion Navy and Marine Corps Intranet system, and the $2 billion "Project Groundbreaker" of the National Security Agency. In fact, according to the White House, the federal government spends a total of about $50 billion a year on information technology.

That may be a good thing. Perhaps even more money should be spent. But while such sums are being spent to modernize each agency's own information systems, some of it relevant to homeland security, almost none of this money is being spent to solve the problem of how to *share* this information and intelligence among theose federal agencies. To be fair, we acknowledge that agencies inside the Department of Defense do spend money on sharing data with each other. On a lesser scale, agencies inside the community of foreign intelligence agencies, like the CIA, also invest in sharing data with their colleagues in the Pentagon and the National Security Agency. But when it comes to homeland security and using integrated information systems, adequate efforts and investments are not yet in sight.

In its $38 billion FY 2003 budget request for homeland security, the administration requested only $200 million for information integration, and is having trouble getting even that. The administration originally sought to create an Information Integration Program Office in the Commerce Department. That faltering effort is now being superseded in hopes of creating such a program in the new Department of Homeland Security. The White House Office of Homeland Security and the Office of Management and Budget are developing promising plans and using their powers of persuasion to realize them. But they need money to make their plans become reality, and money to give agencies positive inducements to cooperate, and the money is not there.

Washington, D.C., is important. It is where foreign and domestic information can often come together, a place where varieties of domestic, foreign, law enforcement, and military information can readily be combined, and where central coordination of a national community can be organized. If anything goes wrong, the spotlight will be on the President. It is up to him to set the expectations for the strong but balanced system we will need. But such a system cannot be based in or directed just from Washington. The President needs to set an expectation and design a system that is truly national and decentralized.

Most of the real frontlines of homeland security are outside of Washington, D.C. Likely terrorists are often encountered, and the targets they might attack are protected, by local officials—a cop hearing a complaint from a landlord, an airport official who hears about a plane some pilot trainee left on a runway, an FBI agent puzzled by an odd flight school student in Arizona, or an emergency room resident trying to treat patients stricken by an unusual illness.

Seen from New York, or Texas, or Utah, or California, the homeland security picture is very different. Those officials think *they* are the ones who really manage homeland security. They have a point. Consider that:

- There are only 11,500 FBI agents; there are more than 50 times as many state and local law enforcers.

- There are only a few thousand professionals in the Federal Emergency Management Agency (FEMA); there are about two million potential emergency responders in the field.

- To work on domestic intelligence against terrorism, the FBI currently has only about a hundred analysts, even by the FBI's definition of the term. Meanwhile there are 40 counter-terrorism analysts just in the Los Angeles Police Department and the NYPD's analytic effort is larger still.

Seen from outside Washington, D.C., local leaders in law enforcement and emergency services have also realized that, although the necessary technology is often beyond what their budgets can afford, linking the right people together is even harder.

The intelligence and other information critical to homeland security will come from across the country and around the world. Washington, D.C., is a critical node in that network, but only one of many. To bring together this far-flung community of analysts and operators working directly on the problems is the real challenge.

Within the federal government we should focus on two key institutions to bring information together for "all-source" analysis. First, there is the Counterterrorist Center (CTC) based at the CIA. It is run as a service for the entire intelligence community by the Director of Central Intelligence. The CTC endeavors to bring together all the agencies concerned with gathering and acting on intelligence from other countries.

The second principal focal point should be the new intelligence analysis center that will be created in the Department of Homeland Security (DHS). This center should bring together relevant information from all sources within the United States, as well as foreign intelligence and open-source information gathered through the Counterterrorist Center. It should combine this information on threats with a mapping of America's vulnerabilities at home and plans to respond.

The DHS should become the base for building up a national community of intelligence contributors and analysts. To create a national infrastructure that is aware, robust, and resilient to the many challenges we face in the 21st century, we have to harness the power and dynamism of information technology by utilizing the strengths and mitigating the weaknesses of our networked society.

## Connecting for Security

The technological advances that created and define the information age have primarily taken place in three arenas (the "three C's"):

- computation (raw computing power);
- communication (degree of connectedness); and
- caching (data storage).

The last 50 years have seen tremendous increases in the capacity of all three of these defining technologies of the information age. Computation tools have advanced from slide rules to pocket calculators to personal computers. Processor speeds have increased by many orders of magnitude. Memory and storage technology have advanced to the point where it is possible to archive previously undreamed of quantities of data. Just in the U.S., connectivity of the Internet has grown to include more than 150 million computer hosts, with far greater numbers connected from these hosts to the Net.

Analytic capacities have grown accordingly. For instance, the tremendous utility of increased processing power combined with increased storage capacity has had a noticeable impact on biotechnology, as the human genome project has made genetic data available online for sophisticated searches and data-mining, leading to new drug candidates and cures for genetic diseases. Everything from economic forecasting to weather forecasting has been significantly enhanced by increases in the capabilities of the three C's.

Just as important is the massive increase in interconnectedness that we have experienced in our daily lives. Dynamic, efficient networks dominate our environment and shape every facet of modern life (the power grid, financial networks, air-traffic and transportation networks, and, most recently, the Internet). Through these networks, moving things like words or money from here to there can be just a click away.

We are gaining a far better theoretical and practical understanding of the natural forms, inherent efficiencies, and inherent vulnerabilities of these interconnected relationships. Whole new areas of study and new scientific disciplines are springing up around these networks and network effects.

The threats to national security are also decentralized, networked, and dynamic. As the new Department of Homeland Security takes shape, we have a unique opportunity to design and implement systems that will enable the best use of central and local resources. We have learned a great deal from the rapid growth in networks of all types in recent years. We can draw on our accumulated knowledge and our existing networks to create a robust, decentralized, and networked national security framework.

As our society has grown more interconnected, communications networks have evolved. Traditional communication networks typically were hierarchical. Primary directories and data repositories were centrally located, with information flow regulated from the top. Emerging communications networks, though, tend to be peer-based, forming dynamic connections among individual participants at and often across levels of an information community. Directories and data repositories are frequently distributed and dispersed.

Participation in such networks can take many forms. Individuals act in a variety of roles, as part of changing organizations. In a national security infrastructure, local police officers, state health officials, and national intelligence analysts are all important actors in the network. Communities of practice—groups of participants in fields like public safety, transportation, agriculture, or energy—can also collectively act in a network. These communities benefit greatly from increased connections to those with similar roles in different organizations or at other levels. In addition, the collective community may come together as ad hoc workgroups, mobilized for specific tasks.

Ad hoc workgroups evolve as they respond to a particular challenge. Members may change in response to community needs. For example, a public health community might include state officials, local hospitals and the Center for Disease Control and Prevention, and in the case of a community with a vulnerable water system, might also include public utility commissioners, building inspectors, and watershed conservationists. In times of crisis, these groups might also involve school officials, transportation officials and the local Red Cross chapter.

These participants are not distinguished by their relationship to a central gatekeeper, but by their relationship to one another. In a distributed, decentralized network, they can, will, and should form unique and utilitarian relationships in order to best support their particular role in national security, whether in prevention, analysis, response, or protection. This peer-to-peer collaboration allows federal, state, and local participants to draw upon the collective expertise of the community.

In an environment of such great risks, empowerment of local actors will lead to better prevention or response management. What we face today is a global, multifaceted problem, and the tools for addressing the challenge may be dispersed among thousands of police officers, state public health officials, firefighters, emergency room staff, or soldiers.

Without waiting for instructions from Washington, D.C., we are already seeing these networks take shape in pioneering pilot efforts around America. Here are some examples:

- In hosting the 2002 Winter Olympics, Utah created a Utah Olympic Public Safety Command, handling dozens of venues and entry points. With resources from the State of Utah and the Pentagon's Defense Threat Reduction Agency, an extraordinary Incident Management System linked—in real time—local and state law enforcement, fire and emergency medical services, and a variety of federal and military agencies. It worked flawlessly.

- Using local resources from the FBI's InfraGard program (an infrastructure protection effort connected to the National Infrastructure Protection Center, now at the FBI but proposed for transfer to the DHS), the Dallas office of the FBI has created an Emergency Response Network that can receive law enforcement or emergency information from the public or any agency operating in north Texas and disseminate it in minutes to thousands of relevant offices through phone, e-mail, or pagers, all while immediately locating the best contacts organized by skills, duties, time of day, and proximity to the incident. The network already links about 500 local police and sheriff's offices, 33 federal and nine state agencies, all branches of the U.S. military, more than 30 fire departments, 15 different critical infrastructure systems, and more than 250 private corporations and organizations.

- The California Department of Justice has established the California Anti-Terrorism Information Center (CATIC) that links federal, state, and local law enforcement agencies throughout the state. CATIC helps organize special task forces, an all-source "situation unit" to analyze and distribute terrorist-related intelligence, and a group analysis effort striving for a broader understanding of terrorist incidents and how to prevent them. Running off RISS.Net (a law enforcement regional information sharing system), the California effort has attracted help from entrepreneurial officials at the Defense Intelligence Agency (DIA), who are connecting the California system to DIA and the New York City Police Department.

- The Houston Police Department and the local FBI's Joint Terrorism Task Force have helped create a Texas Coastal Region Advisory System (TCRAS) to support federal efforts to get homeland security related information to law enforcement and emergency service agencies.

- Within the Department of Defense, the Defense Advanced Research Projects Agency (DARPA) has created an Information Awareness Office that is developing a prototype system for "total information awareness." This system will integrate ideas and technology from more than eight individual DARPA R&D projects. The new Information Awareness Center is based at the U.S. Army's Intelligence and Security Command. That Command also supports the Army's Land Information Warfare Activity at Fort Belvoir, which Congressman Curt Weldon (R-PA), among others, credits with already having one of the most effective open-source data analytical capabilities in the intelligence community.

- Law enforcement officials in Pennsylvania have benefited significantly from JNet, a Java-based tool that can query police, parole, probation, corrections, and motor vehicle databases at the state and local levels. JNet is accessible to more than 2,800 state law enforcement personnel and is often used by federal officials to track suspects. JNet will soon be available to law enforcement officials statewide. But already it has been touted as a model for future information sharing infrastructures.

- The Los Angeles County Sheriff's Department has created a Terrorism Early Warning (TEW) group to connect law enforcement, fire, health, and emergency management agencies to circulate warnings, analyze possible dangers, check public health and epidemiological indicators, and manage possible consequences of a terrorism event.

These systems use various technologies and different standards to format and exchange data. What unites them and makes them successful models is that they have incorporated and expanded upon existing organizations and professional networks already working in their communities and regions. They took local needs, practices, and input into account. They are "ground-up," not "top-down." They are "integrated," not "stovepiped." As Dallas ERN Coordinator Art Fierro (an FBI special agent) told our staff, "We serve as an umbrella. We don't replace local business and infrastructure. We build and work through the networks and individuals that are already there." That is a start. What is needed now is national leadership to combine these experiences and knowledge into a truly national system.

Emerging Bush administration plans for homeland security information sharing envision a three-layer system, or enterprise architecture:

- The top layer would be comprised of top secret information drawn from sensitive sources or methods of collection. Dominated by foreign intelligence, this network would build on existing

intelligence community networks like "CT Link," connected by the Joint Worldwide Intelligence Communications System.

- The middle layer would have secret information, including military data. This network would use existing networks like "IntelLink," joined by the Defense Department's Secret Internet Protocol Router Network (SIPRNET).

- The bottom layer would contain unclassified information, including the actionable data fed down from the higher layers, and sending unclassified information upward. This information would principally be of a law enforcement or domestic character. Existing and emerging networks might be linked through some still undetermined mix of the Defense Department's Unclassified Internet Protocol Router Network (NIPRNET) or a single Web interface for the two main Justice Department networks for law enforcement—Law Enforcement Online (LEO) and the Regional Information Sharing Systems (RISS.net).

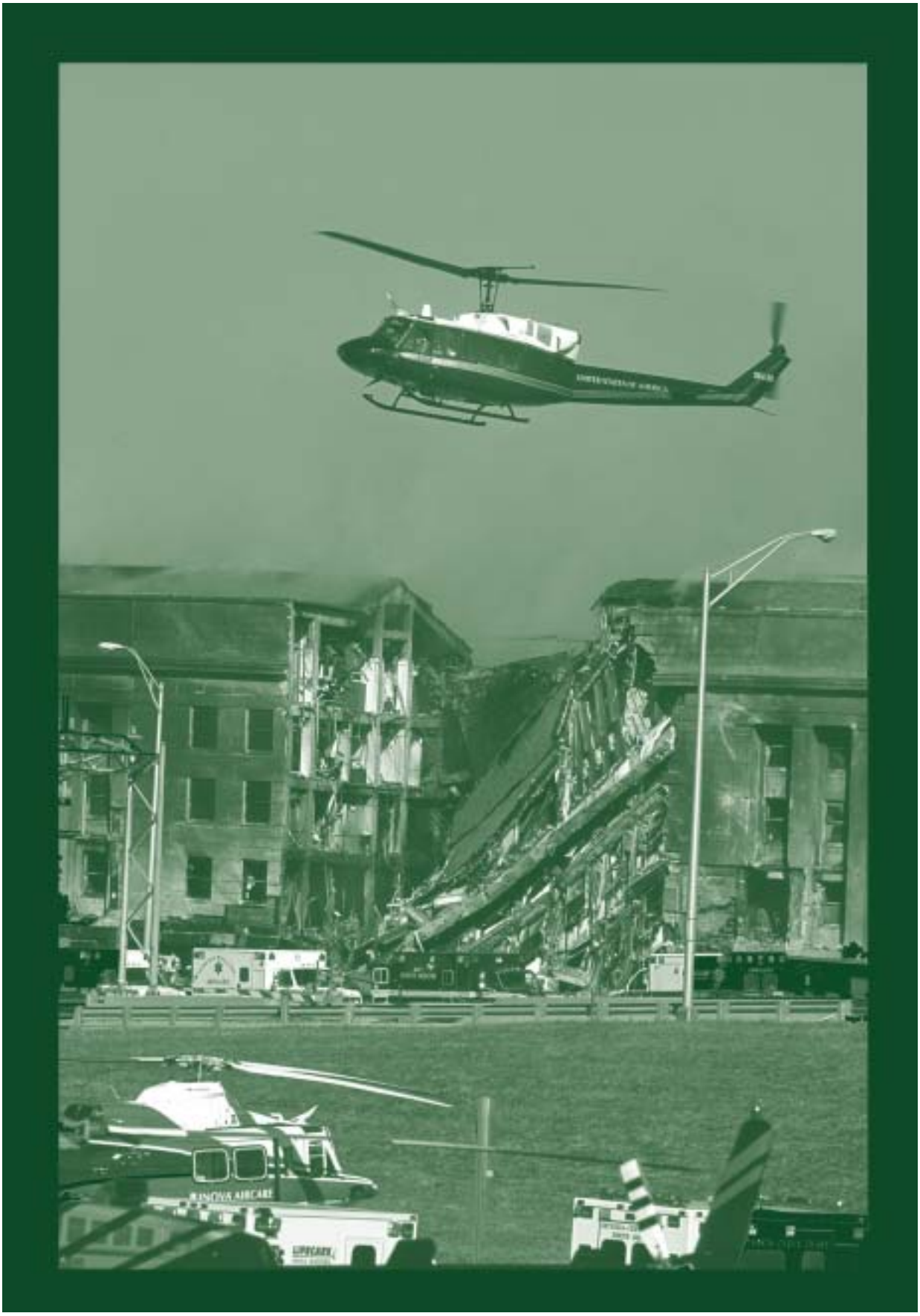
This planned system would be governed by the agencies that host the networks (like DOD for SIPRNET), perhaps with some overarching guidelines supplied by the White House Office of Homeland Security and the new Department of Homeland Security.

While we welcome this emerging plan as a starting point, we believe that this concept is too Washington-centered, too hierarchical, and too narrow in its scope. It does not go far enough to take advantage of the distributed, networked concepts already becoming evident in some of the pilot projects mentioned above.

The federal agencies are rightly concerned about the security of this prospective network and the security of the data being shared on it. We understand the importance of protecting intelligence sources and methods as well as sensitive personal or law enforcement information. A balance must be struck. But we believe the current balance should tilt further in favor of using the power of networked information and analysis, letting much more varied ad hoc communities of practitioners work together without waiting for central permission. Parts of the Defense Department are already realizing some of this potential in the way they are conducting the ongoing war in Afghanistan. DOD researchers sponsored by DARPA's Information Awareness Office have also concluded that the whole government should adopt ambitious networked information strategies for homeland security. Leaders may need to craft bolder architectural designs and then pull their agencies toward building them. Technology solutions, like firewalls, can help, and so can the use of audit trails to record and check on who has accessed which data.

To guide and support—not quash—local initiative, the new Department of Homeland Security, working with the President's Office of Management and Budget can develop guidelines to "charter" projects involving federal, state, local, and private sector participants. These projects can become the elements of a next-generation national security infrastructure. To show what we have in mind, we offer **ten elements** of effective programs in Illustration #1, "Some Characteristics of a Next-Generation Homeland Security Information Network."

We welcome the initiative of the National Governors Association to build on the burgeoning pilot projects and develop model "charters" that can facilitate creation of a national, networked analytic community across America. We are encouraged by the support this initiative has received from governors and from administration officials. This Task Force will be a partner in that effort.



## Illustration No. 1: Some Characteristics of a Next-Generation Homeland Security Information Network*

**1. Empower Local Participants**

Local participants must be empowered to contribute, access, use, and analyze data. At the same time they must be allowed to identify, access, communicate with, and assemble other participants in both the public and private sectors.

Expert groups must be allowed to form at the edge of the network. Data should be maintained and rule sets should be developed and implemented by and among local participants. Each should be allowed to undertake as much work as they are capable of doing.

Push computing requirements away from the center to utilize excess capabilities at the "edge" of a network, allowing mini-centers to develop around local expertise, which can then be accessible to other network participants.

**2. Provide Funding and Coordination**

Centrally designed and controlled systems are too rigid to evolve quickly, but a well-coordinated system of empowered participants can be nimble, effective, and responsive. Such a system is not only desirable, but also crucial to the success of our national security personnel in the future.

The DHS has the unique power to coordinate the many elements of this system. There are many areas that demand coordination: appropriate data sharing technologies such as XML must be identified and evaluated for applicability; decentralized and comprehensive directories will be required to ensure that individual participants can identify and access information; querying systems must be developed and maintained; network traffic and usage must be tracked and analyzed; and a common vision must be articulated and rewarded to effect cultural change.

**3. Create Safeguards and Guidelines to Protect Civil Liberties**

National security systems should raise concerns about privacy, civil liberties, and due process. To protect against abuse in how information can be used, accessed, or shared, participants need clear guidelines based on our laws and social values.

The DHS should take the lead in creating robust permissioning structures and audit trails that will help enforce appropriate guidelines. These critical elements could employ a wide variety of authentication, certification, verification, and encryption technologies. Role-based permissions can be implemented and verified through the use of certificates, for example, while encryption can be used to protect communications and data transfers. A robust Public Key Infrastructure (PKI) or other authentication system within the network, driven by DHS at the core, may turn out to be crucial. Auditing tools that track how, when, and by whom information is accessed or used ensure accountability for network users. These two safeguards—permissioning and auditing—will free participants to take initiatives within the parameters of our country's legal, cultural, and societal norms.

**4. Eliminate Data Dead Ends**

Intelligence and law enforcement officials have already identified the stovepiping of information within an agency as a dangerous impediment to national security. But they have failed to overcome it.

Information must be shared on the network, subject to need, suitable permissions, and classifications. In some cases the information shared may not be the data itself, but pointers to the person

who controls the data, or who is informed about a topic, or who has access to more classified information. This allows for an object-oriented and self-organizing approach to the information. Participants must be able to identify, contact, and engage their peers through robust directories and identity systems, and access useful and relevant information by using comprehensive querying and analysis tools.

A national security infrastructure must enable, facilitate, and at times, demand two-way communication. To the extent feasible, one-way communications should be eliminated, ensuring that users never reach a "dead end" on the network. Networks that only enable one-way communication often break down into insular groups and isolated regions, inhibiting the flow of information needed to address today's threats. Individuals who contribute to the network must also receive information and feedback from the network and other participants, ensuring that participants at the edge of the network remain engaged and motivated.

**5. Design a Robust System**

The network must be designed and deployed to withstand extreme stress or crisis. Points of failure must be identified and minimized, just as points of access must be maximized to encourage widespread usage among qualified participants. Systems must be designed from the "bottom-up," in order to facilitate dynamic and rapid evolution in response to changing needs.

Redundancy, interoperability, and open standards are all elements that constitute robust networks. Ensuring that the network can continue to operate in the event of the loss of a portion of the network is crucial—a so-called "graceful collapse" will prevent catastrophic failures. The ability to find, access, and use data demands common or interoperable data structures and schemas; the industry standard, XML, is an obvious option that can facilitate access to legacy data as well as provide utilitarian structures for to-be-collected data. Meta-data, watermarking, and indexing tools can facilitate data interoperability, storage, and retrieval. Communications standards—TCP/IP, HTTP, and other common Internet technologies—can help simplify and ensure that connectedness is maintained throughout the network. Keeping computation and storage at the edge of the network also allows for redundancy and capacity building.

**6. Create Capacities for Network Analysis and Optimization**

Network traffic and usage analysis is a powerful tool. Noticing a surge of inquiries from public health officials about a particular problem might alert analysts to a larger danger. The homeland security infrastructure should employ a wide variety of these techniques for counter-intelligence, finding network vulnerabilities, and enhancing robustness. Future networks should be designed with interfaces that give insight into transactions across the network and take advantage of new applications that enable and enhance analysis.

Network traffic and usage data may reveal significant findings, especially when collected and compared over time. Increased activity in one area or an increase in searches on a particular topic may in itself be useful knowledge. The development of local expert groups may alert other network participants to potential concerns or especially useful information.

Modeling of optimal coordination among the network players can provide empirically based scenarios on how to centralize, decentralize, or otherwise improve local coordination based on events and needs.

**7. Design for Growth and Plan for Upgrades**

Networks should be implemented with the simplest design possible and designed from the bottom up, allowing the requirements of local participants to shape the growth of the network.

Multiple, layered simple elements always provide a more robust and evolutionary environment than preplanned systems. For example, requiring minimal common data formats allows for interoperability and does not limit the organization to a specific or outdated technology solution, while at the same time such minimal common formats can provide for future growth and expansion.

Such a design also allows for the addition of new technologies with minimal disruption to the existing infrastructure or operations. Increased use of sensors and telemetric devices in data collection, for example, can be incorporated into a flexible system based on open standards much more simply than into centralized, proprietary systems. Redundant systems allow for the continued operation of the network even as upgrades are made on portions of the network.

**8. Enhance Existing Infrastructures**

Existing data collection and analysis processes and infrastructures remain crucial. Emerging infrastructures must be designed to exploit these existing tools. The ability to share and transfer data between older "legacy" systems and the new ones will depend, for example, on the use of open data standards. Connecting local participants at the edge of the network with users who still use more traditional, centralized information systems may require bi-directional communications and appropriate permissioning and authentication systems.

**9. Create Network Aware Scenarios**

With today's ever-increasing computational power, we can use the data being provided by the various local participants to explore new scenarios. Models for possible attacks and responses—"red" and "blue" team exercises—are enriched by being able to explore, generate, and simulate complex scenarios. These models can then inform or make better sense of puzzling but disturbing queries that might come from analysts in the field.

**10. Create a Connected Culture**

A cooperative, collaborative culture is required for the success of dynamic connectedness. Just as individuals are empowered through next-generation network designs, participants must also support the successful exploitation of these technologies through positive reinforcement, peer pressure, and accountability as well as repudiation of users who abuse the system.

Feedback systems that reward valuable contributors will help establish credibility both for individual participants and the network as a whole. Reliable, robust, and secure communications will encourage interactivity. Appropriate and verifiable permissioning systems will support the development of trustworthy relationships. Networks that drive both electronic and traditional collaboration can create a mutually reinforcing environment for all involved.

**This illustration was drafted principally by the Task Force's working group on "Connecting for Security," with particular contributions from Tara Lemmey, Lauren Hall, James Morris, John Gage, Governor Michael Leavitt, Robert Clerman, and Mary McKinley.*

## Organizing the National Homeland Security Community

It should be apparent by now that we believe the new Department of Homeland Security (DHS) offers an extraordinary institutional opportunity to create the new capacities for government action that the country will need. The new Department should be the hub for accumulating, analyzing, and networking domestic information and intelligence from every available source. This analysis would then be linked firmly to action from a federal executive department operating in every part of America, in concert with state, local, and private sector partners.

With this conception in mind, the most important organizational challenge for the President and Congress may be to sort out the respective roles of the DHS on the one hand and the Department of Justice, specifically the FBI, on the other.

America's past experience with domestic intelligence is illuminating. During and after World War I, without special statutory authority, the predecessor of the FBI and other federal agencies engaged in activities that a subsequent Attorney General, Harlan Fiske Stone, described in 1924 as "lawless, maintaining many activities which were without any authority in federal statutes, and engaging in many practices which were brutal and tyrannical in the extreme." When the FBI was created, Stone instructed its new director, J. Edgar Hoover, that "the activities of the Bureau are to be limited strictly to investigations of violations of law."

In the mid-1930s, based upon vague, conflicting, and informal presidential requests to investigate "subversion" and "potential crimes" related to national security, the FBI built up a broad domestic intelligence program, notably in a "General Intelligence Division," *in addition* to its growing and vital counterintelligence efforts. The executive branch chose not to seek any legislative authorization for these moves, and Congress declined to confront President Roosevelt or Hoover about it. The programs expanded and became institutionalized as part of the effort against internal Communist subversion from 1946 to 1963. The FBI became increasingly isolated from effective outside control. During the 1960s and early 1970s these domestic intelligence programs were applied to a widening range of domestic activity by American citizens, as documented in the Church Committee report of 1976.

As presidents and Congress reacted to these abuses, the FBI's domestic intelligence activities were dismantled. The Bureau returned to a narrower definition of its law enforcement mission. During the 1980s, and especially the 1990s, growing dangers from domestic and international terrorism forced the FBI to devote significant resources to investigation of terrorist groups in addition to its continuing counterintelligence duties. But until quite recently the FBI has not developed a systematic domestic intelligence capability, in part because of its dedication to its traditional law enforcement mission and in part because of internal factors—pressed on one side by leadership at headquarters anxious to avoid the abuses of the past and pressed on the other by public criticism and lawsuits.

Today the FBI is under pressure once again to return to the work of domestic intelligence that needs to be done, to hire and train hundreds of new intelligence analysts and use the collection authorities that were recently expanded by the USA PATRIOT Act and revised investigative guidelines issued by the Attorney General.

The proposed creation of a new Department of Homeland Security is a remarkable opportunity to reflect and consider the way ahead. The administration and many leaders in both houses of Congress agree that this new Department should have a key role in domestic intelligence.

Our Task Force's basic conception is that the Department of Justice and its FBI should be the lead agencies for law enforcement, exercising the power to investigate crimes, charge people with crimes, perhaps take away their liberty, and prepare cases for trial and appeal. The DHS should be the lead agency for shaping domestic intelligence to inform policymakers, especially on the analytical side, so that there is some separation between the attitudes and priorities of intelligence analysis and the different, more concentrated, focus of people authorized to use force on the street to make arrests and pursue or detain citizens.

We understand that criminal investigation (and counterintelligence) often overlaps with intelligence work. Some overlap is natural and good. We believe the FBI should continue to be the entity responsible for domestic intelligence collection operations in countering terrorism that are undertaken under their criminal and foreign intelligence collection guidelines. But there is a strong case for a fundamental separation of the analytic function, which will also gather information that is publicly available or volunteered. Intelligence has much broader purposes than criminal investigation. The operational objectives are different. The training is different. The rules about how to collect, retain, and share information are different. The relationships with sources of information are different.

The working group paper in Part II, drafted for that group by John Hamre and Mary DeRosa, points out that, unlike an intelligence agency, the orientation of a law enforcement agency is primarily reactive. Its purpose is to capture and prosecute criminals. Law enforcement agencies often will prevent acts of terrorism or other crimes by catching a criminal before a crime is committed, but they collect information to detain criminals, not to provide warnings, assess vulnerabilities, or inform policymakers. The customer for law enforcement information is the prosecutor and a significant concern in its collection is the suitability of the information for use in court. Law enforcement and foreign intelligence information are collected using many of the same tools and techniques, but different legal authorities and guidelines.

The FBI's culture is that of a law enforcement agency. There is little representation, particularly in the senior levels of the agency, from people with experience in national security. Although senior personnel interact regularly with national security policymakers, there is a resistance ingrained in the FBI ranks to sharing counterterrorism information with the national security community or others outside of law enforcement channels. Unlike our foreign intelligence agencies, the FBI has no effective process for providing intelligence on terrorism to policymakers and others outside of the law enforcement community who need it. Moreover, the FBI has not prioritized intelligence analysis in the area of counterterrorism. The role of analysts is not valued at the FBI the way it is in other intelligence agencies. There is insufficient funding and staffing to conduct the kind of intelligence analysis that is needed for domestic intelligence in the counterterrorism area.

For the FBI to achieve its important potential in this field, it should concentrate on its own law enforcement, counterintelligence, and counterterrorism mission. As Director Robert Mueller has acknowledged, the FBI should do a better job of analyzing its own law enforcement information, and in the process it can also reach its potential as a contributor to the intelligence community as a whole.

The DHS should rely on the FBI to carry out FISA wiretaps and recruit informants or other clandestine agents, under its existing legal authorities. Thus the implementation of clandestine collection would remain under the supervision of the Attorney General, without requiring the enactment of any new warrant authorities for the DHS.

The FBI has few true intelligence analysts working against terrorism. It is only beginning to build a serious capability. We think those efforts should focus on the analysis of law enforcement intelligence to support the FBI's own operations and contribute to the intelligence community. Some highly skilled analysts now at the FBI may then transfer to the DHS, perhaps finding a better career niche in an environment more devoted to intelligence analysis.

The problem of the FBI's multiple roles has been spotlighted recently by the U.S. Foreign Intelligence Surveillance Court. In an unusual May 2002 opinion the Court publicly voiced grave concerns about the FBI's past failures to maintain a distinction between gathering foreign intelligence and gathering evidence for criminal prosecution. The Court sharply criticized repeated FBI distribution of its intelligence information to criminal squads and to prosecutors who were trying to build cases for trial. (The case is *In re All Matters Submitted to the Foreign Intelligence Surveillance Court,* written by Presiding Judge Royce Lamberth with the concurrence of all seven judges of the Court.)

The Justice Department is appealing the decision, arguing that the USA PATRIOT Act passed in 2001 has lowered the wall between law enforcement and intelligence gathering. The DOJ may prevail in its argument that the newly revised law permits prosecutors and law enforcement agents to run intelligence wiretaps. But that does not mean it is a good idea to combine the two functions. The war on terrorism needs good police and good prosecutors, but it does not have to put them in charge of all information gathering and intelligence collection.

The FBI and its judicial overseers must go through elaborate and inefficient contortions in order to manage the combination of so much sensitive intelligence collection and law enforcement responsibility in one set of institutional hands. In proposing a new Department of Homeland Security that has explicitly been granted substantial domestic intelligence responsibilities, Congress and the President now have an excellent opportunity to devise a more workable division of responsibilities.

Whatever they decide, in order to justify keeping the clandestine collection mission in the FBI, the Bureau needs to build up a dedicated and specially trained collection staff, with its own structures for accountability and oversight. To keep this mission in the FBI as we have suggested, one option might be to create a separate division with these special characteristics and its own career track within the Bureau, a service within a service.

We agree with the administration and both Houses of Congress that the DHS should receive and analyze foreign and domestic intelligence from every part of the government. We further believe it should collect and sift information about vulnerabilities from many kinds of federal, state, and local agencies as well as from hundreds of firms in the private sector. Meanwhile it should coordinate plans, training, exercises, and federal assistance for responding to many kinds of emergencies that may arise. Specifically in the area of information, the DHS should be the main federal coordinator for the next generation homeland security network we recommend in the previous section.

The DHS should have lead responsibility as the all-source intelligence analysis center for all relevant domestic information, which should be integrated with assessments of vulnerability and incoming foreign intelligence. The bills moving through Congress would make the intelligence portion of the DHS a formal part of the intelligence community.

In the United Kingdom, Israel, Germany, France, and Canada, distinct agencies have lead responsibility for domestic information and intelligence gathering as well as all-source analysis. We are not advocating that the United States mimic the precedents set in any of these countries. But the precedents are suggestive. In these countries the domestic intelligence agencies are separate from the lead law enforcement agencies. But once a terrorist incident occurs, or operations are mounted against particular suspects, the lead is handed off to the national or local police, who often, and rightly, have strong anti-terrorism operations of their own.

- The domestic intelligence organizations in the United Kingdom (the Security Service, also known as MI-5), Germany (BfV), France (DST and DCRG), and Canada (CSIS) are separated from their countries' law enforcement organizations but are within the same ministry (the UK's Home Office, Ministries of the Interior in Germany and France, and Canada's Ministry of the Solicitor General). In Israel, the domestic intelligence agency (the Security Agency) is also separate from the law enforcement organizations, but in this case the Security Agency reports directly to the Prime Minister, while the national police are under the Ministry of Public Security.

- All of these relationships have been worked out through painful experience. None are easy. But each of these countries has found that law enforcement and intelligence work do not mix easily. Law enforcement has special requirements, including an overt, dominant presence in tactical operations "on the street" and the preparation of cases for trial. Intelligence planning and analysis is a long-term craft, usually operating best behind the scenes with different training and objectives.

As part of an interagency collection management process, the DHS should have the lead responsibility for setting priorities, and giving overall guidance, for obtaining the collection of domestic intelligence required in order to deliver the robust analysis policymakers need. As a statutory member of the intelligence community (such provisions are in both the House and Senate bills), the DHS should develop intelligence collection priorities in concert with the Director of Central Intelligence, the FBI, the Department of Defense, and the National Security Adviser to the President (as well as the Homeland Security Advisor, if that position is retained).

Of course, nothing should prevent the DHS itself from overtly gathering domestic information. In the foreign intelligence world, overt collection is what the Department of State or even the CIA's Directorate of Intelligence can do on its own: go about openly, talk to people, and buy or collect open source data. It would not recruit clandestine agents or secretly eavesdrop on communications.

The DHS could take the lead in processing and analyzing the full "take" from such operations where they have an intelligence purpose, while the FBI retains all its current collection and analytical responsibilities in its own law enforcement, counterintelligence, and counterterrorism work. Where the intelligence and law enforcement material is mixed, the DHS can filter and pass information back to the FBI for specific criminal investigations.

Foreign/domestic distinctions also matter in the way information is shared. By putting the DHS at the hub of the distribution, that agency can filter the flow of domestic intelligence into the hands of police and prosecutors preparing a possible criminal case, where this information could also be discoverable by attorneys representing the criminal suspect. The DHS can also filter the flow of domestic intelligence into foreign intelligence agencies like the CIA, which are still restricted in their domestic activities by laws and executive orders.

Since protecting the homeland is a responsibility shared by every citizen, private sector cooperation will be easier as part of the wide-ranging analysis of domestic information that the DHS must necessarily perform as part of its responsibilities for protecting critical infrastructure. Even now, the private sector is much more likely to cooperate with government agencies in administrative proceedings than in the shadow of criminal investigations.

Clarifying lead responsibility in the DHS for shaping the priorities and analysis of domestic intelligence is a major undertaking, but this executive responsibility is already stated or implied in both the House and Senate versions of the legislation that would create the new Department. This arrangement could become a source of friction between the new department and federal law enforcement agencies like the FBI. Some of that is unavoidable and will need to be worked out in day-to-day practice.

Finally, the networked, national community we have described earlier should be built around organizations that bring together people, not just their computers. We therefore endorse the administration's proposed creation of Homeland Security Task Forces in every state, and recommend that they be supplemented by regional Homeland Security Task Forces as well.

Each of these Homeland Security Task Forces could be co-chaired by a representative of the President—a state or regional DHS representative—along with a representative of the governor (or top regional/local official)—such as the state's director of public safety. These task forces should bring together law enforcement, health, and emergency management officials from all levels, along with representatives from Defense Department elements such as the National Guard and the new Northern Command, and key representatives from the private sector.

In our conception, shared by at least some senior administration officials, these Homeland Security Task Forces would be broadly based. They should include but transcend the existing law enforcement interagency bodies like the Joint Terrorism Task Forces. They can be constructed by using the foundation already laid by the regional organization of the Federal Emergency Management Administration, an organization that is likely to be absorbed into the DHS.

Such a virtual homeland security community could eventually be extended internationally to include countries that have the closest information-sharing relationships with the United States. This would be part of a national security policy that extends the concept of joint planning from the military sphere to the wider range of agencies involved in homeland security. This is an aspect of NATO's transformation. Our institutions for bilateral cooperation may need to adapt too. The varied counterpart officials in these countries would be expected to respect our guidelines to avoid misuse of information.

## What the Analysts Should Do

### (A) Wide Scans to Identify Vulnerabilities.

Intelligence is often conceived as perpetrator-centered and event-focused, locating individuals associated with terrorism and uncovering their plots. As the paper from the working group on analytic methods (included in Part II of this Report) points out, however, the highly focused threat-based approach should be supplemented by peripheral vision. Working with other relevant agencies, the DHS center should map and prioritize the most vulnerable potential *targets* and the most dangerous *means* that could be used to attack them. This is why it is so essential that intelligence and critical infrastructure protection *both* be placed under the DHS's Undersecretary for Intelligence. The analysis of threat and vulnerability must be combined in one place.

Scenario analysis is one name for a method that puts analysts in the place of a potential enemy and then works through the specifics of how that enemy would work through the operational details of a possible attack. This kind of analysis is also sometimes referred to as using "templates," or a "project planning paradigm," or "red-teaming." This analytic effort can be top-down, which in this context means that intelligence analysts might organize the effort and then reach out to specialized teams drawn from the agencies that focus every day on those subjects, like agriculture or nuclear reactor safety.

But scenario-generation should also come from the field—from the "nodes" of the networked analytic community. They may add some original ideas because they start with different preconceptions. (An example is the "Phoenix" memo from an FBI agent in Arizona who encountered a particular local case and began worrying about Muslim terrorists in U.S. flight schools.)

"Means" analysis, looking hard at access to particular technologies or vehicles of attack, is another powerful tool, especially if combined with countersurveillance of possible targets or means of attack. Means analysis might reveal the most cost-effective forms of prevention. For instance, means analysis would think about how to harden airplane cockpit doors to prevent terrorists from being able to take over a plane.

Risk analysis is an especially prominent technique among engineers and other safety experts. That field has developed some proven methodologies for ranking and filtering possible dangers and assessing the most effective ways of preventing them.

Once wide-scan efforts can home in on key access points to high value targets or means of attack, national guidelines can be developed for screening individuals for entry through these "gates." Biometric identification systems work best in controlled settings, where combinations of biometrics (*e.g.,* facial recognition algorithms and digitized fingerprints) can be taken more reliably and compared in real time against reference databases or watch-out lists.

### (B) In-Depth Focus on Known Concerns.

The all-source centers for intelligence analysis at the DHS and the CIA should mount overlapping efforts to analyze extensive information about people and groups that potentially pose real dangers to

the United States, whether they live in the United States or in foreign countries. The analysts should understand who they are: their goals, strategies, capabilities, networks of contacts and support, the context in which they operate, and their characteristic habits/patterns across the life cycle of operation—recruitment, intelligence and reconnaissance, target selection, logistics, and travel.

Linking together available information can yield rewards, but the analytic techniques must be used carefully to avoid mismatches and false identifications. We need to build the expertise, systems, and "middleware" that can draw out reasonably straightforward sets of connections from data that government agencies already collect. Here are some hypothetical examples:

> Illustration #1: Analysts could have asked how many holders of visas from certain countries had spent more than a month in Afghanistan and then correlated those people with others who have spent time in Afghanistan to see who shares addresses, phone numbers, credit cards, or bank accounts. Such searches can and should be done in ways that reveal only the identities of the matches.
>
> Illustration #2: Analysts could identify purchasers of airline tickets who have telephoned persons on a terrorist watch-out list during the past year.
>
> Illustration #3: Analysts checking applicants for visas to come to the United States could correlate dates of travel to Afghanistan or certain cities with the times of known terrorist activities in those places.
>
> Illustration #4: An example to avoid: Analysts put someone who just has the same last name as a known terrorist on a watch-out list.

In other words, linking of information should be based on criteria that are developed to balance security gains against the potential for overreaching and threatening liberties.

Existing law for the *collection* of information and intelligence in general permits very extensive analysis. If properly interpreted and defined by new guidelines that balance privacy and security, recommended later in this report, existing law may be sufficient for adequate information sharing among government agencies that will perform such analysis without intruding on essential liberties.

The DHS intelligence analysis center or the DCI's counterterrorist center do not need to accumulate and hold all relevant databases to which they may gain access. In other words, there is no need to build one big data warehouse. Instead, the centers should interface with such databases as needed.

Data mining can be a useful tool. But it is also a tool that invites concern about invasion of privacy. Extravagant claims have been made about the potential uses of data mining, matched by similarly extravagant notions of the vast private or public databases that should be opened to such journeys of exploration. Neither the real needs nor the real capabilities are so exotic. Though there are areas where more data may need to be collected, the immediate challenge is to make more effective use of the mountains of data that are already in government hands or publicly available. Data mining, like any other government data analysis, should occur where there is a focused and demonstrable need to know, balanced against the dangers to civil liberties. It should be purposeful and responsible.

### Linking Analysis to Protective Action: Using Watch-Out Lists

The first type of analysis we described was "wide scans to identify vulnerabilities." There we introduced the idea of specifying critical "gates" where officials can lawfully control access to especially dangerous means of attack. Airport security is a natural focal point, but others might include points of access to dangerous pathogens, transportation of extremely hazardous materials, or vulnerable points of access to the country's electronic networks.

We also just discussed a second type of analysis—an "in-depth focus on known concerns." That effort gathers and analyzes information on known concerns, like suspected terrorists. That information can contribute to lists of people wanted for arrest, for questioning, or just for surveillance of their movements.

To bring the two forms of analysis together in practice, governments can combine "gates" and "lists" for protective action. As officials try to notice and analyze the people who pass through certain kinds of "gates," the use of watch-out lists becomes critical. This tool can be exceptionally valuable, *if* it is used in a responsible and reliable way and focused on the terrorist danger.

To illustrate the power of such "gates" and access to quite modest forms of data, we examine the concrete case of the 9/11 hijackers in Illustration No. 2.

## Illustration No. 2: "Watch-Out Lists" and "Gates": A Hypothetical Application to the 9/11 Attacks*

*Hypothesis:* Each person buying an airplane ticket is checked against lists of possible terrorists. If there is a "hit," that person's available information is checked to identify possible associates.

- Software already exists that can check names and addresses against multiple databases. It is capable of accounting for errors and variations in the way names are spelled, and can perform these functions on very large databases in seconds.

*The Application:*

- In late August 2001 Nawaq Alhamzi and Khalid Al-Midhar bought tickets to fly on American Airlines Flight 77 (which was flown into the Pentagon). They bought the tickets using their real names. Both names were then on a State Department/INS watch list called TIPOFF. Both men were sought by the FBI and CIA as suspected terrorists, in part because they had been observed at a terrorist meeting in Malaysia.

- These two passenger names would have been exact matches when checked against the TIPOFF list. But that would only have been the first step. Further data checks could then have begun.

- Checking for common addresses (address information is widely available, including on the Internet), analysts would have discovered that Salem Al-Hazmi (who also bought a seat on American 77) used the same address as Nawaq Alhazmi. More importantly, they could have discovered that Mohamed Atta (American 11, North Tower of the World Trade Center) and Marwan Al-Shehhi (United 175, South Tower of the World Trade Center) used the same address as Khalid Al-Midhar.

- Checking for identical frequent flier numbers, analysts would have discovered that Majed Moqed (American 77) used the same number as Al-Midhar.

- With Mohamed Atta now also identified as a possible associate of the wanted terrorist, Al-Midhar, analysts could have added Atta's phone numbers (also publicly available information) to their checklist. By doing so they would have identified five other hijackers (Fayez Ahmed, Mohand Alshehri, Wail Alshehri, Waleed Alshehri, and Abdulaziz Alomari).

- With days still remaining before the scheduled flights, additional investigations could have turned up information about attendance at flight schools (information that the U.S. government then did not have in a digitally searchable form) or on puzzling foreign links (like common financial links to Hamburg, information that the government was not able to access in real time.)

- Closer to September 11, a further check of passenger lists against a more innocuous INS watch list (for expired visas) would have identified Ahmed Alghamdi. Through him, the same sort of relatively simple correlations could have led to identifying the remaining hijackers, who boarded United 93 (which crashed in Pennsylvania).

** Information for this illustration was drawn from work done by Systems Research & Development, one of the firms that has developed relevant software, in this case with the help of venture capital supplied by the CIA-sponsored firm, In-Q-Tel.*

In this hypothetical illustration, combining the "gate" with a virtual watch-out list works because two of the 9/11 hijackers were wanted as suspected terrorists and bought airplane tickets using their real names. Let us assume, then, that future terrorists use false names or otherwise attempt to conceal their identity. The individuals can still be identified, not by a name but instead with a biometric algorithm derived from a photograph of the face or the digital measurement of fingerprints.

Facial recognition and other biometric identifiers can be evaded or defeated, although it is difficult, especially when compared to the paper-based ID systems (driver's licenses and passports) now used in the United States. But evasion becomes far more difficult if the photograph or other identifiers are taken, and then checked, under controlled conditions by a human observer.

Hence the concept of the "gate" is important as a way of focusing the use of these potentially intrusive technologies and increasing their reliability. For example, if the visa applicant and the person passing through an airport security checkpoint are scanned, voluntarily, under controlled conditions, the technology is powerful.

If multiple biometric identifiers are used, such as both photos and fingerprints, as a check against false positives, the technology can be still more effective. The biometric identifiers can go into a government database when the information is originally acquired (when someone applies for a visa, or is arrested, or receives a driver's license, for instance), regardless of whether the biometric information is encoded on the visa document itself. If the information is in the database and then can be compared under controlled conditions with the actual individual, the suspect cannot beat the system just by switching or forging identity documents of the kind ordinarily used now.

Such checks are not foolproof. No system is. But it raises the bar significantly, adding more complications to enemy planning. As plans become more elaborate and difficult to carry out, the chances of mistake and exposure go up as well.

But with any such protective system the preparation of guidelines is essential. These guidelines must standardize the conditions under which the biometric data is gathered and compared by various agencies, and how any biometric identifier is issued, and regulate what actions will be taken if a person at a gate is a "match."

Various agencies of just the federal government currently maintain more than a dozen different kinds of watch-out lists. Each of these were created for different purposes. We do not recommend combining them into one vast list. But we do recommend the creation of "virtual" consolidated watch-out lists. The DHS should be able to pass names across the various lists to check for "hits," without actually building a data warehouse of its own.

Other agencies at all levels of government will want to perform such checks. The White House can take the lead in requiring all such lists to meet certain common, minimum standards—including interoperability and accessibility from one agency to another. Therefore we also recommend that:

- Guidelines and procedures are needed on what information will get a person on such a list, and off of it. It should not take months to get someone on a list. Nor should it take even longer, and a team of lawyers, to get someone removed from it.

- Guidelines are also needed on how such information or lists would be used in the field—whether for arrest, interviews, or simply for tracking location or movements. These databases should have common protocols for data entry and indexing, such as digital fingerprint and facial recognition algorithms. The DHS should develop these guidelines as a national service for various federal, state, and local agencies.

- Also, as a common national service, the DHS could be responsible for quality control, and thus also be accountable for operation of the system in compliance with the written guidelines. Frequent review will be needed. The use of such lists must be consistent with constitutional requirements (detailed in the background research paper on profiling and watch lists) and with the democratic ideals of our nation. Targeting citizens based solely on a single factor, like their race, or their gender, or their political or religious beliefs, should be expressly prohibited in the guidelines for operating these systems.

As illustrated in detail in our 9/11 hypothetical, the method can be reasonably straightforward. It can start with a search for specific individuals already wanted or otherwise known to government agencies—like the hijackers Al-Midhar and Alhazmi before 9/11. And, if such people are identified, it is then reasonable to try to identify any associates of those people, by checking for common addresses, phone numbers, and so on. Even in our other hypothetical illustrations we are still using relatively concrete correlations (travel to/from Afghanistan and dates of terrorist activity, etc.).

Employing watch-out lists without proper preparation of the kind we describe could be counterproductive, discrediting a valuable tool. As an example of such more ambitious worrisome "profiling" efforts, the new Transportation Security Administration (TSA) wants to check passenger lists against watch-out lists. But, even though it is not yet able to perform the simpler data analysis tasks recommended above, TSA is reportedly trying to develop a CAPPS II system for screening air travelers, in part by creating "profiles" of possible terrorists by analyzing behavioral characteristics of the general population. According to one report, by Robert O'Harrow in the September 4 *Washington Post:*

> Under the plan, passengers would be required, when making their reservations, to provide identifying information, such as a name, address, and driver's license, passport, Social Security and frequent-flier numbers. Those details would be used by private data services, such as ChoicePoint, Inc., an identification and verification company, to supply more information about the individual.
>
> TSA computers would then use artificial intelligence and other sophisticated software, along with behavior models developed by intelligence agencies, to determine whether the passenger is "rooted in the community"—whether he or she is well established in the United States—and find links to others who might be terrorists, according to government documents and interviews.

> The aim is to create an "automated system capable of integrating and simultaneously analyzing numerous databases from Government, industry and the private sector…which establishes a threat risk assessment on every air carrier passenger, airport and flight", according to a government document.

If the "TSA computers" step in to use "behavior models" to assess the general population, that would be profiling. Some federal officials have reportedly discouraged adoption of the simpler analytic approaches we recommend, fearing that adoption of such strategies will hinder acceptance of their more ambitious plans to "score" passengers for presumed riskiness.

All profiling is not inherently bad. But we are cautious about claims that "behavior models" of the kind postulated here can effectively identify possible terrorists in the general population. Such a profiling system would also need to consider the risk of false positives that could number in the tens of thousands when such searches for correlations are applied to pools of people numbering in the tens of millions. The quality control issues arising from bad underlying data are also compounded in such a system.

We recommend that, first, our governments as promptly as possible at least acquire the capability to do the simpler analytic tasks they still cannot perform. Using watch-out lists more effectively is imperative. We should see how well that works. Meanwhile these experimental behavioral explorations should be treated as research projects that need to be tested before they are tried out upon the vast community of American air travelers.

## Guidelines to Balance Privacy and Security

As we have suggested in the use of watch-out lists, guidelines must be set by the President so that all agencies come to share a common, minimum set of goals and standards. To succeed, the system must have the confidence of the American people it serves, while the analysts and operatives involved must feel confident that they know what they are expected and allowed to do, and that their work is lawful and appropriate.

The scope of domestic intelligence work should be defined. Specific guidelines are essential to guide intelligent analytic work, draw on the strengths of a national community, and provide a basis for training. Guidelines are also a key to assessing performance.

Guidelines also enable managers to embed respect for privacy and civil liberties into the core definitions of the analytic work itself. That too becomes a basis for training and developing routines, and for holding the officials accountable for compliance with the rules.

The Task Force formed an ad hoc working group on "Collection, Use, and Analysis" to develop a concrete framework illustrating the kinds of guidelines we recommend. That sample framework is presented as Illustration No. 3.

## Illustration No. 3: Guidelines for Database Access and Use*

Fighting terrorism requires new weapons. One weapon being used by the government is the increased use of public and private databases to prevent attacks. The analytic purposes of this work have not been well defined. In specified circumstances, these guidelines will require analysts to identify the types of databases involved, define the purpose of the data review, and clarify the authorization for collecting and disseminating whatever is found. Such considerations must be addressed before embarking on broad new uses of information resources. This is not just because of the privacy and constitutional interests at stake, but also to avoid fruitless searches for intriguing but essentially meaningless correlations.

Guidelines like those illustrated below seek to employ the capabilities of new technology to provide new protections for privacy—protections that will allow the effective use of information in the war against terrorism while respecting individuals' interests in the use of private information about themselves.

Existing guidelines are inadequate. Developed in the course of traditional, reactive law enforcement, they often require some degree of individualized suspicion and prior judicial approval before information can be accessed. This impedes the quick, effective use of existing databases to identify and prevent terrorist acts. Once the data has been lawfully gathered, however, existing approaches offer little or no privacy protection at all.

The following recommendations spell out some of the principles that will allow more effective use of information in the war against terrorism. Proceeding from the premise that security and privacy can coexist, these suggested new guidelines are a first step toward designing a system that will allow us to fight terrorism effectively and secure modern privacy protections for individuals.

**1. Importance of Access to Information in Public and Private Hands**

Access to information in the hands of public and private entities is an essential tool in the fight against terrorism. Government agencies responsible for combating terrorism—including state and local as well as federal authorities—should have timely and effective access to needed information, pursuant to appropriate legal standards. The legal constraints and exceptions provided by current laws are generally sufficient to allow a homeland security agency to gain necessary access to information held by other government agencies. These new guidelines offer a framework and procedures to allow that information to be effectively used, analyzed, and disseminated. At the same time, these guidelines are intended to ensure that information about people in the United States is used in a responsible fashion that respects reasonable claims to individual privacy.

**2. Purpose and Interpretation**

a. These guidelines should be interpreted and applied in a fashion that encourages rapid, effective, and responsible access to data that can assist in the task of identifying, thwarting, or punishing terrorists. These guidelines should also be interpreted and applied in a fashion that encourages respect for fundamental liberties, creativity, innovation, and initiative in the use of data for the purpose of fighting terrorism.
b. These guidelines should be used only for the gathering and analysis of information for intelligence in the war against terrorism. The procedures and authorities for using the legal process for obtaining information for law enforcement purposes should remain unchanged.

**3. Coordination and Authorization**

An intergovernmental body, chaired by the Secretary of the Department of Homeland Security and composed of representatives of the relevant federal, state, and local agencies, should be formed to coordinate the procurement and use of private as well as state and local databases containing information about United States citizens. Because databases have varying degrees of utility, privacy interest,

and reliability, the Task Force concluded that a single point of coordination would provide accountability for privacy concerns as well as allowing for the effective and efficient use of information. In addition, this intergovernmental body will provide a focal point for private companies and state and local administrators' concerns about burdensome, duplicative, and inconsistent requests for information.

Similarly, the authorization for procuring or requesting access to databases should not be burdensome on investigators and analysts. These guidelines envision a process in which a single authorization for the procurement of the database will be sufficient for all necessary and continuing access by agency personnel, if it is for the authorized use.

**4. Relevance**

Agency personnel should have access to and use information available under these principles only for purposes relevant to preventing, remedying, or punishing acts of terrorism.

**5. Accountability**

Agencies and their employees should be accountable for the ways in which they access and use information available under these guidelines. An agency should be able to identify how its uses of databases are relevant to preventing, remedying, or punishing acts of terrorism. While it would be plainly inconsistent with the purposes of these guidelines to require that an agency or employee explain the relevance of every query before gaining access to data, mechanisms such as database access records, audits, and spot checks, should be used to ensure that agencies move toward demonstrable compliance with this principle.

**6. Dissemination and Retention**

Information about American citizens should not be disseminated or retained by the collecting agency unless it is demonstrably relevant to the prevention of, or response to, an act of terrorism. Administrative rules, training procedures, and technology should be implemented to prevent the unauthorized disclosure of private personal information. An electronic audit trail in how information is used, and penalties for misuse, can reinforce these guidelines.

**7. Reliability of Information**

Agencies should strive to use the most accurate and reliable information available. Nevertheless, information used under these guidelines may include data of questionable or varying reliability. Where feasible, and to promote effective antiterrorist action, limitations on the reliability or accuracy of data should be made known to those using the data. In the event that an agency determines that information is materially inaccurate and that an individual is likely to be harmed by future use of that inaccurate information, reasonable efforts should be made, and a process put in place, to correct the inaccuracy or otherwise avoid harm to the individual concerned.

**8. Information Technology Tools**

To the extent consistent with the purpose of these guidelines, information technology tools should be developed and deployed to allow fast, easy, and effective implementation of the relevance, accountability, and reliability principles of these guidelines.

Consistent with a vigorous defense against terrorism, these guidelines envision tools that create audit trails of parties who carry out searches, that anonymize and minimize information to the greatest extent possible, and that prevent both the intentional and unintentional dissemination of irrelevant information to unauthorized persons or entities.

**9. Information in the Hands of Intermediaries**

a. Much of the information relevant to the fight against terrorism will be in private hands. As a general principle and where consistent with the purposes of these guidelines, it is preferable to leave information in the hands of private intermediaries rather than consolidating it into agency databases.
b. In many cases, an agency may be required to transfer information into an agency database because it does not have the tools needed to search privately held data effectively and quickly. Agencies are encouraged to develop and deploy tools that would allow such searches and thereby allow information to remain exclusively in private hands.
c. Private databases are not created for the government; they are created by private parties for their own commercial purposes and subject to the constraints of the marketplace. An agency seeking access to such databases should treat these intermediaries fairly. In particular, the agency should
    i. preserve necessary confidentiality and protect intermediaries from liability for any assistance they may provide to the agency in good faith; and
    ii. use commercial contracts or similar arrangements to compensate intermediaries for any assistance provided to the agency.
d. Agencies should initiate and maintain a cooperative dialogue with the private sector to develop voluntary data retention policies that maintain information necessary for the war on terrorism. Agencies should endeavor to identify critical information and advise private firms of the importance of their voluntary efforts to retain such data. If necessary the government may even encourage the formation of self-policing groups within the private sector to help achieve the data retention objectives. In other words, the more the government does to articulate specifically what information should be retained and why, the greater the obligation the private sector should feel to cooperate with these agency requests. In a narrowly defined set of circumstances, such as with airline passenger manifests and sales of certain biological pathogens, data retention may appropriately be required.

**10. Revisions and Public Comment**

a. These principles are preliminary steps toward establishing the fundamental authorities and protections for the use of information in thwarting terrorism. They should be reviewed, revised, and made more specific in the light of actual experience.
b. These guidelines and any future revisions and specific rules that are established based on the guidelines should be available to the public and subject to public comment, unless the President finds that disclosure will endanger classified intelligence collection or analytic methods and threaten the national security of the United States.

**11. Agency Implementation**

a. Compliance with these guidelines should be achieved to the greatest extent possible through training, advice, and quick correction of problems rather than through after-the-fact punitive measures that may lead antiterrorism agencies or employees into risk-averse behavior.
b. Investigations of suspected violations should be performed by a single office and should focus principally on systemic measures to avoid future violations.

**12. Congressional Oversight**

Nothing in these guidelines restricts review of the guidelines by Congress. Members of Congress or Congressional staff conducting reviews of the guidelines or their implementation should expressly agree to protect an individual's privacy, classified information, and confidential sources and methods used to combat terrorism.

**These guidelines were developed by a working group chaired by William Crowell and reflect particular contributions from Robert Atkinson, Stewart Baker, Jerry Berman, Ryan Coonerty, James Dempsey, Mary DeRosa, Esther Dyson, Daniel Ortiz, Jeffrey Smith, James Steinberg, and Michael Vatis.*

Although the new DHS can be a hub for development and accountability in using guidelines, they should apply to all responsible agencies. For this reason and to promote transparency and accountability, the guidelines should be promulgated in the form of public Executive Orders and—if necessary—classified National Security Presidential Directives issued directly by the President. They should supersede older, analogous documents that now are out of date.

The full range of information activities needed for new national security requirements will gain the confidence of the American people by being accountable to Congress. The Congress should concentrate these oversight responsibilities in *new* committees that can consolidate and focus oversight over the new Department.

- The oversight system can benefit from using the written guidelines that we have recommended be developed for the most sensitive activities that the DHS and other government agencies will conduct.

- Under the bills moving forward in Congress, the DHS will likely have at least an Inspector General and a Privacy Office, and possibly a Civil Rights and Civil Liberties Office as well. The Task Force endorses the goal, but the duties of these various internal overseers need to be clarified by combining the two offices into *one* well funded and staffed civil liberties and privacy office, and then spelling out the referral criteria for the agency's Inspector General.

- Since the DHS may have unusual duties thrust upon it, it needs effective mechanisms for oversight. The purpose of these mechanisms would be proactive, helping to guide officials on how to achieve what they need to do, as well as steering them away from what is out of bounds.

The domestic intelligence capabilities of the DHS must be managed as part of the intelligence community. That system is and should be overseen by the President and the interagency process organized under the National Security Council. This aspect of its duties should also involve the Director of Central Intelligence's role in managing the intelligence community, including the interagency boards operating to assist the DCI.

Within the NSC system, the highest-level resource planning for the intelligence community can be managed by reconstituting an interdepartmental Executive Committee for this purpose. It should include the DCI, the Secretary of Defense, the Secretary of Homeland Security, and the Attorney General, with the President's national security adviser serving as the executive secretary for this group.

The President could also adapt his Foreign Intelligence Advisory Board and its Intelligence Oversight Board to help him continue to oversee the intelligence community in all its activities, both foreign and domestic.


JOHN DOE N34079 - RETURN NAME MATCH
KNOWN ASSOCIATES : 3
HITS RETURNED : 3
RECORD VERIFIED : 09/19/02
KNOWN ASSOCIATES : 20
HITS RETURNED : 11
RECORD VERIFIED : 07/06/02
KNOWN ASSOCIATES : 9
HITS RETURNED : 0
RECORD VERIFIED : 10/01/02
KNOWN ASSOCIATES : 112
HITS RETURNED : 31
MATCH

## … And Training People to Do the Work

Pending legislation anticipates supplying needed expertise to the DHS by detailing employees from other government agencies. This may be inadequate. The needed skills are currently in short supply across the government.

The DHS, or at least its intelligence and information directorates, will need the flexibility to be able to hire certain key employees with needed skills. Another option is to allow the DHS to rely on staff they may be able to find in government-supported research centers.

Aside from the disadvantage of diverting scarce talent from other agencies, a number of the specific needed skills may not exist in adequate supply in the federal government at all. There is a particular shortage of people with both the needed analytical *and* data skills. At a minimum, significant investments in training will be needed, training oriented to the analytic methods and challenges described above and the networked, decentralized approach to using these methods.

In addition, the DHS and other agencies will need much better access to IT expertise in the private sector, a topic to which we now turn.

## Roles and Risks for the Private Sector

A large portion of the costs of homeland security, tens of billions of dollars, are already being borne by the private sector. The strategies currently contemplated to enhance our homeland security are likely to generate even greater costs. An overbroad and rigid approach to homeland security will make that worse, creating severe economic burdens for the country, and eroding historical strengths of the American workforce such as its members' mobility, speed, diversity, and willingness to think for themselves.

But if systems are designed effectively, they can enhance security and cut costs. Expensive and time-consuming paper- and person-based processes can be replaced with processes that take advantage of information technology. Information is also the key for how government regulators can avoid unnecessarily disruptive strategies. Properly analyzed information and intelligence can yield powerful insights about which policy interventions are likely to be cost-effective and which are not.

The government will need access to public and private sector data for national security. The DHS should develop innovative service-delivery models for using information held within and outside of the government (on trade or specific cargo, for example) and guidelines on the circumstances and procedures for purchasing or requesting access to such data.

## Exploiting America's IT Advantage

While government agencies have been instructed or have attempted to acquire and use more advanced IT, progress has been slow. Widespread inadequacies still exist in the full range of IT related issues, relative to technology or methods used in the private sector.

Many reasons have been identified for the inadequate use of IT by government in the United States, including: excessively restrictive procurement rules; bureaucratic resistance; inadequate skills and knowledge by government personnel; ineffective, top-down planning for IT improvements instead of user-based perspectives; inadequate and inconsistent support by Congress and state legislatures of IT investments, especially for interagency cooperation; unwillingness of private sector experts to join or work with government due to perceived rigidity, absence of protection of intellectual property, potential liabilities, and by the failure of some large IT projects and vendors to deliver the promised results.

Consolidation of agencies or departments along functional lines is potentially helpful in enhancing efficiency. But to contribute to IT improvements, consolidation must add the new capacities needed to overcome barriers that have led to failures to use existing IT or to develop needed capacities.

In a Fiscal Year 2003 budget request of more than $38 billion, the information management and integration task received a share of about $200 million. Congressional appropriators have cut back even that very modest request. The Information Integration Office proposed by the President has been zeroed out. This was an unfortunate decision because investments in the proper use of information can make all the rest of the spending more productive.

But now a National Strategy for Homeland Security has been announced. A new Department of Homeland Security is being created. The best reason to create this Department is to create entirely new capacities for government action, above all in the area of information.

Information and information processing is to homeland security as the brain is to the human body. Once a convincing information strategy is in place, the President and Congress should allocate the resources to make it work.

A particular problem is the need for resources for activities that cut across agencies, specifically individual agency budgets. The DHS can be a focal point for appropriations that can benefit the entire country, horizontally across the federal government and vertically in supporting networked national operations.

Adequate resources are also essential to create positive incentives for interagency cooperation, rather than relying on White House (OMB) coercion.

Finally, adequate resources are critical to a robust research and development program, if that program is designed to take full advantage of the best practices that have been developed in the private sector. Some specific suggestions follow.

Procurement rigidities and an NIH (Not Invented Here) culture are frequently noted as a major problem in technology acquisition by government. Improvements can be made in the procurement process, but this is not the principal problem. Ways to overcome traditional difficulties are being developed and used. Several helpful ones are likely to be included in the homeland security legislation.

Among these are the following:

- Government entities should have the flexibility to engage in "Other Transactions," as has been authorized for the Department of Defense when acquiring IT for national security purposes. These contracts enable agencies to enter into joint ventures, to extend intellectual property protections to companies doing business with the government, and to engage in other exceptional arrangements. This authority should not be limited to a five-year period.

- Agencies involved with national security IT issues should be able to procure personal services of a limited set of experts without regard to the usual civil service limitations. This authority exists in draft legislation for the DHS, but the power to hire should not be limited to periods of less than a year.

- Agencies should also be given the broad authority to procure essential items and services for homeland security and, when appropriate, to waive normally applicable rules. This is also likely to be included in the DHS' powers, and most limitations and reviews should be eliminated.

- Congress should avoid creating funding inconsistencies and disincentives for IT necessary for national security. Congress has been too prone to give IT expenditures a low priority, and has refused thus far to support IT expenditures that are intended for multi-agency projects in part because its appropriations process does not support interagency acquisitions. This must change.

- Congress should support the training of a corps of IT acquisition specialists for assignment to each of the agencies needing sophisticated procurement advice. Current personnel are unable to utilize the flexibility that exists in the Federal Acquisition Regulation (FAR).

- To fully utilize its IT edge, the United States must find ways to tap existing capacities, to secure private sector support, and to provide government support for particularly promising projects. Recruitment of experts from the private sector, and training of existing personnel, have led to improved IT utilization, but in a slow, inconsistent, and unreliable manner. Research and development in IT within government has also been insufficiently productive. We support the proposal of the National Academy of Sciences' committee on technology and terrorism to create an Institute or similar institution to provide a vehicle by which government can derive advice and assistance on a range of issues from private sector experts. This non-governmental entity should not attempt to duplicate R&D functions already being provided by DARPA, the National Science Foundation, and existing national laboratories.

For a specific outline of how this Institute might work, see Illustration No. 4.

## Illustration No. 4: A Research Institute for Homeland Security

The Institute should be available to the DHS Secretary and to other federal, state, and local agencies to assist on IT issues, and should be authorized by Congress to perform at least the following functions:

- Provide guidance in all its IT activities based on a customer orientation that maximizes operational effectiveness;
- Assist the DHS and its component agencies in developing their IT enterprise architecture;
- Provide solutions transfer support for all DHS agencies as well as other federal, state, and local entities, as necessary;
- Assist in developing protocols (but not rigid standards) for meta-data (interagency interface), data entry, security, and storage;
- Ensure that necessary testing is conducted to certify products from private vendors as meeting protocols;
- Establish a committee to screen proposals for research, development, or purchase of IT products from private sector companies;
- Provide advice and assistance to state and local governments and entities with regard to IT related issues;
- Assist through a committee designated for this purpose in recruitment of IT specialists, as well as in placing them with government agencies;
- Assist Chief Information Officers of federal, state, and local agencies in developing IT related plans for homeland security, and in certifying such plans as meeting relevant protocols and IT requirements;
- Establish and operate an IT clearinghouse for public and private exchange by IT experts and users of needs, capabilities, and experiences;
- Provide advice and assistance in developing methods for enhancing international cooperation and interface; and
- Engage with DARPA or other R&D entities in specific IT development initiatives designed to provide substantial and project-based federal government support to work with private firms in developing IT technologies or capacities that are recognized as urgently needed for national security purposes. Special efforts of this sort, such as the Manhattan Project and the Y2K initiative, successfully focused national resources in a highly productive way.

Examples of such projects include the creation and deployment of operative, consolidated watchout lists; or designing a nationwide, Emergency Response Network on the Internet.

In addition, an entity should be created within the DHS to assist the Secretary and agency CIOs in providing effective IT training, planning, and implementation. This DHS entity should have the capacity, continuity, and authority to help satisfy the functional needs required to overcome recognized deficiencies that have resulted in inadequate IT exploitation.

- This DHS IT Center should be provided with multi-year budgetary support, including in particular funds to be used for interagency IT activities and for monetary awards to DHS agencies or departments that perform effectively in adopting IT recommendations. The Center should be required to review all IT infrastructure proposals made by or on behalf of any DHS entity, and to certify such proposals to Congress as warranting legislative support.

Finally, the DHS should join the CIA as a major sponsor and client of In-Q-Tel, using that firm as an effective, working vehicle that can tap cutting-edge expertise about new IT developments and help convert these ideas into usable, deployable products that can make America safer and freer.

Current drafts of legislation to create the DHS include the creation of entities that satisfy some of these requirements. But the entities created must provide roles for private sector experts that are assured, and not dependent on the discretion of the DHS Secretary or other government officials. In addition, these entities should be given functions and authorities that go well beyond those of a conventional federal advisory committee.

# Part Two: WORKING GROUP ANALYSES

# Report of the Working Group on Analytic Methods

*This Working Group was chaired by James B. Steinberg, who drafted this report on behalf of the group. Participants in this group were John Arquilla, Bruce Berkowitz, Anne-Marie Bruen, Ashton Carter, William Crowell, Sidney Drell, Stanley Feder, Andrew Frank, John Gage, Lauren Hall, Margaret Hamburg, Tara Lemmey, Michael Mazarr, Douglas McDonald, James Morris, Alan Schwartz, Jeffrey Smith, Stefaan Verhulst, and Philip Zelikow, with assistance from Mary McKinley and Laura Rozen.*

Working Group I was tasked with examining the information requirements and analytic methods needed to meet the challenge of new security threats, particularly threats to the homeland.

## The Nature of the Challenge

The information/intelligence challenge of today's new security threats is dramatically different from the Cold War security problem. During the Cold War, the United States had an information collection method that was highly focused; a known target; rich detail on the adversary's capabilities; collection technology designed specifically for well defined objectives (*e.g.* satellites to access denied areas); highly trained analysts with long experience and high degree of specialization in each aspect of the adversary's capabilities and methods; and a well-defined set of indicators and warnings. In short, we had a reasonably high degree of confidence of what to look for, and why it was important (at least on the military threat side). By contrast, today in the context of terrorism and unconventional threats, the adversary is poorly known and understood, potentially diffuse in geography, and small in numbers. What's more, our collection tools are limited (difficulty of human intelligence access, successful denial strategies against signals and imagery intelligence, etc.); we have few well trained and experienced analysts; and generally, we lack well recognizable indicators and warnings.

The Working Group therefore focused on how to develop an information strategy to address these challenges/deficiencies. Four core concepts emerged from our discussions.

1. We need to better understand our adversary—its membership, methods, capabilities, intentions—what we call the threat-based, or "focused," dimension of strategic analysis.

2. Because our knowledge of even known adversaries is likely to be limited, and because some threats will emerge from previously unidentified sources, we also need an information collection and analysis strategy that will allow us to detect and prevent dangers from these unanticipated sources (vulnerability analysis, which includes both targets and means of attack).

3. Given the diffuse and dynamic nature of the threat, a broad range of information may be relevant to identifying the threat, and an equally broad range of sources may have relevant information. It will be difficult to specify *a priori* who may have relevant information. Therefore, there is an especially critical need to break down the compartmentalization of collection and analysis to allow the formation of constantly reforming virtual communities of analysis and connect them to users in at the international, federal, state, and local levels, as well as to the private sector. At the same time, the information and analysis system must remain sensitive to security of information concerns.

4. Because this form of analysis is heavily dependent on large volumes of data (to detect patterns and to make correlations) assuring the quality of data is critical.

## Strategic Analysis: "What" We Want to Know—Threat and Vulnerability Analyses

### Threat-based analysis: "Know thy enemy"

This dimension of strategic analysis centers on a focused, in-depth concentration on known threats. It is similar in kind to the analysis used against traditional state adversaries, but is adapted to take into account some of the peculiar characteristics of the non-state, non-hierarchical (or network) threat posed by terrorism. As in the traditional analysis, we are interested in knowing about the adversary's goals/motivation, strategy, and capabilities (order of battle/membership, technical capabilities). But we must adapt how we learn these things. Considerable stress has been placed on improving HUMINT as the best (and in many cases only) way of learning these kinds of facts directly. But given the nature of these groups, there will be practical limits to the development of human sources, irrespective of the level of resources devoted to them. Therefore, other tools must be developed, including the following:

> **network analysis**—drawing on the literature and tools of mathematics and physics, as well as social sciences, including group dynamics of like-minded individuals, and the properties of horizontal networks with many nodes; and
>
> **contextual analysis**—drawing on history, culture, etc.; and allows in-depth knowledge to help reveal key indicators (the example of the "Afghan" connection of many al Qaeda members) that can be linked to pattern analysis (travel, financial flows).

The threat-based analysis should pay particular attention to the life cycle of attack planning and execution, because the information to be acquired will change dramatically in each phase. The life cycle is as follows:

1. target selection and planning
2. recruitment
3. intelligence and reconnaissance
4. logistics
5. strike

Gaining information on early stages is particularly important for the disruption and denial function.

### Vulnerability analysis: "Discover thy enemy"

The danger of an in-depth, or threat, focus is that we will lose peripheral vision, and thus be highly vulnerable to surprise. This is particularly worrisome in the context of terrorism, because the adversary is highly adaptable, and because the means of causing serious harm are more widely available at relatively low cost and are employable by small groups or even individuals. No intelligence system will be perfect, but we have an especially high priority not to miss potential attacks

that will have large-scale impact. Thus we need to complement our threat-based analysis of known threats with crosscutting strategies that will reduce our vulnerability to "big" surprises.[1]

This dimension of strategic analysis focuses on "vulnerabilities," in two aspects—the vulnerability of targets and the vulnerability of means (that is, the ability of adversaries to acquire and use dangerous materials—biological, chemical, radiological, nuclear or conventional). Since there is an almost infinite number of targets and a broad array of materials that could be used as weapons, this dimension of analysis will require prioritization.[2] There are a number of ways to approach the problem of prioritization, including ordinal ranking of potential targets based on the magnitude of the consequences of a successful attack; focusing[3] on "priority check points and portals;"[4] and the development of templates that provide illustrative schema of attacks for planning both information collection and preventive measures.[5] Tools for this form of analysis include:

**Scenario analysis**—including modeling terrorist plans through tools such as Hierarchical Holographic Modeling and other risk management techniques,[6] Project Planning Paradigm[7] and techniques such as red-teaming. Templates and scenarios should be the product of both "top down" approaches (experts from relevant agencies developing scenarios based on their own expertise and experience) and "bottom up"—the acquisition of new data prompting the development of scenarios or templates to "explain" the data. Large scale computer generated scenarios could prove particular useful in connection with bottom up analysis triggered by data mining, as correlations derived from *data mining* could be cross-checked against computer generated scenarios which in turn could suggest additional data gathering priorities which in turn could either validate or refute the scenario.[8]

**Means analysis,** of what is necessary—in terms of personnel, expertise, material, access—to carry out an attack and how might each be acquired and deployed.

**Counter-surveillance**—what kind of information is the adversary trying to acquire.

**Vulnerability surveys of key sites and networks**—with particular attention to second and third order effects, such as the impact of a port attack on shipping commerce.

## Technologies

Both threat and vulnerability analysis may lead to different technological requirements, such as transferable "expert" systems to allow additional analysts to read in quickly for threat-based analysis, and advanced search and data mining for vulnerability analysis. For the most part, technologies can be adapted from civilian use, although in some cases, the unique needs and lack of a civilian market may require direct government support for R&D.

Considerable information that will be valuable to analysis now resides in the private sector. It will be important for government to gain access to needed data, but in a way that is sensitive to civil liberties concerns and the business interests of private sector holders. By developing guidelines governing access, acquisition, and use of private sector data for analysis, the twin goals of enhancing

security and preserving core liberties are best assured. And greater government access to private databases should be accompanied by greater private sector protections on information not related to legitimate government security related requirements. This will give citizens greater confidence that providing accurate information will not lead to broad intrusions on privacy.

## Architecture of Analysis

### How Do We Use the Information We Collect?

**1. Building virtual analytic communities**

Under the traditional threat paradigm, the intelligence/analytic community was a highly formal organization, with a fixed set of collection assets, analytic specialists, and a well-defined user community (largely the military and foreign policy/diplomatic community). Information was highly compartmentalized with fixed channels through which it flowed (largely vertically up through the intelligence channels until "finished" then laterally to users).

Because of the diverse, constantly adapting, and furtive nature of the new security threats, "hard-wiring" the analytic and user communities is not only difficult, but also counterproductive. Relevant information comes from a much wider range of sources (dedicated intelligence collectors, users themselves, state and local officials and the private sector), and it is difficult to know *a priori* what information will prove relevant to analysts or useful to users. For this reason, it is necessary to create a more horizontal, cooperative, and fluid process for intelligence collection, sharing and analysis. A good example is the virtual chat room used by the U.S military in the Afghanistan war, when the full range of actors and information (from sensor data, to imagery analysts, to experts on Afghanistan to fighter pilots) could interact in real time with access to the same data. New teleconferencing technologies may make it possible to engage in even more sophisticated community creation.

Key required features of this virtual community include the following:

- relatively open access (reduction or elimination of pre-clearance, need-to-know barriers) to the information base assuming basic levels of security clearance for trustworthiness;

- accessible platform/portals available to all potential users (modeled, perhaps, on DoD's SIPRNET)[9]; and

- common cross-community technical standards drawn, if at all possible, from existing technologies and protocols. These should include the following:

    1. communication standards including TCP/IP;

    2. compatible databases (or alternatively, meta indexing or directory systems that can draw on existing but noncompatible technologies) that allow for sharing and integrated analysis; and

    3. data protocols that facilitate sharing while protecting especially sensitive information, such as sources and methods.

An important virtue of such an arrangement is that it avoids "turf" problems, since no single agency would own the process. But it would create a new opportunity for the standard-setting agency to leverage the ways that individual agencies operate to facilitate synergies among agencies.

### 2. Accountability

Although the virtual community has the advantage of empowering a broader community to contribute information, expertise, and perspective, by itself—given the horizontal nature of the network—there is a risk that no actor will be responsible for harnessing the power of the framework. Therefore, the network structure must be augmented by arrangements that ensure the following: 1.) that information in fact flows to all who need it; and 2.) that information is provided to decisionmakers and policymakers with responsibility and authority to act, who are ultimately accountable to the public for the performance of the system.

### 3. Linking Information Collection, Analysis, and Users

As noted above, in the new security threat environment, the line between collectors, analysts, and users is increasingly blurred. In addition, the relevant community of collectors, analysts and users extends beyond the federal government to include state and local governments and the private sector. This means strategies will be necessary to facilitate connectivity of information flows across intergovernmental and public/private lines in both directions. These strategies include the following:

- providing appropriate technology to state and local governments and the private sector to allow them both to provide and to receive information in a timely manner;

- eliminating barriers to information flows across the public/private boundary (including, where appropriate, liability rules, FOIA, Privacy Act, and antitrust limitations);

- facilitating coordination at the local level (integrated task forces), connected in a two-way flow to federal authorities, and convened by a representative of the DHS; and

- increasing ongoing interaction with users/policymakers to sensitize them to the analytic challenges and to provide the analytic community with a more operational sense of how information/analysis will be used.

### 4. Attracting Expertise

A common critique of existing efforts is the lack of expertise in the government's analytic community—be it language, regional/cultural experience or scientific and technological expertise. While it is possible to increase the capabilities of the federal government through greater resources and incentives, the virtual community model provides a way of tapping into expertise beyond the federal work force, and a way to continuously adapt the mix of skills as the environment evolves. For the federal intelligence/analytic work force, particular emphasis needs to be placed on developing the analytic and data skills that can take advantage of new information-based technologies.

### 5. Data Quality

Both the threat and vulnerability analytic frameworks depend heavily on data collection and management tools. But these are only as useful as the quality of the data collected in the first place. Thus special emphasis needs to be placed on the quality of the "first tier"—data input. This means well designed protocols that are both useful and realistic given the nature of the collector (for example, not expecting highly detailed syndrome data to be collected and reported by emergency room physicians).

Data quality also has significant civil liberties implications, so procedures need to be devised to assure high degrees of accuracy without compromising security (*e.g.,* giving potential terrorists access to their records in the name of assuring accuracy). There is also the related privacy concern with respect to mega-databases. There is a clear tradeoff between protecting privacy through limits on who can access databases and maintaining the open nature of the virtual community as described above.

## Recommendations

The imminent creation of a new Department of Homeland Security provides a unique opportunity to implement the concepts identified in this Report. Under the administration's proposal, the new Department is charged with both threat and vulnerability assessment. In addition, the Department will have broad-ranging responsibilities for key parts of the user community, including border and transportation security, emergency response (with ties to state and local governments), and infrastructure protection (thus with important ties to the private sector).

An urgent task of this new Department should be to take the lead in setting in motion both the substantive strategic analyses and the creation of the virtual analytic community described above. Although the Department will "own" key elements of this community, it is critical that the Department itself not "own" the process, since fundamental elements of collection, analysis, and use (such as the CIA, FBI, Treasury, HHS/CDC, etc., not to mention state and local governments and the private sector) will remain outside the Department, no matter what form it finally takes.

The creation of this virtual community and the implementation of new forms of strategic analysis will not happen overnight. We need a sense of time scale—what can and must be done immediately, and what can be phased in over time.

In the short term, the new all-source analytic unit at the DHS could immediately implement the strategic analysis strategies identified above in Section A since both provide a framework for the Departments assigned mission.

With respect to creating the virtual community, this could be phased in over time. As an interim measure the Department could do the following:

- establish an inventory of all relevant collectors, analysts and users;
- establish an inventory of databases and data repositories;
- identify technical and operational ("work around") bridges between key elements to facilitate communication during the period in which individual users continue to use non-compatible systems;
- establish local task forces that would include all key actors from the federal, state and local governments and the private sector to facilitate local real and virtual communities;
- review barriers to information flow between the public and private sector, and either act through Executive Order or propose legislation to make necessary modification; and
- convene an ongoing private sector advisory group to facilitate adoption of advanced IT technologies and strategies into the Department's analytic work.

Meanwhile, on a more long-term time scale, the Department should begin to establish the infrastructure that would make possible an integrated virtual community. This would include the following:

- identifying a common information platform for the virtual community with procedures that provide for basic security of access while assuring that all classes of potential participants will have access;
- establishing database and information-sharing standards to be used by all would-be participants in the virtual community;
- providing technical standards and funding that would support connectivity for state and local users; and
- identifying personnel and skill needs, and developing recruiting and training strategies to enhance analytic capabilities at all levels.

## Endnotes

[1] This approach thus helps break the straitjacket imposed by the concept of limiting planning to "validated" threats (an approach which drives much military planning) since by definition, surprises are unlikely to present the kind of evidentiary predicate that would "validate" a threat. In this sense, the approach here bears some similarity to Secretary Rumsfeld's suggestion of a "capabilities" based approach to military planning.

[2] The Working Group identified, but did not try to resolve, the difficult question of the impact of large numbers of small attacks (*e.g.* individual suicide bombers using crude conventional explosives), and the difficulty of using horizontal analysis of this kind to detect and thwart such attacks.

[3] This approach is developed in O'Hanlon et al. *Protecting the American Homeland,* Brookings 2002.

[4] The idea is to focus information collection on individuals who seek access to key sites or materials, for the purpose of pattern and anomaly recognition, and also for use against reference database(s), either compiled from information previously collected at the priority checkpoints (*e.g.* individuals repeatedly trying to access a sensitive computer site), or from other sources (such as a watch list developed by threat-based analysis of a terrorist organization).

[5] An illustrative example of such a template would be an attack on the U.S. electrical grid. The development of such a template would guide various aspects of intelligence collection (*e.g.* surveillance of critical transformers and cyber-infrastructure such as control devices associated with the operation of grids, counter-surveillance on websites that

provide information on the electrical grid) and point to remedial measures (*e.g.* elimination of single node failure points, enhanced security at key nodes, etc.).

[6] See Horowitz, Barry M. and Yacov Haimes, "*Risk Based Methodology for Scenario Tracking for Terrorism: A Possible New Approach for Intelligence Collection and Analysis,*" unpublished paper from the Center for Risk Management of Engineering Systems, University of Virginia, July 22, 2002.

[7] See, *e.g. Defense Science Board Task Force on Intelligence Needs for Homeland Defense,* Office of the Undersecretary of Defense for Acquisition, Technology and Logistics, Washington, D.C., January 2002, pp. 21-22.

[8] For example, data mining across two databases (workers in pharmaceutical research laboratories and airline ticket purchasers) might reveal that an individual who worked in a sensitive lab also bought a round-trip ticket to Kabul. This correlation would match with a scenario (man- or computer-made) of creating a manmade pathogen for a bioterror attack.) This might lead to a further database search of previous work histories of researchers in the lab—which might reveal that the individual in question graduated from Jihad U (thus reinforcing the probability of the scenario), or alternatively, that she was on secondment from WHO doing research on diseases of the Afghan highlands (and therefore tending to discount the probability of the scenario). The advantage of computer-generated scenarios is that very large numbers could be created without the unintended constraints of human definitions of "likely" or "plausible", thus decreasing the chances of surprise through novelty.

[9] SIPRNET (SECRET Internet Protocol Router Network) is a dedicated DoD wide data transmission network at the "secret" level, which provides for a degree of security since clearances and authentication are required, but without the constraints of higher level, compartmented information. An alternative might be the creation of a secure virtual private network that rides on the open internet.

# Report of the Working Group on Acquiring Information-Related Technology

*This Working Group was chaired by Abraham D. Sofaer, who drafted this report on behalf of the group. Participants in this group were Robert Atkinson, James Barksdale, Jennifer Barrett, Eric Benhamou, Bruce Berkowitz, Wayne Clough, Esther Dyson, Dave Farber, Slade Gorton, Tara Lemmey, Gilman Louie, Judith Miller, Harvey Nathan, Michael Turner, Michael Vatis, Gayle von Eckartsberg, Rick White, and Philip Zelikow, with assistance from Mary McKinley.*

## Acquiring Information-Related Technology to Combat Terrorism

### I. The Need for Advanced Technologies

The U.S. effort to prevent and respond effectively to terrorist acts depends on using advanced technologies. President Bush's call for a Department of Homeland Security (DHS), and the National Strategy for Homeland Security, issued on July 16, 2002, are designed in part to enable the nation to take full advantage of its technological edge. The National Strategy recognizes that "the nation's advantage in science and technology is a key to securing the homeland," and it calls for a "systematic national effort" to deploy "new technologies for analysis, information sharing, detection of attacks, and countering chemical, biological, radiological, and nuclear weapons."

Advanced technologies can help attain many potential improvements in the nation's capacity to prevent and respond to terrorism. Some commonly cited information-related areas in need of improvement are as follows:

- data collection, integration, and mining
- data analysis for management and risk control (reference databases)
- sharing of information across multiple databases (watch lists)
- secure communications networking for real-time crisis management
- systems for identifying and responding to conventional, chemical, biological, and nuclear threats
- systems for enhancing personal security controls through identity recognition and access management
- systems for enhancing physical security controls of vehicles and cargo
- enhanced, secure, wireless point-to-point communications

Almost all of these requirements have been recognized for years, by Congress, presidents, OMB, GAO, national laboratories, and private entities. Yet, repeated calls for enhanced use by federal agencies of advanced technologies have largely been ineffective, and the United States remains remarkably ill equipped to handle the challenges that homeland security presents.[1] The National

Strategy recognizes this, and rests on the premise that the U.S. government's widespread failure to adopt necessary and even mandated technological innovations would be overcome once most homeland security functions are consolidated into one department. It states the following:

> To date, research and development activities in support of homeland security have been underfunded, evolutionary, short-term in nature, fragmented across too many departments, and heavily reliant on spin-offs from the national security and medical sectors. Many of the involved agencies have little frontline knowledge of homeland security and little or no experience in technology acquisition and supporting research. The new Department would be responsible for overcoming these shortfalls by ensuring the pursuit of research and development activities where none existed previously.

Merely stating that the new Department would be "responsible for overcoming these shortfalls" will not enable it to do any better than its preexisting, component agencies have done. Consolidating agencies involved in homeland security will not ensure the development of new capabilities, functions, and techniques.[2] What Task Force member Ashton B. Carter has said about consolidating agencies into the DHS applies equally to the proposed consolidation of technology acquisition programs: "DHS should not just bring order to existing functions, but should accomplish new functions, especially development and practice of new types of 'intelligence' and new technology and techniques for homeland security."[3] To make a difference, the new agency formed to regulate homeland security must actually deploy those technologies best suited to make the nation secure. That will be achieved, not by consolidation alone, but by overcoming the barriers that have thus far interfered with or prevented achieving this goal.

## II. Barriers to Utilizing Necessary Technologies

What are the barriers that have prevented the U.S. government from utilizing the best possible information-related technologies? Among the difficulties and inefficiencies in the government procurement process that have long been recognized are the following:

- inadequate acquisition planning
- complexity and rigidity of procurement processes
- security classification issues
- existence of legacy systems
- unresponsive regulatory environment
- liability and intellectual property issues for the private sector

This formidable set of problems is exacerbated in connection with cutting-edge information-related technologies. Government agencies have talented scientists and managers, and some exceptionally capable technology centers.[4] But government agencies typically lack personnel with the expertise to understand, conceptualize, and formulate solutions for their information needs.[5] They are also often unaware of potential solutions that exist in the private sector for their information management problems. Knowledgeable private sector contractors widely view government officials as incapable of even understanding their technological needs, and as unwilling to risk taking positions

when difficult choices need to be made. Those agencies that have acted have often attempted to adopt comprehensive solutions that take years to implement and tend to be outdated before they are fully in place. Agencies have failed to plan their information strategies based on their missions, and they lack the ability to develop information infrastructure plans,[6] without which no amount of effort can produce acceptable results .[7]

Understandably, agencies have reached out to information experts for assistance in overcoming these difficulties. Private companies are currently doing a very substantial portion of the IT work of federal, state, and local governments,[8] and federally funded research and development centers (FFRDCs) are doing much of the research and development.[9] Delegating complex, mechanical tasks has proved helpful, and the FFRDCs are more productive than government centers would be. But hiring outsiders to come into agencies and craft solutions for the fundamental problems that cause inadequate utilization of information and other technology has proved ineffective. Outsiders, no matter how expert, and even if given broad authority as chief information officers (CIOs), are often unaware of the operational details of the working levels of their agencies. Affected workers, who are seldom included in developing these solutions, often view such efforts with suspicion and skepticism. Experience has demonstrated that the "top-down" solutions outside experts have typically provided are unsuited for identifying and satisfying information needs in an operationally effective manner. Outsiders, frustrated by the problems their reform efforts generate, frequently leave their posts well before completing the programs for which they have been retained.

Problems in the private sector also help explain the failure of government to satisfy its information-related technology needs. First, many of the technological capacities needed by government agencies to deal with terrorist threats have not been developed. In general, moreover, the ability to develop these technologies exists largely in the private sector, where funding has recently become difficult to secure from private sources. A real need currently exists for "seed" capital from government. The smaller companies most likely to produce elements of necessary advances are, in addition, poorly equipped to deal with the government's conventional procurement rules and procedures. These companies are also in general unable to develop usable systems for deployment; their contributions must be coordinated and consolidated with other technologies into products or solutions by groups able to work with both private sector contributors and government customers.

The need for reforms in government procurement to overcome these barriers is widely recognized. Studies routinely call for legal reforms and the removal of bureaucratic obstacles.[10] Some legal and regulatory adjustments are, in fact, necessary for effective reform. But the need for formal changes in procurement rules is overstated. Established devices already being utilized in existing agencies have greatly alleviated difficulties traditionally associated with procurement. The most significant of these are included in the Administration's proposed legislation to create the DHS, and Congress seems prepared to adopt those provisions (and perhaps others) on at least a trial basis.

Ad hoc reform of existing procurement rules will not suffice, however, to ensure that any new homeland security agency is structured and empowered to achieve government-wide, mission-oriented planning, development, and deployment of the best information technologies. Actual deployment of advanced technologies can only be achieved by building into the new DHS capacities and mandates designed to provide needed expertise and to overcome practices and "cultural"

realities that currently prevent effective technology utilization. This will require, as both the President and Congress recognize, new entities within and outside the new Department that are assigned new activities, and that involve and exploit private sector resources in new and more productive ways. The public/private mix must be changed far more radically than is presently planned. The analytic, planning, research, testing, and development processes must be opened up to a far broader spectrum of non-governmental players than is currently the case, and the standard for adequate performance must be raised dramatically. In addition, when it becomes clear that the deployment of certain technologies is essential to homeland security, Congress and the Administration should demand more than business as usual from the DHS and other responsible agencies. They should require the DHS to institute special projects to focus on and achieve the rapid and effective development and deployment of exceptionally necessary technologies and capacities, and should provide the institutional arrangements and funds required for such projects.

## III. Ensuring Government Deployment of Necessary Technologies

### A. Improving Procurement Procedures

Commissions and Congress have repeatedly examined government procurement activities, and numerous reforms have been implemented to enhance efficiency and provide flexibility.[11] The draft Homeland Security Act of 2002 incorporates powers developed in response to the need for flexible procurement laws. Thus, Section 732(a) of the proposed law would authorize the Secretary of the new Department to utilize the authority granted to the Secretary of Defense under 10 USC, Section 2371 to engage in "transactions other than contracts, grants, and cooperative agreements" when carrying out "basic, applied, and advanced research and development projects."`[12] This power to engage in "Other Transactions" (OT) would add considerably to the new Department's potential effectiveness in fulfilling its purposes.[13] In particular it would enable the DHS to form joint ventures with private companies, and to accommodate the strong desire of companies with valuable intellectual property assets (or aspirations) to retain the power to exploit their discoveries while licensing to the government. These devices will, in turn, enhance the government's capacity to raise private sector funds for projects intended to serve public sector needs and to help in encouraging high-tech companies, entrepreneurs, and technicians to work for or with government under conventional employment or procurement strictures.[14] This authority should not be limited to five years, as bills adopted by the House and Senate provide.

The proposed legislation includes two other significant authorities. Section 732(b) would allow the Secretary to procure "personal services, including the services of experts and consultants (or organizations thereof)" without regard to the limitations in 5 USC Section 3109 that such services be obtained by direct hire under competitive appointment or other procedures under civil service laws. This provision will enable the Secretary to create employer-employee relationships with experts whose services could not readily be secured under civil service requirements. It should not be limited to periods of employment of one year, as Congress presently seems willing to allow.[15] Specific efforts should be required to train individuals to become experts in the application of the Federal Acquisition Regulations, which control procurement. The regulations have significant flexibility, but they are extremely complicated, and only individuals who know and can apply them competently are able to take advantage of the flexibility provided.

Section 732(c) would add the DHS to the list of agencies in Section 602 of the Act of June 30, 1949 (40 USC 474) that are empowered to avoid the application of any procurement statute or regulation that would impair accomplishment of the Department's mission by limiting authority for necessary purchases or disposal. These provisions should be examined to determine whether the exemptions are themselves too limited to satisfy the DHS Secretary's likely requirements.

Congress should also ensure that special legal authorities now available to some agencies in acquiring information technologies are made available to the DHS.[16] These provisions are useful, but Congress has heretofore failed adequately to support multi-agency technology improvements and projects. Experts agree that such projects are essential to enable the government to learn to share information across agencies and engage in other cooperative efforts. One underlying problem is that Congress' appropriations process does not support multi-agency activities, because the committee structure is divided largely along agency lines. Congress must address this deficiency in the DHS legislation. Bills passed by the Senate and House would allow the DHS to engage in joint projects with other agencies. One bill, for example, would allow DHS to spend certain categories of funds through the Department of Energy pursuant to agreements to develop certain technologies.

## B. Creating New Capacities for Homeland Security Technology

A successful homeland security plan, in addition to including the necessary resources, personnel, and legal authority to achieve the plan's objectives, must call for organizational capabilities for providing the expertise, focus, and continuity needed to ensure that technology-related requirements are satisfied. Experience has demonstrated that conventional government mechanisms will fail to deliver technological improvements in a timely manner, if ever. Technological progress depends, not only on a centralized, empowered and well-funded government leadership,[17] but also on creativity, skilled planning, knowledge, experience, and effective implementation. Government can "marshal and direct" these resources,[18] but the resources themselves must necessarily be drawn from private sector experts, who, in fact, create and use most advanced technologies.[19] This point is made clear by the fact that 80% of the nation's infrastructure is owned and operated privately. It is this fact that caused President Bush to mandate government officials to establish concrete mechanisms for public/private cooperation.[20]

The range of issues the proposed DHS will face, moreover, is certain to be vast, and to include highly complex scientific and engineering problems at the cutting edges of many areas of expertise. The sheer complexity and array of tasks facing the new DHS Secretary makes it unreasonable to expect that acquisition issues will receive the depth and intensity of attention they require unless new mechanisms are created—mechanisms that are designed to encourage innovation and success. These mechanisms must require government to consult with and rely upon individuals who are capable of conducting mission-oriented planning and are aware of the best available technologies to accomplish those missions. The planning and acquisition of information technology, in particular, should be structured to avoid the top-down, inflexible, and ineffective initiatives that have done much to undermine Congress' confidence in the government's capacity to spend money constructively on information initiatives. Congress should consider using as a source for ideas the Internet Engineering Task Force (IETF), the principal body through which Internet technology has been shaped and regulated .[21] While the Internet is a product of government-sponsored research, it

has been built up to its present virtually universal acceptance by a group of private sector experts, who have collaborated as volunteers in a structured yet open format. Government agencies cannot be expected to function in precisely the same manner as the IETF, but they would benefit from the disciplined, creative, and diverse input of private sector experts.

As discussed below, the changes proposed by the Administration and included in bills passed by the two houses of Congress are inadequate. They permit, but fail to require, the new agency and its officials to break with past practices and include innovative and open planning and technology development. Rather than the many offices and centers that would be created by pending legislation, Congress should create essentially two, new entities with built-in private sector participation and authority: (1) a government department, or Center for Technology, under the direction of the DHS Under Secretary for Science and Technology; and (2) a non-government entity, or Institute for Technology, created to serve DHS, that is assigned meaningful roles in setting and implementing the technology agenda, as well as given the task of developing and deploying on an expedited basis particular technologies considered essential to homeland security.

### 1. DHS Center for Technology and IT Support

The Bush Administration has recognized in proposed legislation to create a new DHS, as well as in its National Strategy, the importance of deploying the best possible technologies in homeland security. The Administration also recognizes that, in order to harness science and technology in the war on terrorism, the DHS must rely on the private sector. "The private sector has the expertise to develop and produce many of the technologies, devices, and systems needed for homeland security. The federal government needs to find better ways to harness the energy, ingenuity, and investments of private entities for these purposes."[22] The DHS is to take the lead in overcoming the obstacles to using private capacities that the Administration recognizes exist: lack of experience and/or desire to work with the federal government due to rules and restrictions; lack of programs that solicit research and development proposals related to homeland security; lack of experience within agencies in acquiring technology; and lack of adequate funding and planning for security technology. With regard to information technology, the Administration would assign to DHS the task of securing better systems, once again with private sector advice, as well as the task of securing more cooperation among federal agencies and others in sharing information by overcoming both technological as well as "cultural" barriers.

The Administration proposes a general plan and several specific programs to achieve its objectives. The general plan is to create within the DHS "a management structure to oversee the agency's research and development activities and to guide its interagency coordination activities." To this end, the DHS is to engage in "constant examination" of vulnerabilities, "continual testing" of security systems, and "updated evaluations" of risks; it is to establish a "national laboratory" for developing and demonstrating new technologies; to solicit independent and private analysis; to set standards for equipment; to establish mechanisms for rapidly producing prototypes and for "high-risk, high-payoff" research; and to conduct demonstration and pilot deployments. The DHS would, with regard to information, coordinate the sharing of information, the government's acquisition of information systems, and the overcoming of legal and cultural barriers; adopt common "metadata" standards for electronic information related to homeland security; and improve public-safe-

ty emergency communications.[23] At no point, and on no issue, does the Administration propose any definitive or authoritative role for private sector experts or institutions; and virtually every proposed use of non-governmental resources deals with institutions, entities, or ideas that already exist, such as use of the national laboratories.

It is essentially this plan that both houses of Congress have adopted in two bills that at the time this paper was written were being considered in conference committee. Both bills establish a management system within the DHS to determine technology needs and ensure production, testing, acquisition, and deployment. The Secretary of the DHS is assigned these tasks in general terms, and an Under Secretary for Science and Technology is given direct responsibility for most of the anticipated activities.[24] In addition, the bills create several other offices that are given significant responsibilities for evaluating and acquiring technology; among these is an Under Secretary for Information and Infrastructure, who would be assigned the task of determining technological needs for information systems and their protection.[25] To coordinate the technology-related activities of the many offices and programs that would be created, the bills would also establish bodies assigned that task, such as the Homeland Security Science and Technology Council, described in the House legislation,[26] or the somewhat different Council described in the Senate bill .[27] Both bills also contain provisions authorizing the use of national laboratories and private sector experts and resources for various purposes, suggesting recognition that such advice is needed.[28] Some provisions require the agency to supply some information to the private sector, or to establish methods for private entities to obtain information from the agency.[29] The Senate bill does, moreover, signal a clear intent to support private sector research and development, particularly of critically important technologies.[30] But neither bill requires any use of private sector advice, and neither mandates any specific role to any private person or entity.[31] Both bills give DHS officials or entities exclusive responsibility for planning, research, development, and deployment of technology, including information technology.[32]

The Administration and the bills passed by the two houses of Congress have the correct objectives. The DHS must have ultimate responsibility for the government's technology programs, and given the many functions to be assigned to the DHS, it is essential that an entity be created under the projected USST to coordinate technology activities for all DHS agencies and departments. That entity should, however, be given clear authority over all technology-related proposals and functions, regardless of the number of issues assigned to officials other than the Under Secretary for Science and Technology. Further, an individual with technical and private sector experience, appointed by the DHS Secretary, who works as a full-time Director under the Under Secretary for Science and Technology, should run it. The entity should have within its structure, and subject to its coordination, all the government laboratories and specialized bodies that have technology-related missions and are included in the DHS.[33] It should be provided with multi-year budgetary support, including funds to be used for interagency IT activities, and for monetary awards to individuals (and departments) at the DHS who perform exceptionally well in implementing IT initiatives. Among other things, the DHS Technology Center should be required to review all major IT infrastructure proposals made by, or on behalf of, any DHS entity, and to evaluate and, where appropriate, to certify such proposals to Congress as warranting legislative support.[34]

The Center should be designed with specific roles for private sector experts. Its membership should include not only leading DHS and other agency officials, but also the heads of national laboratories and one or more businesspeople, academics, and scientists. These skilled outsiders should rotate over time to ensure fresh perspectives. While they serve, however, they should be full participants in the work of the Center, with the right to convey their individual opinions to the Secretary. The Center would be far more likely to call upon and give credence to private sector analysis and standards if it has some distinguished private sector participants. The Center will also be more effective at assigning work to, and evaluating the work of, a non-governmental entity established to enhance technology utilization.

**2. Non-Governmental Technology Institute**

The idea of having an expert entity guide the federal government on technological issues has been endorsed in principle in the National Strategy. The Administration supports creating "a laboratory—actually a network of laboratories—modeled on the National Nuclear Security Administration laboratories that provided expertise in nuclear weapon design throughout the Cold War." But the national laboratories already exist, and their mere availability has proved insufficient. While the National Strategy anticipates that a "central management and research facility" may be created, even *that* is not mandated, and the plan gives no special authority or role to the facility. Instead, it reads as continuing and perhaps expanding the use of scientific resources available at existing laboratories. Repeated references are made in the National Strategy to non-governmental expertise, and "centers of excellence," but once again nothing is proposed in that document or in the draft legislation that would vest any particular role in any private entity or individuals.

The bills passed by Congress also support making available additional non-governmental resources and expertise to enable the DHS to enhance its utilization of technology, as described above. The provisions for technology acquisition contained in these proposals would provide enhanced organizational elements, but no new capacities to overcome recognized and crippling deficiencies. These provisions would essentially continue, or, at best, marginally expand existing opportunities to utilize non-governmental resources. More is needed. It is inadequate, for example, merely to enable the DHS to "solicit independent and private analysis for science and technology research" on an ad hoc basis; Congress should ensure in the legislation establishing the DHS that independent, private expertise is a permanent feature of the agency's structure, and a resource that must be used. The Administration and Congress should create a non-governmental entity—a technology institute—that has a clearly defined structure and fulfills specific roles needed to improve government performance.

The concept of creating an independent institute with significant functions in defining and achieving federal technology objectives has important support. A panel of distinguished scientists and engineers on the National Research Council Committee on Science and Technology for Countering Terrorism recently proposed that the challenges associated with deploying advanced technologies can best be achieved by creating a Homeland Security Institute empowered and funded to enable government to fulfill the mandate of using the best available technologies to protect the American people.[35] The panel studied prior reports and evaluations concerning the use of technology by government agencies in the national security arena. They concluded that "America's historical strength

in science and engineering is perhaps its most critical asset in countering terrorism without degrading our quality of life," and that the nation had to take advantage of its "immense capacity for performing creative basic research, at universities, government laboratories, industrial research facilities, and non-governmental organizations."[36] The panel agreed that a central office should be created that would be responsible for strategy and coordination,[37] but it frankly stated its belief that the federal government lacked the capability to perform these roles: "The committee believes that the technical capabilities to prove the analysis necessary to support this organization do not currently exist in the government in a unified and comprehensive form. Thus **the committee recommends the creation of a Homeland Security Institute to serve the organization setting priorities for homeland security."**[38] In its report concerning information systems, the Committee makes clear the special importance of acquiring the technology needed for effective protection, and the special need to rely in this area on private sector expertise:

> All phases of counterterrorism efforts require that large amounts of information from many sources be acquired, integrated, and interpreted. ...Thus, information fusion and management techniques promise to play a central role in the future prevention, detection, and remediation of terrorist acts. Unlike some other sectors of national importance, information technology is a sector in which the federal government has little leverage. Thus, constructively engaging the private sector by emphasizing market solutions seems a desirable and practical way for the government to stimulate advances that can strengthen the nation's information technology infrastructure.[39]

The concept of an institute to provide expert support for all aspects of the DHS' technology work is strongly supported by the distinguished members of the President's Council of Advisors on Science and Technology, as well as by Dr. John J. Hamre, former Deputy Secretary of Defense, and a member of this Task Force.[41] The DHS is far more likely to succeed in exploiting the technological potential of the United States if the agency has, and is required to use, the advice and assistance of an institute of the sort so strongly supported by the nation's scientific elite. The legislation creating the DHS should therefore also create an institute whose authority and procedures are structured to enable it to succeed in accomplishing the technological objectives the Administration and Congress properly seek. Here are some ideas on the key issues.

**Structure.** The institute should be, as the NRC Committee recommends, "located in a dedicated, not-for-profit, contractor-operated organization" that is committed to serve, but outside the DHS.[42] Its executive director should be an expert in some relevant technology, appointed by a non-partisan board of directors chosen by the President and Congress, and including public sector (federal, state, and local) CIOs and private sector experts as members. In addition, the institute should have a relatively large body—a scientific assembly—composed of agency CIOs and experts, private sector participants, and state and local officials. The scientific assembly, or some similar body, should be empowered to propose and regularly review and comment on institute activities. It should operate through committees, whose members should be selected on the basis of experience and expertise. The committees should perform the initial research and study on technology-related tasks assigned to the Institute by Congress or the DHS Secretary, or spontaneously undertaken on the basis of assembly resolution. These committees should develop proposals for assembly and board consideration, including protocols and certification standards, and should conduct pro-

grams to satisfy other institute responsibilities. Committees should welcome, to the extent possible, the participation of qualified experts on a voluntary basis, in order to inculcate an atmosphere of creative interaction, analogous to that of the IETF.

**Tasks.** The Institute should perform, or monitor the DHS performance of, the most demanding tasks assigned to the DHS, such as developing and implementing the DHS IT architecture; preparing and implementing necessary protocols for information-related activities, including those necessary to assure meta-data capacities that enable systems to be interoperable, for reliable security and storage of data, and for access by state, local, and foreign participants;[43] developing standards for information-related technological products such as identification cards; certifying private sector products that meet government requirements, and providing guidance concerning such products to federal, state, and local officials; monitoring and reporting to the DHS Secretary, the President, and Congress, on all government-funded information-related technological research at government labs or in the private sector; providing accessibility and responsiveness to private sector developers and vendors by screening their products and proposals, thereby lowering barriers to market entry, aiding R&D, and enhancing competition; searching throughout the world for technologies that could prove useful to agencies; generating ideas to enhance security through technology; developing standards for achieving security-related objectives with minimal intrusion on privacy and other recognized civil liberties; deploying funds through private entities such as the government-owned venture capital fund, In-Q-Tel, to provide "seed" or other capital needs for promising technological innovations; and recruiting and placing talented high-tech people in DHS agencies.[44] To perform these roles, the Institute should possess the expertise required to deal with scientific issues and technological objectives in the full range of relevant disciplines.

**Powers.** Congress should empower the institute to perform at least some of the functions listed above, such as the tasks of evaluating major IT proposals and of screening technologies proposed for use by private companies. In addition, Congress should authorize the DHS Secretary, GAO, or the President to assign to the Institute any relevant task, and should itself assign the institute the task of developing and deploying particularly important technologies.

The institute should rely upon persuasion rather than compulsion. Information specialists widely believe that mandated changes, imposed without consideration of the needs of users, are likely to fail. Protocols, rather than inflexible standards, should set operational requirements, leaving room for innovation and experimentation consistent with operational necessities. The institute should, however, be empowered to advise the DHS Secretary, or Congress, if it concludes that any DHS entity is failing to adopt appropriate methods or technologies.

**Budget.** The institute should not be wholly reliant on annual appropriations. It should be required to engage in many, long-term efforts, including special development and deployment projects of the sort described below. Congress should therefore provide funds for the institute in multi-year tranches, where appropriate, subject to annual review.

**Conflict of Interest Limitations.** Institute personnel, including board, assembly, and committee members, and consultants, should be required to comply with strict, open standards regarding disclosure and participation. No person should be allowed to decide or vote on any matter in which

he/she has a financial interest. It will be necessary to rely on experts and consultants, however, at all levels of the institute, who have various levels of involvement in particular fields. The participation and opinions of such individuals should be allowed, subject to full disclosure of their interests.

**Special Projects.** The DHS Secretary and/or the institute should be authorized by Congress—and where appropriate even required—to establish special projects to expedite development or deployment of technologies needed to satisfy specific requirements critically important to homeland security. Experience in government acquisition has demonstrated that, in the face of urgent needs, the United States has been successful in developing and deploying technologies by establishing special projects for those purposes. The Manhattan Project is the most famous of such initiatives; others include the Fleet Ballistic Missile Program; the original work in creating the National Reconnaissance Office acquisition system; the Y2K Project; and the Army's Force 21 initiative. These programs are characterized by the following: (1) a recognized, time-driven need of the highest priority; (2) funding stability sufficient to overcome the uncertainties of the normal, annual approval cycle; (3) funding levels sufficient to meet project deadlines; (4) a cooperative relationship between government and contracting entities based on teamwork rather than the adversarial relationship that normally exists with contractors; (5) continuity of personnel within both the private and government entities involved; and (6) small government/contractor program office teams empowered with complete end-to-end contracting and execution responsibility, including technical development, production, installation, and operational support. Projects may, but need not, be located at specific, secure locations.[45]

Among the specific technological requirements widely recognized as necessary for homeland defense are sensors capable of identifying the full range of threats in a timely and reliable manner;[46] bridging the information gap that exists between agencies for the purpose of permitting access to information that may lead to identifying dangerous individuals (i.e., a watch list);[47] and developing a system to track all aliens in the United States. [48] Congress has indicated it is prepared to order specific projects aimed at producing security results based on technology. In creating the TSA, Congress ordered the installation of explosive detection systems, or the use of alternative methods, to screen luggage on passenger planes by the end of 2002. The deadline is unachievable, and Congress seems prepared to extend it for a year. But the decision to force such screening has expedited development of the necessary technology. Coupled with a plan and resources, such efforts would have an even greater impact on security.

## IV. Conclusion

The call for enhanced use of technology to prevent and respond to terrorism is valid and deserves a credible and effective plan for action. Government must set the nation's objectives and the policies needed to procure the best possible technologies. Government possesses neither the capacities nor the culture, however, to create and deploy new technologies in an efficient manner. To assign this task to government agencies that have repeatedly failed to deliver will be no more fruitful merely because the same agencies have been consolidated into one DHS. Nor will it suffice to create new government entities with new, catchy names to perform this work. None of this ensures sufficient new capacities.

The President and Congress should require the DHS to involve those people and companies actually responsible for America's extraordinary technological achievements. The legislation will be far more effective at achieving its aims concerning technology if the legislation is narrowed and simplified, and if it mandates roles for companies, individuals, and universities at every stage of planning, development, and implementation.

## Endnotes

[1]To illustrate, the testimony of the GAO's Director of Information Security Issues, Robert F. Dacey, before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives, released on July 9, 2002, contains detailed evaluations of the failures of agencies to adopt mandated measures concerning the most important of all homeland targets, critical infrastructure, as well as seriously inadequate development of information sharing technologies and practices, and egregiously insufficient measures related to cyber security. The GAO concluded that the nation continues to lack a national critical infrastructure protection strategy, despite many public statements and the creation of several specialized entities on the subject. It also concluded that the new DHS would have to address "pervasive weaknesses in federal information security." On the latter issue, GAO stated:

> Our November 2001 analyses of audit results for twenty-four of the largest federal agencies showed that weaknesses continued to be reported in each of the twenty-four agencies. These analyses considered GAO and Inspector General (IG) reports published from July 2000 through September 2001, which included the first annual independent IG evaluations of agencies' information security programs required by government information security reform legislation (commonly referred to as GISRA).

The weaknesses GAO identified covered "all six major areas of general controls, including security program management; access controls; software development; segregation of duties; operating systems controls; and service continuity." GAO-02-918T, p. 29.

[2]This point is concretely made by Jim Puzzanghera in commenting on the prospective absorption of INS into the new DHS: "But the new agencies would be saddled with the same outdated technology that has left the INS unable to effectively guard the nation's borders or cope with growing immigration." San Jose Mercury News, April 29, 2002, p.1A.

[3]Testimony to the Comm. on Gov't Affairs, U.S. Senate, June 26, 2002, p.1, at http://www.senate.gov/~gov_affairs/062602carter.htm

[4]For example, the National Institute of Standards and Technology, currently part of the Department of Commerce but likely to be included in the DHS, has provided measurements, standards, and technical advice related among other things to terrorist threats. See generally, "Technologies for Improved Homeland Security," describing its functions, at https://axess2.Stanford.edu/a2kprd76ha/user/campnet/cn_frameset.asp

[5]The GAO testimony, supra, calls for a "human capital strategy" to overcome the problem of properly protecting the nation's critical infrastructure. The GAO clearly recognizes that "few federal departments and agencies" have either the personnel or the management practices necessary to develop and implement technologically sophisticated initiatives, such as enterprise architecture.

[6]The GAO reports that "a March 2001 report by the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency (PCIE/ECIE) identified significant deficiencies in federal agencies' implementation of PDD 63 requirements to (1) establish plans for protecting their own critical infrastructure that were to be implemented within two years, or by May 2000, and (2) to develop procedures and conduct vulnerability assessments." GAO-02-918T, "Critical Infrastructure Protection," p. 9 (July 9, 2002).

[7] The FBI, which is not going to be made part of the DHS, has been widely criticized for its failures in information technology, despite the importance of the tasks it is assigned. Among other things, it has failed to develop an adequate strategic plan, has no comprehensive strategic human capital plan, has personnel with inadequate language skills, antiquated computer hardware and software, no enterprise architecture, and several disabling cultural traditions. See generally, "FBI Reorganization," GAO-02-865T, pp. 8-11, 15 (June 21, 2002); "How Outdated Files Hamper FBI Effort to Fight Terrorism," *Wall Street Journal,* p.1 (July 9, 2002); "War on Terrorism Highlights FBI's Computer Woes," *Los Angeles Times,* July 28 & 29, 2002. The INS has also been severely criticized for its information shortcomings. See "Homeland Security," GAO-02-886T, p.23 (June 25, 2002).

[8] An Intellibridge Analysis reports an estimate that federal agencies will spend $13.2 billion on private workers to manage and run their technology systems by 2006. It also quotes Norman Lorentz, CTO of OMB, predicting that outsourcing will increase far beyond current levels (August 20, 2002).

[9] Several specific instances now exist of efforts to force agencies to use the private sector, or to adopt technologies already being used in the private sector. The Government Information Security Reform Act of 2000 (GISRA) requires agencies to integrate security programs into their computer networks and capital plans, or face budget cuts. Many agencies are reported to have begun "doing things they should have been doing long before." "Taking Security Concerns Private: U.S. Appeals to IT Firms," *Washington Post,* p. EO5 (June 20, 2002).

[10] A CFR study calls for a "Red Team" project to create a Counter-Terror Information Technology system (CTIT) that combines data from a wide variety of border administration and security agencies, private sector firms in transportation and finance, educational institutions, and foreign sources; in a common format that can be swept by a variety of data-mining technologies; and return useful information on suspicious patterns and behavior in a timely fashion to line agents and law enforcement agencies. It states, however, that "the business-as-usual federal IT contracting approach will not create what the Terrorist Tracking Task Force needs in any reasonable time frame," and calls for "throwing out the rulebook." Jan M. Lodal & James J. Shinn, "Red-Teaming The Data Gap," pp. 2-4, http://www.cfr.org. The Markle Task Force agrees with the need for and feasibility of bridging technologies for sharing data, though it advocates a more discriminating collection of data, and regards the procurement obstacles as far more manageable than the CFR study assumes.

[11] *See* "Reinventing Federal Procurement," describing the many initiatives underway to modernize, streamline, and simplify procurement, available at http://govinfo.library.unt.edu/npr/library/nprrpt/annrpt/vp-rpt96/appendiz/federal.html

[12] The DHS Secretary would be required to comply with limitations and conditions applicable to the Secretary of Defense, in using this authority, including the requirement that he/she determine "that the use of a contract, grant, or cooperative agreement for such project is not feasible or appropriate." This limitation may prove too restrictive in dealing with smaller companies far less able to deal with government than large, defense contractors.

[13] See generally the discussion in David S. Bloch & James G. McEwen, "'Other Transactions' with Uncle Sam: A Solution to the High-Tech Government Contracting Crisis," *10 Tex. Intell. Pro. L.J. 195* (Winter 2002).

[14] A somewhat revised form of the same OT authority, given to the Defense Advance Research Projects Agency (DARPA) in Section 845 of the 1994 NDAA, to "carry out prototype projects that are directly relevant to weapons or weapon systems," is also proposed to be given to the new Department in Section 732(a)(2). This, too, is a sound proposal, though the statute should be revised to make clear that the authority extends beyond "weapons" to any prototype project that the DHS Secretary finds would enhance homeland defense.

[15] The Task Force supports flexible rules for key personnel needed to enhance homeland security. It has not considered the need for broader reform of personnel rules.

[16] For example, federal information policy provides authority for coordination (44 USC 3504), for capital planning and investment control, and for pilot programs to "test alternative approaches for acquisition of information technology by executive agencies," including on a multi-agency basis, and to use pilot programs to test "solutions-based contracting" for information technology acquisition (40 USC 1422, 1471 & 1492). See generally the FAR, Part 39: Acquisition of Information Technology, Vol. 1, Parts 1-51 (Sept. 2000).

[17] The emphasis on internal government reform was signaled in the instructive and otherwise sound analysis in William B. Bonvillian & Kendra V. Sharp, , which at one point speculates that "the overwhelming public support for the fight against terrorism suggests that first-rate scientists and engineers would be willing to work for this entity [DHS' DARPA] in this time of crisis." "Homeland Security Technology," *Issues in Science & Technology,* Winter 2001, p. 6.

[18] *Id.* at 1. Mr. Bonvillian is legislative director and chief counsel to Sen. Joseph I. Lieberman of Connecticut; Ms. Sharp is an assistant professor of mechanical engineering at Pennsylvania State University.

[19] The GAO explained this in commenting on the FBI reorganization: "There is also a growing understanding that all meaningful results that agencies hope to achieve are accomplished through networks of governmental and non-governmental organizations working together towards a common purpose." GAO-02-865T, p.17 (June 21, 2002).

[20] Executive Order 13231, entitled "Critical Infrastructure Protection in the Information Age," and issued on October 18, 2001, requires the Critical Infrastructure Assurance Office to establish a broad-based partnership with the private sector, to encourage the exchange of assistance on information security practices.

[21]The IETF is a purely voluntary organization that nonetheless has been able to develop and approve the standards under which the Internet operates. It taps the talents of private (and public) sector experts who are eager and able to participate in fulfilling ambitious technological missions, such as identifying and proposing solutions to operational and technical problems of the Internet; specifying the development or usage of protocols and near-term architecture to solve such problems; making recommendations regarding the standardization and usage of protocols to the Internet Engineering Steering Group (IESG); facilitating technology transfers from the Internet Research Task Force (IRTF) to the wider Internet community; and providing a forum for information exchange among Internet vendors, users, researchers, agency contractors, and network managers. See generally, The Tao of IETF: A Novice's Guide, RFC 3160, (August 2001). https://axess2.stanford.edu/a2kprd76ha/user/campnet/cn_frameset.asp

[22] National Strategy, p.51.

[23] *See id.* at 53-58.

[24] *E.g.,* H.R. 5005, Sec. 301. The Senate bill (and Lieberman amendment) describes the DHS Secretary's duties in some detail, including the duty "to identify and promote key scientific and technological advances that will enhance homeland security," and "to oversee and ensure the development and implementation of an enterprise architecture for Department-wide information technology, with timetable for implementation." S. 5005, Sec. 102(8), (16), & (17).

[25] H.R. 5005, Secs. 201, 204, 206. In addition, an Under Secretary for Management would be responsible for "information technology and communications systems, and a Chief Information Officer would separately report directly to the Secretary on all information-related issues. Id. 601(4); 603. The Senate bill also would create several offices with overlapping technology-related responsibilities, including: an Under Secretary for Critical Infrastructure Protection with wide authority over key U.S. industries and cyber security; an Under Secretary for Science and Technology to run a Directorate of Science & Technology with comprehensive responsibilities for homeland security technology; an Under Secretary for Emergency Preparedness; and a Chief Information Officer. It would also create an additional layer of authority over information technology by assigning to the Director of the Office of Management and Budget the task "in consultation with" the DHS Secretary, "of creating a comprehensive architecture for information systems," as well as the task of developing a "plan to achieve interoperability between and among information systems….of all agencies with homeland security responsibilities."

[26] The House version of the Council would be composed of all the DHS Under Secretaries, and chaired by the Under Secretary of Science and Technology, who would decide when to call meetings. The Council would "establish priorities for research, development, demonstration, testing, and evaluation activities conducted or supported by the Department," and to "ensure that the priorities established" reflect the Department's acquisition needs. Sec. 306(a) & (b).

[27] The identically named Council in the Senate bill would have senior DHS officials as members, but would also include the Director of the Office of Science and Technology Policy, the Director of a new organization, the Security Advanced Research Projects Agency (SARP"), and officials of the Executive Office of the President. This Council would coordinate homeland security research and development among all agencies "and entities in the private sector and academia..." recommend specific areas to fund for rapid deployment, and assist the Under Secretary of Science and Technology in developing the technology roadmap assigned to the Directorate for Science and Technology for preparation. Beyond even this, the bill would create an Office for Technology Evaluation and Transition, which would serve "as the principal, national point of contact and clearinghouse for receiving and processing proposals or inquiries regarding such technologies;" would identify and evaluate promising new technologies; test and assist in deploying them; and coordinate with SARPA to accelerate the transition of technologies it develops. If the DHS Secretary finds even this insufficient, the Secretary could assign any aspect of the Science and Technology Directorate to be carried out through or in coordination with a Technical Support Working Group or similar entity.

[28] H.R. 5005, Sec. 304. The House bill says the Under Secretary of Science and Technology "may establish a headquarters laboratory" for the DHS, after following certain procedures, "at any national laboratory and may establish additional laboratory units at other laboratories" p. 46. This provision adds nothing to existing resources, other than the designation of a lead lab. The bill also provides that the Under Secretary of Science and Technology "shall operate extramural research, development, demonstration, testing, and evaluation programs . . . " involving entities from as many geographic areas as practicable and on the basis of competitions as open as possible. Within one year or enactment, the Secretary, through the USST, "shall establish" a university-based center or centers for homeland security, taking into account a number of technology and terrorism-related capacities. The next section, however, gives the Secretary "discretion to establish such centers," and requires a report to Congress on implementation. This may mean that a center will be designated, but the bill nowhere provides any particular role for such a center, or assigns it any particular responsibility, p. 44. The House bill goes through the trouble of providing for a "Special Assistant" to the DHS Secretary, who would be required to interact and foster communications with the "private sector," other agencies, national labs, FFRDCs, and academia, including creating "advisory councils" from which to

obtain advice on various issues. The Under Secretary of Science and Technology would, in addition, be required to create a "centralized Federal repository of information related to technologies" regarding possible use of unconventional weapons, and to disseminate that information to federal agencies, state and local governments, and the private sector. The Under Secretary of Science and Technology would also create a repository of information "for persons seeking guidance on how to pursue proposals to develop or deploy technologies that could contribute to homeland security," or to assist in evaluating and implementing technologies and research and development. Sec. 301(8), (9), & (10).

[29] For example, the Under Secretary of Science and Technology is instructed in the Senate bill to share and disseminate research and development discoveries and opportunities with other entities, including the private sector, and to contract with or establish FFRDCs "determined useful by the Secretary" to provide independent analysis and support.

[30] The bill would create an "Acceleration Fund" to support technology research and development, to be used for projects selected by the newly created SARPA (in contrast to DoD's existing DARPA), with recipients to include private sector entities or individuals, universities, or FFRDCs. SARPA would support especially "high-risk, high-payoff" technologies that "may lie outside the purview or capabilities of the existing Federal agencies," and emphasize "revolutionary rather than evolutionary or incremental advances."

[31] The Senate bill would require the DHS to prepare a "Strategy for Countermeasure Research," or "plan for engaging non-Federal entities, particularly including private, for-profit entities, in the research, development, and production of homeland security countermeasures for biological, chemical, and radiological weapons," and to submit the plan within 270 days of enactment for Congress' consideration. Regrettably, this plan would not explicitly extend to information systems.

[32] The House bill would create a Federal Information System Security Team, consisting of agents and scientists, to provide technical expertise to agencies (when requested). This team would assist them in securing critical information systems by conducting security audits, vulnerability assessments, and testing the effectiveness of information security control techniques. No non-government participants are provided for, despite the obvious superiority of private companies in this work.

[33] The technology-focused entities the President has asked to be included within the DHS include the three research laboratories at Los Alamos, Sandia, and Livermore, as well as the National Infrastructure Protection Center, the Critical infrastructure Assurance Office, the Computer Security Division, the National Infrastructure Simulation & Analysis Center, the Federal Computer Incident Response Center, and the Special Adviser of Cyberspace Security. Other technology-related entities exist, within the White House and in other agencies. Congress should give serious consideration to including all these within the overall control of the Institute, in addition to the President's personal advisor on science and technology.

[34] If, as one bill provides, the DHS is required to put together an overall plan for information security, or any other comprehensive plan, the Center should review it.

[35] *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (Nat'l Academy Press 2002). The Committee is composed of 118 of the nation's top scientists, engineers, and doctors, drawn from the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine, all independent research organizations chartered to advise the government on technical issues. In addition to an Executive Summary, the report contains chapters detailing recommendations concerning nuclear threats, threats to humans and agriculture, toxic chemicals and explosives, information technology, energy systems, transportation systems, cities and fixed infrastructure, human response to attacks, complex and interdependent systems, and various aspects of technology.

[36] Pages ES-19 & 17.

[37] The Committee recommended establishing the office of Under Secretary for Technology in the DHS to provide a focal point for guiding key research and technology programs across the department, but added **"and most importantly, engaging commitments from the major science, engineering, and medical science agencies that will remain outside the proposed new department."** Chap. 12-6 (emphasis in original).

[38] Page ES-17 (emphasis in original).

[39] ES-9.

[40] The Council's report to the President of July 23, 2002, spells out the case for an independent institute, and a variety of other measures. With regard to the importance of involving the private sector in the DHS' work, it states: "Just as most of America's critical infrastructure is private owned (85 percent), the majority of research and technology capacity resides in the private sector, i.e., in business, academia or not-for-profits. Capturing this capacity for homeland security R&D presents challenges. We believe that homeland security R&D should focus on setting require-

ments, establishing budgets, determining priorities, awarding and managing grants and contracts, testing and evaluating products, and other related functions. Most 'hands-on' R&D work can best be done in academia, industry, and national laboratories, with a very few important exceptions. …" Draft Report, pp. 5-6.

[41] Dr. Hamre, who is President and CEO of the Center for Strategic and International Studies, testified in detail on DHS issues to the Senate Committee on Government Affairs on June 28, 2002. Among other things, he called for establishment of an FFRDC dedicated to the technological support of several critical homeland security functions, essentially identical to many of those recommended in this study. Testimony, pp. 17-18.

[42] ES-17. This form was settled upon in creating the Institute for Information Infrastructure Protection. The Institute for Defense Analyses considered the four structural alternatives, and settled on a national research and development institute for much the same reasons applicable to the present situation. *See A National R&D Institute for Information Infrastructure Protection (I3P),* Chap. 10 (IDA Paper, P-3511) (April 2000).

[43] It seems dubious to assume that regular government personnel will in fact develop the meta-data standards that would enable agencies to establish interoperable information systems, as Congress still seems to assume. They lack the capacity to bring about that result.

[44] The NRC Committee proposes a similar set of functions: "The institute would perform systems analysis, risk analysis, and simulation and modeling to determine vulnerabilities and the effectiveness of the systems deployed to reduce them; perform sophisticated economic and policy analysis; manage red-teaming activities; facilitate the development of common standards and protocols; provide assistance to agencies in establishing testbeds; design and use metrics to evaluate the effectiveness of homeland security programs; and design and support the conduct of exercises and simulations." Report of the NRC, p. ES-17.

[45] The Department of Transportation's Security Agency resorted to such an approach in connection with its role in improving airport security. It invited proposals by airports to find, test, and deploy technologies needed to accomplish certain recognized requirements, including the capacity to prevent explosives from being taken onto aircraft, and to identify persons likely to pose a risk sufficient to warrant preventing them from boarding passenger aircraft. The 2002 Silicon Valley Blue Ribbon Task Force for Airport Security and Technology submitted such a proposal to the Agency, in a report that specifies the security aims of San Jose's airport and how it intends to go about achieving them. This approach will expedite identification of useful technologies and trigger intense and focused efforts to secure their effective utilization.

[46] Research is currently underway to develop sensor technologies in several government laboratories and private sector institutions. This research needs to be better coordinated, and to be made more focused on producing devices that are deployable in the near future. PR events are no substitute for actual deployment. The task is formidable. Materials that must be sensed to provide security include, in addition to metal, the nuclear, chemical, and biological substances likely to be used in bombs and weapons of mass destruction. Sensors are needed, moreover, that have the capacity to detect these materials in differing physical contexts, and at much greater distances than is now possible. Shipping containers, cars, ships, and other moving objects, are among the most likely vehicles terrorists will use in future attacks, and sensors capable of detecting the full range of suspect substances within these vehicles would greatly enhance security. Advanced sensing capabilities are also desirable at bridges, tunnels, and other critical physical infrastructure. We are far from having the capability to detect suspect substances on a timely basis in these contexts.

[47] There is widespread recognition of the need for a system that provides more than simple information sharing, "information awareness." Comprehensive databases are unnecessary impingements on privacy and other protected interests. Consolidated watch lists are needed, however, to overcome the failures associated with the September 11, 2001 attacks and other failures based on a lack of sufficient information coordination. Fashioning and deploying watch lists is well within the technological capacities of IT experts. Respected and experienced individuals uniformly claim to have created, or to be able to create, in relatively short time periods (less than six months), the technological equivalent of government watch lists far larger and more complicated than any that might be required for most government functions, such as airport and border security. Access control for such lists is readily managed through available programs that can be incorporated. A database can be designed to permit partial or complete disclosure of information to particular groups or individuals, and can be limited whenever desired to providing notice of the existence of information to which the user is invited to seek access on a need-to-know basis, or upon which the user is instructed to act in a specific manner, such as to refuse access to, or to arrest, a particular individual. IT experts suggest that an entity with authority to insist that a needed database be established, even with partial coverage and incomplete data, could provide the breakthrough necessary to put these capacities to the service of the nation.

[48] The pending bill, H.R. 5005, Sec. 435 would establish a Technology Advisory Committee on the feasibility of a system to track all aliens in the United States. This is the type of task that the Institute would be ideally suited to perform.

# Report of the Working Group on Organizational Challenges

*This Working Group was chaired by John Hamre. This report was drafted on behalf of the group by John Hamre and Mary DeRosa. Participants in this group were Alexander Aleinikoff, Robert Atkinson, Zoë Baird, James E. Baker, Stewart Baker, Jerry Berman, Robert Bryant, James Dempsey, Amitai Etzioni, Eric Holder, Arnold Kanter, Michael Leavitt, James Lewis, Mary McCarthy, Dave McCurdy, Beth Nolan, Joseph Onek, Daniel Ortiz, Larry R. Parkinson, Harvey Rishikof, Jeffrey Smith, Paul Schott Stevens, Michael Vatis, and Philip Zelikow, with assistance from Ryan Coonerty.*

Working Group III was asked to examine two issues about government organization. First, how must government structures adjust to accommodate new information needs? Second, as our approach to information collection, analysis, and sharing changes, how do we oversee these new practices and structures effectively to protect the liberties and values that define our society?

## Organizing for Effective Collection, Analysis, and Use of Information

New security threats require new approaches to information collection, analysis, and dissemination. We no longer face only known enemies who operate almost entirely overseas. Although the terrorist threat is foreign, they operate all over the globe including, as we know so well since September 11, in this country. We know relatively little about their methods and many traditional intelligence techniques are of limited use in providing warning of their plans. The traditional compartmentalized approach to collection, analysis, and use of information about vulnerabilities and adversaries will not work with this new, dynamic threat.

To keep ahead of this threat, vastly more information must flow to and from elements within the federal government, state and local governments, and the private sector. Working Group III examined whether the dramatic changes we need to make in our approach to collection and use of information will require revisions to current governmental structures and agency roles.

The working group discussed three ways in which our institutions must adjust to satisfy these new information needs.

**Remove barriers to information sharing between and within federal government organizations.** The federal government must develop an integrated information system that allows sharing of all sources of information related to homeland security. This would involve not only members of the intelligence community and the FBI, but organizations such as the INS, Customs, other border agencies, consular offices, health agencies, and many other entities that come across information in carrying out their responsibilities that could be critical to uncovering terrorists' plans. Information must flow not only up chains of command, but out to the agents in the field. There has been a good deal of attention to "breaking stovepipes" since September 11 because of the many stories of important information that did not make it to people within the government who could have used it.

There already have been some improvements, largely resulting from increased use of mechanisms that were in place, but underused, before September 11. What is needed most is coordinated and sustained attention to improvement of information systems so that they are interoperable and, to the maximum extent possible consistent with security, eliminate barriers to information flow.

**Develop an effective, coordinated mechanism for exchange of information between the federal government and state and local entities.** State and local law enforcement, health, and other government agencies are the source of the vast bulk of domestic information that is relevant to the fight against terrorism at home. After all, the FBI has only 11,400 agents across the country; there are many hundreds of thousands of local police, sheriffs' office employees, and other government personnel collecting information every day. Several federal agencies have relationships with state and local actors: the FBI and other federal law enforcement agencies communicate regularly with law enforcement personnel; FEMA has ties to state and local first responders; the Department of Health and Human Services interacts with the public health community. But sharing is ad hoc and inconsistent. The local entities often do not know what to share or with what federal agency they should share it. Federal agencies often resist sharing information with state and local entities because of concerns about operational security and the potential for leaks.

There are several promising information-sharing initiatives among states and in local jurisdictions. For example, Pennsylvania's Justice Network, known as JNET, links databases from various state law enforcement agencies. JNET participants have access to approximately 60,000 images of criminal suspects, driver's license photos, and other information useful for identification. There are other new projects in Dallas, Houston, and California, to name a few. What is missing is a federal effort to promote and coordinate these initiatives and ensure they are effective and interoperable.

**Improve domestic collection of foreign intelligence and its analysis and use for prevention, warning, vulnerability analysis, and policy decisions.** The United States has never had a separate agency devoted to domestic intelligence. In countries such as Canada, France, Germany, Israel, and the United Kingdom, internal security agencies are charged with providing the government the domestic intelligence it needs for terrorism prevention and policy decisions related to terrorism. These agencies collect intelligence within the country using surveillance and other techniques, analyze it, and provide it to those within the government who need it for prevention of terrorist attacks and policy decisions. These agencies are separate from the countries' law enforcement organizations.

In the United States government we have a different structure. A law enforcement agency, the FBI, is also the primary agency responsible for domestic collection of foreign intelligence, including intelligence on terrorist threats, and analysis of that intelligence. Approximately one-quarter of the FBI's almost 28,000 employees are devoted to collecting and analyzing intelligence pursuant to the Attorney General's Foreign Intelligence Collection Guidelines. Their priorities are counterintelligence and counterterrorism. The FBI has a long history of effectiveness in the area of counterintelligence. With its newer counterterrorism role, the FBI's effectiveness is undercut by its cultural and organizational bias in favor of its law enforcement mission.

Unlike an intelligence agency, the orientation of a law enforcement agency is primarily reactive. Its purpose is to capture and prosecute criminals. Law enforcement agencies often will prevent acts of

terrorism or other crimes by catching a criminal before a crime is committed, but they collect information to catch criminals, not to provide warnings, assess vulnerabilities, or inform policymakers. The customer for law enforcement information is the prosecutor and a significant concern in its collection is the suitability of the information for use in court. Law enforcement and foreign intelligence information are collected using many of the same tools and techniques, but different legal authorities and guidelines.

The FBI's culture is that of a law enforcement agency. There is little representation, particularly in the senior levels of the agency, from people with experience in national security. Although senior personnel interact regularly with national security policymakers, there is a resistance ingrained in the FBI ranks to sharing counterterrorism information with the national security community or others outside of law enforcement channels. Unlike our foreign intelligence agencies, the FBI has no effective process for providing intelligence on terrorism to policymakers and others outside of the law enforcement community who need it. Moreover, the FBI has not prioritized intelligence analysis in the area of counterterrorism. The role of analysts is not valued at the FBI the way it is in other intelligence agencies. There is insufficient funding and staffing to conduct the kind of intelligence analysis that is needed for domestic intelligence in the counterterrorism area.

## A New Structure

The first significant step in government reorganization to accommodate new information needs is creation of a new Department of Homeland Security. But the legislation creating the department raises many more questions than it answers about the roles of the players—within the federal government and outside—in information collection and analysis. It is critical that these roles be clarified in the new department's first days. We provide here our views on the most sensible roles for the key players.

**The Department of Homeland Security.** The Department of Homeland Security will be a significant consumer of domestic intelligence and a significant producer as well. The new department will bring together the border authorities and other entities that collect significant domestic information. Its Secretary will be among the principal policymakers responsible for domestic security.

The legislation establishing the Department's new intelligence directorate envisions a center to receive, collate, and analyze intelligence from all sources, including domestic intelligence. This is a significant step toward an internal security function—although it would not combine all domestic collection and analysis in the U.S., as the internal security agencies in other countries do. If done well, this directorate could be enormously useful as a nerve center for intelligence related to domestic security. If mismanaged, it will be toothless, ignored by CIA and FBI, and useless to policymakers.

To be sure that the new intelligence directorate lives up to its promise, it must have authority to receive the information it needs from other federal government sources. The question whether the Department of Homeland Security may "task" the FBI and CIA for intelligence collection and analysis has generated significant controversy and concerns that the new department would become a "super agency" with too much power. Similarly, there is enormous resistance to giving the new department the authority to receive intelligence in its "raw" form from other entities. But with-

out these authorities the new directorate will be hampered significantly. An intelligence directorate with no collection powers of its own will not be able to set its own priorities or pursue avenues it considers important if it cannot influence directly the intelligence it receives. One of the Administration's first priorities once the Department of Homeland Security is established must be to coordinate a set of understandings among the relevant entities that will give the Department of Homeland Security real authority—without bureaucratic hurdles—to receive the information and analysis that it needs.

The new directorate is also the most sensible place to assign some newer domestic intelligence responsibilities that are not traditionally "investigative" and for which the FBI has no special expertise. The best example of such a function is the use of government and private databases to identify terrorist planning and activities before attacks occur. There is growing understanding that access to information in government and private hands is an essential tool in the fight against terrorism. Obtaining and analyzing this information is a natural role for the new intelligence directorate.

**The FBI.** The FBI is the federal government's chief law enforcement agency and law enforcement will always be a critical part of anti-terrorism policy. In addition, information collected during criminal investigations often will have value outside of the law enforcement context, for prevention, warning, and policy. The FBI must improve its ability to analyze and retain law enforcement information and to share it within its own agency and with others. The FBI is taking a number of steps to improve its ability to share this information internally, including development of Trilogy and other more advanced information systems.

The FBI's role in the separate discipline of intelligence collection and analysis for counterterrorism is more difficult. The FBI culture's strong bias in favor of the law enforcement mission has interfered with its ability to be effective at collecting, analyzing, and sharing domestic intelligence related to counterterrorism. There are sound reasons why many countries have chosen to separate their law enforcement and intelligence functions.

There are advantages, though, to keeping certain domestic intelligence functions and law enforcement in the same organization. First, there are synergies between the two disciplines. An agency with both foreign intelligence and criminal investigative authorities can use the criminal authorities when the intelligence authorities are not available to gather information on suspected terrorists. Sometimes an investigation of, for example, a computer attack, will begin as a criminal investigation because the source of the attack is unknown, and therefore there is no way to make the connection to international terrorism or a foreign actor. Once more is learned through criminal investigation about the source of the attack, a determination might be made to pursue an intelligence investigation. An agency with both disciplines also may have less difficulty with a transfer if a decision is made to end an intelligence investigation and instead pursue prosecution of a suspected terrorist.

Second, many of the tools and techniques used in intelligence collection and law enforcement are similar. The FBI has significant experience with use of the tools and techniques in intelligence collection—electronic surveillance, physical searches, and interrogation, for example. Because of this familiarity, FBI personnel are accustomed to paying attention to the constitutional issues that the

domestic use of surveillance tools raise. In addition, the Attorney General has historically played an important role in approving and overseeing use of these methods.

We believe the FBI should continue to be the entity responsible for domestic intelligence collection for counterterrorism using electronic surveillance and other investigative tools and techniques, and the Attorney General should continue to supervise that collection. The FBI also must be responsible for providing its products to policymakers at the Department of Homeland Security and elsewhere in the national security community.

To perform its counterterrorism intelligence mission effectively, the FBI will have to reorient significantly. The reforms that Director Mueller has instituted will not be enough to overcome the FBI's overwhelming cultural and organizational pull toward its law enforcement mission. Additional reforms are necessary, both to elevate the importance of analysis in the FBI culture and to increase FBI's familiarity and communication with the national security policy community. These reforms should include:

- Bringing people with national security experience into the senior FBI leadership.

- Making it a requirement for promotion that FBI analysts rotate through the Department of Homeland Security or the CIA. In much the same way that the Goldwater-Nichols Act's requirement of "purple" tours transformed the military's attitude toward jointness, this requirement will elevate the value of intelligence analysis among FBI personnel, increase analyst competence, and improve working relationships between FBI personnel and other members of the intelligence community.

- Creating a more attractive professional track for intelligence analysts.

- Revamping training at Quantico to increase focus on terrorism analysis and the uses of intelligence outside of the criminal justice system.

- Hiring more agents and analysts from disciplines other than law enforcement, including some with foreign affairs or national security backgrounds.

- Continue to improve information systems and procedures for sharing information so that information travels not only up to headquarters from local offices, but throughout the FBI system and—just as important—can be accessed by those who need it outside of the FBI.

**Foreign Intelligence Agencies.** CIA and other foreign intelligence agencies are currently prohibited from collecting intelligence on the domestic activities of U.S. persons. Although relaxing this restriction could allow the government more effectively to take advantage of CIA expertise for homeland security, the restriction should be maintained. The CIA and other foreign intelligence agencies are accustomed to collecting intelligence on foreign nationals, but collection on U.S. persons and in the United States involves a range of constitutional protections with which CIA personnel are not familiar. A change that permitted CIA collection on U.S. persons would require changes to culture, procedures, training, and oversight. This could hamper the agency's effective-

ness in collecting foreign intelligence. A decision to give CIA a significant role in collection on U.S. persons would cause discomfort in a public suspicious of this very secretive agency and aware of past abuses by the Agency when it last took on a domestic collection role.

Current law and regulations do permit the CIA to receive, retain and analyze domestic intelligence with a foreign "nexus" that has been collected by the FBI or others. That the CIA does not regularly receive this intelligence is a result of poor procedures and communication, not a legal restriction. This authority should be clarified and procedures developed for effective and timely sharing of that information. Other uses of foreign intelligence agencies for domestic intelligence, such as use of NSA information on U.S. persons collected as part of its foreign intelligence mission, should be examined.

**The President/National Security Council.** Coordination is one of the great challenges for our executive branch. Now more than ever, agencies must work together as a team, rather than act as separate fiefdoms fighting over limited turf, money, and power. There have always been a number of players in the intelligence community; creating a Department of Homeland Security adds a new, very large player. Its presence will do nothing to calm the interagency battles and the jockeying for position in the early days is likely to be intense. Unless there is a strong hand coordinating and leading these departments little that is productive will be accomplished.

Responsibility for this coordination must rest with the President. The President is the only one with clear authority to direct agency action. Since the National Security Act of 1947, the President and the National Security Council have driven the foreign intelligence process and operations—setting priorities and, in the area of covert action, making operational decisions. The President and National Security Council must play a similar role with intelligence collected domestically.

Particularly once the Department of Homeland Security is up and running, a continuing bifurcation in the White House structure between "national security" and "homeland security" makes no sense and would be counterproductive. In the case of terrorism, the homeland threat and the foreign threat are inseparable. To create a coordinating mechanism that institutionalizes this false distinction would not only cause practical and bureaucratic problems, but could result in seams in coverage and coordination that would allow important issues to be missed.

Within the National Security Council interagency process, a reconstituted Executive Committee should be responsible for coordination of the intelligence mission. This group should include the National Security Advisor, the Director of Central Intelligence, the Secretary of Defense, the Secretary of Homeland Security, and the Attorney General. The Director of the FBI should be involved in all the group's meetings. Having this group meet regularly to sort through what inevitably will be myriad management and substantive issues that involve all members of the intelligence community will be critical to effective coordination.

**State and Local Governments.** One fundamental shortcoming with most discussion of organizing for homeland security has been a tendency to focus only on the federal government's role. This is understandable. Difficult as it is to sort through the federal government's structure, the task pales by comparison to the challenge of coordinating more than 50,000 state and local jurisdictions. But an effective national strategy to combat terrorism will have to address this challenge.

Over the next five years, there must be creative thinking about how our federal system will work in an age when coordination and information networks are so important to our security. Without new ideas, the current trend of increasing central control inevitably will continue. The first step should be to focus on how information from states and localities, which is so crucial to the homeland security effort, can reach those in the federal government who need to act on it, and how the federal government's information can reach those on the front line. To be effective at collecting and using all relevant information, the entire national system must work like a network, coordinated at the federal level but controlled locally. Two concrete steps can help start this process. First, states must begin organizing themselves to gather and share information more effectively. Second, the federal government needs one entity responsible for coordinating its role in this effort.

To do their part, states should form task forces or use other methods of coordinating important local information. The state task force formed in Utah in advance of the Salt Lake City Olympics is illustrative of a structure that encouraged input from all relevant entities in the state and established a direct line of communication with interested federal government entities. State and local health, police, and emergency officials worked together with representatives of the INS, FBI, DoD, FEMA, the National Guard and key members of the private sector to coordinate activities and share information. Although this task force was created for a specific event, it was so effective that it is being maintained indefinitely and will be chaired by the state's Director of Public Safety on behalf of the Governor. Other states may choose somewhat different models, but some coordination mechanism that involves all relevant parties in each state—or perhaps involving groups of states—will be essential.

There currently is no coordinated strategy in the federal government for interaction with state and local entities. Although many federal agencies, including the FBI, DoD, and HHS will always have relationships with state and local entities, one agency—the Department of Homeland Security—should take on the responsibility for promoting and coordinating these relationships. The federal government has a responsibility to support state, local, and regional information sharing efforts with funding. With this support must come requirements for interoperable systems and coordinated information-sharing mechanisms. The Department of Homeland Security must establish minimum guidelines and procedures for sharing and impose some order on a system that currently is almost entirely ad hoc.

## Oversight: Protecting Civil Liberties and Sustaining an Effective Homeland Security Mission

The events of September 11 exposed the need for changes to the structures and methods we have used to protect national security. To keep ahead of the new threats requires the government to collect information from a much wider range of sources and share it more broadly. Many of the changes to information collection that have been implemented or proposed—such as collection and mining of data from private sector databases, linking of federal databases, and compilation and use of watch lists—would require lifting traditional protections for civil liberties. Creating a more robust domestic intelligence structure—although clearly necessary—will present increased civil liberties challenges that our current system of oversight is not adequately equipped to address.

The American way of life is a critical part of what our government is protecting when it provides for America's security. An open society and civil liberties are essential components of that way of life. In the past, we have avoided certain structures and practices because they make the potential for government abuse greater. If these restrictions must be relaxed because they interfere with our ability to counter the terrorist threat, we can still be vigilant about protecting liberties. The government must institute a system that sets clear standards, keeps tabs on government action, and holds it accountable for abuses. Moreover, in this new environment, the government must be creative and energetic in pursuing new models for protection of civil liberties.

Too often, civil liberties protections and security are seen as in conflict; more attention to one means the other is shortchanged. In fact, the right guidelines, the right measure of review, and the right process are essential to effective national security decision-making. They allow decision-makers to allocate finite resources and redirect them from ineffective operations or away from activities that sap resources for very little gain.

## An Effective System of Oversight

A system of oversight has three levels of protections: environmental, structural, and transactional protections. To ensure our system is healthy and effective, we must strengthen each level.

**Environmental.** The first category of oversight involves the environment in which the activities exist: the statute or other authorization that establishes the scope of permissible activities and the congressional and executive branch entities that keep tabs on activities.

*Congress.* In the case of homeland security, Congress is taking steps to create a new intelligence agency and there is discussion of new authorities and techniques for collecting and using intelligence. What is missing from this debate so far is how Congress intends to provide oversight for this new intelligence capacity. As it stands, the new Department of Homeland Security will have seven or eight committees in each of the House and Senate looking over its shoulder. It is not clear what this means for oversight of the intelligence/information function. Will the judiciary committees—the committees that oversee law enforcement activities—have jurisdiction over the government's new, more robust collection and analysis function, or will the task go to the two intelligence committees? Will all of these committees claim responsibility for oversight?

Congress has a responsibility to clarify its own process. When too many congressional committees have oversight responsibility, we end up with both too little and too much. There is insufficient institutional expertise in any committee to review and assess the effectiveness of a system on an ongoing basis, but when something goes wrong every committee wants to be involved in investigating and assessing blame.

Congress should simplify its oversight of homeland security. The ideal approach would be to form standing committees on homeland security. Difficult and disruptive as this would be for Congress, it is no more than is being asked of the Executive Branch and it is the only way to assure sensible, effective congressional oversight and responsibility. If Congress does not elect to form standing committees, at the very least it should create select leadership committees with the responsibility to

oversee all agencies and activities involved in intelligence/information collection and analysis for homeland security. These committees would include the chairpersons and ranking members from the committees and subcommittees that now exercise oversight over the various agencies involved in homeland security.

*The Executive Branch.* Even if Congress acts to improve its oversight, there are limits to what it can accomplish. It is necessarily removed from management of the programs it oversees. In addition, in the area of oversight, the culture of the legislative branch is, more often than not, reactive. This argues for some environmental oversight mechanism within the Executive Branch. The President can provide this by instructing his Foreign Intelligence Advisory Board's Intelligence Oversight Board (PFIAB/IOB) to conduct periodic reviews of the newly strengthened domestic intelligence apparatus to ensure standards are consistent, training and compliance are adequate, and guidelines are performing their intended function. This kind of periodic review can identify problems before they result in serious abuse. The PFIAB/IOB is particularly suited to this mission. It reports directly to the President, has long experience with overseeing intelligence operations on the President's behalf, and would have access to intelligence operations and products that other bodies, even within the Executive Branch, would be denied.

**Structural.** Structural oversight involves the internal mechanisms and ground rules for guiding the conduct of activities. The most important elements of structural oversight are standards or guidelines and training.

*Guidelines.* An effective system to protect against abuse requires clear, uniform standards for behavior. If they are clear and consistent, guidelines empower more than they constrain. Fear of crossing the line into prohibited behavior causes timidity. If workers are comfortable that they know what is permitted and what is not, they will be more likely to take action. Development of guidelines should be an immediate priority for the Administration and the Department of Homeland Security. The kind of direction and structure that guidelines provide are particularly important now, given the range of new or increased intelligence activity that is being contemplated. In particular, the Administration must act quickly to establish guidelines for activities such as acquisition of private sector data, use of government databases, analysis of personal data, and development and use of watch lists.

These guidelines should be developed in close consultation with Congress and, to the maximum extent possible, with public involvement. Acting alone is quicker, but legitimacy and acceptance of the resulting product is strengthened when guidelines are developed in a transparent, consultative fashion. Changes to guidelines should be handled in the same way. It is essential that the domestic intelligence system have the confidence of the American people. That will not happen if guidelines are developed and changed under a cloud of secrecy.

*Training.* Standards and guidelines will serve little purpose if employees do not understand them or never learn to apply them to their duties. The Department of Homeland Security should develop and implement quickly training programs in uses of personal and private sector data and other domestic analysis activities. The FBI should also revamp and improve its training on domestic intelligence collection and analysis. Training on standards and guidelines should be an integral part of training for the intelligence mission and should be updated regularly.

*Other Structural Protections.* An important task for the Department of Homeland Security will be to seek out new, creative ways to build structural protections for civil liberties. Technology has the potential to advance privacy in a number of ways. For example, authentication procedures, including use of biometric identifiers for authentication, and methods of tracking access to information systems can increase accountability by recording who sees personal information. Automated information processing techniques can keep information out of the hands of government personnel or others unless it is absolutely necessary. Information can be aggregated or anonymized where appropriate to protect confidentiality. The Department of Homeland Security should review these measures and others like them and employ them in handling private and confidential information.

**Transactional.** Transactional oversight is the way the system deals with individual cases. This includes how permission is obtained to take action and investigation of errors.

*Investigation of failures and abuses.* This is the most familiar element of a system of oversight. It is important that when abuses are discovered they be investigated impartially and that responsible officials be held accountable. But a system is weak if it places too much emphasis on investigation of problems as they occur, rather than routine and periodic review of effectiveness. Investigations are prone to politicization and tend to focus on finding individual culprits. Excessive attention to individual wrongdoing causes timidity in those carrying out their duties because the consequences of errors are so professionally devastating. Scandal-driven solutions are often narrow and ultimately ineffective solutions aimed at only one piece of the problem. It can be a failing of congressional oversight that it focuses more on politicized investigation of errors than periodic review of the effectiveness and strength of a system. Similarly, inspectors general who are not integrated into an agency's decision making or structure often have little voice or stake in maintaining a healthy system and can focus excessively on exposing individual wrongdoing.

A healthy system of transactional oversight will include officers, such as Inspectors General, who can conduct impartial investigations and audits when necessary. But it should also include people integrated into the line offices who can guide and review the way decisions are made on an ongoing basis to prevent failures, not punish them.

The Department of Homeland Security will have an Inspector General and a Privacy Office. It may also have a Civil Rights and Civil Liberties office. The roles of these offices should be spelled out and deconflicted. Only one—the Inspector General—should be charged with investigation of failures or abuses. The others should focus on developing guidelines and training programs and should be integrated as much as possible into the day-to-day work of the intelligence directorate and other offices to promote practices consistent with guidelines, not to punish errors.

# Part Three:
# SELECTED
# BACKGROUND RESEARCH

# A Primer on the Changing Role of Law Enforcement and Intelligence in the War on Terrorism

**By Robert M. McNamara, Jr.**
**Partner, Manatt, Phelps and Phillips, LLP**

## Introduction and Executive Summary

While the "War on Terrorism" has taken on a new urgency since September 11, 2001, it is not a new phenomenon nor is it a reinvented focus of either the U.S. intelligence community, or the federal law enforcement agencies. What is relatively recent, however, is the scope of effort by both groups in terms of human resources committed to the task, the level of sophisticated technology focused against the target(s) and the unparalleled, albeit evolving, nature of cooperation and coordination between the two communities.

For the past few years, there have been repeated calls for closer cooperation, better sharing of information and less friction. While to the outside objective observer, these suggestions seemed both reasonable and doable, there were practical, cultural and legal impediments, which prevented what should have been a seamless continuum from becoming so. The two drive wheels for change in the status quo were George Tenet, Director of Central Intelligence and of the Central Intelligence Agency (CIA), and Louis Freeh, Director of the Federal Bureau of Investigation (FBI). By all accounts, they accomplished more in the past half-decade toward this goal, than had been done in all of the history of their respective agencies.

There were a number of critical factors in this equation of change: necessity, maturity and urgency, to name a few. But the overriding single most important ingredient was the shared belief that things had to change and the unequivocal commitment of both Directors that things were going to change. Each may have had his own reasons for pulling hard on their respective oars, but both were convinced that the alternative—the status quo—was not an option. In fact, the status quo would, in the end, fail the country and its citizens in time of greatest need.

This is not to say that everyone in both agencies was immediately converted or that a residuum of insularity did not exist, and that total transparency was achieved. In fact, that was not the case—and as a recent preliminary report of the House Intelligence Committee investigating the tragedies of September 11 indicates, it is still not the case. But the situation is so much beyond where it was before. The momentum for change is not merely being maintained, but actually it is being accelerated by Director Tenet and the new head of the FBI, Director Robert Mueller.

Before the Task Force can begin to think about the new cooperative law enforcement and intelligence environment, especially when focused on terrorism, it is important to understand where both came from. Each had a totally different mission, was grounded by a different culture, was circumscribed by different laws and authorities and was constrained by different limitations. Within the past quarter-century, both communities have been the subjects of scathing congressional investigations, which had uncovered numerous abuses of the rights and freedoms of Americans. As a result, laws were passed, guidelines were issued and policies were established, which defined the

focus of the respective communities and may have inadvertently contributed to an environment in which each looked out for itself, and neither saw either a value or a need to develop a coordination mechanism in order to accomplish their respective work.

## The Law Enforcement Environment

### Jurisdiction

When we think of "law enforcement" as a concept, we generally think of it in terms of the cop on the street, but obviously it is much broader than that. It not only includes the dozens of federal law enforcement agencies, but also the nearly 700,000 state and local police and peace officers throughout the country. Each of these entities is defined, in the first instance, by the scope of their respective authority. In some cases, there may be an overlap; for instance, nearly all may have arrest authority for various types of illegal drug activity. In other cases, the FBI and the local police may have concurrent authority, such as in a bank robbery case, but the rule of thumb is "the FBI gets it unless they decline it."

Federal law enforcement authority is also defined by jurisdiction, which in turn is circumscribed by its mission, and in most cases arises out of it. For instance, the U.S. Customs Service is responsible for collecting tariffs and duties on goods entering the United States and for ensuring that illegal or prohibited products are excluded or seized. The normal day-to-day responsibility for carrying out this mission falls to the Customs Inspectors, but when illegality is uncovered or suspected, the situation shifts from being a trade matter to becoming a criminal investigation, and Customs Special Agents assume responsibility for handling the case.

The law enforcement investigative authority of that Customs Special Agent, however, is limited by the scope of the mission of the U.S. Customs Service. The Customs Special Agent, for instance, would have no authority to investigate a murder in a national park. Investigative authority for that crime would fall to the U.S. Park Police, which is the law enforcement component of the U.S. Park Service, wherein the same duality exists, as it does in most federal departments, which have regulatory and enforcement components.

The FBI has the broadest law enforcement jurisdiction of any federal law enforcement agency. Its 11,500 Special Agents have nationwide jurisdiction and authority to investigate any federal crime, which is not otherwise within the exclusive jurisdiction of another federal agency, *e.g.* the U.S. Customs Service (for importation crimes), or the U.S. Secret Service (for counterfeiting crimes). As a matter of reality, however, federal jurisdiction may lie with multiple agencies because the criminal activity may involve the violations of multiple criminal laws. In those instances, one agency becomes the "lead agency" for the case, and the others provide assistance as needed for a successful investigation and subsequent prosecution.[1] Because of the FBI's predominance in federal criminal investigations, it will be the focus of this paper.

### Mission

The basic criminal investigative mission of the FBI is to detect and investigate criminal activity, which violates one or more of the hundreds of federal criminal laws found in the United States

Code, primarily in Title 18.[2] The focus can be a specific crime, like a bank robbery, or a pattern of activity, such as an interstate car theft ring, or a criminal enterprise such as an organized crime group or a terrorist organization. The common thread is the underlying criminal activity that has been, is being or is about to be committed.

## Methodology

The FBI's focus is to investigate the criminal activity, to identify those involved, to collect evidence sufficient to prove the criminal activity beyond a reasonable doubt, and to assist the Department of Justice attorneys in the prosecution of those charged. The collection of evidence is the single most important function in this sequence for two reasons; it must be collected lawfully and its integrity (the so-called "chain of custody") must be maintained. If either of these criteria is faulty, the evidence may be excluded from trial and the suspect may go free as a result.[3]

The nature of the evidence collected and the manner in which it is collected can be subject to a spectrum of legal requirements and constraints. Physical evidence in a public place is generally subject only to chain of custody requirements so that it can be introduced into evidence. Physical evidence in a private place, such as a home, is protected by the Fourth Amendment to the Constitution. The FBI usually must get a search warrant from a federal magistrate to search the premises and seize the specific property, although over the years the Supreme Court has carved out a number of exceptions to the warrant requirement, *e.g.,* for items "in plain view" and for "exigent circumstances."[4] Nor is the FBI allowed to search persons, whose privacy is also protected by the Fourth Amendment. However, the Supreme Court has held that a reasonable articulation of criminal activity would justify government action when the intrusion on individual privacy is minimal and outweighed by an important governmental interest.[5] As with searches of property, the Supreme Court has also defined instances in which a warrantless search of a person is permitted, such as searches incident to arrest and searches at fixed checkpoints.

Separate rules apply to interviews conducted by the FBI. If the person is merely a witness to a crime, the law does not require any specific procedure, but if the person is a material witness in an investigation and there is a concern the person may flee the jurisdiction, the FBI can obtain a material witness warrant from a federal judge, and the individual can be detained. Similarly, the FBI is not required to give a person, who is merely fact witness or an eyewitness, any specific warnings. However, if the person is a suspect, he is entitled under the Fifth Amendment to the Constitution to the so-called *Miranda* warnings, and he cannot be forced to incriminate himself or to speak without a lawyer being present to advise him, if he so wishes. These rights, however, can be waived. Lastly, the FBI must respect privileged relationships, such as husband-wife, psychotherapist-patient, and attorney-client, and not attempt to interfere with them.

## Investigative Techniques

The FBI has its own internal procedures and policies for when it initiates a preliminary inquiry, how long it can be opened, who must approve it and what type of investigative techniques can be used during the course of it. As will be discussed, the internal constraints on the FBI are even more restrictive if the person or group is the subject of a domestic terrorism investigation, which could impact on otherwise protected First Amendment activities.

In addition to the forensic evidence, which may be collected at a crime scene and analyzed for possible use at trial, the FBI could obtain evidence in a variety of methods. A classic source of information is informants, some of whom are paid and others who are volunteers. The FBI has developed detailed procedures for approval and use of such persons, which each Special Agent must follow. Undercover FBI Special Agents, who infiltrate suspected criminal groups or enterprises, are the most valuable because of their training and their credibility on the witness stand. Undercover operations are among the most time-consuming and resource-intensive of the techniques, and some of the most creative. Some undercover operations have become extremely sophisticated, and may involve long-term business proprietaries, which are subject to very strict internal approval, accounting and oversight requirements.[6]

Except for the use of confidential informants and undercover agents or operations, many of the sensitive investigative techniques used by the FBI require the intervention of a court for a warrant or grand jury for a subpoena. The FBI must go to a federal judge in order to obtain a search warrant, a wiretap warrant, authorization for a pen register or a trap-and-trace device. The FBI must obtain a grand jury subpoena for a suspect to give hair, blood, saliva, or voice samples or for authority to obtain certain types of financial, medical or educational records, which are protected by various privacy statutes. It must also use the grand jury's powers to force an unwilling witness to testify, especially if that person has been granted immunity from prosecution.

The FBI may also obtain information and records from other federal agencies, such as the Securities and Exchange Commission or the Federal Deposit Insurance Corporation, to aid in the criminal investigation. These and other agencies require that certain reports be filed and often have taken administrative deposition of witnesses. Other federal law enforcement agencies, such as the U.S. Postal Service or the U.S. Border Patrol, may have information about an individual who is of investigative interest to the FBI. A few years ago Congress passed a statute that authorizes the CIA and certain other members of the intelligence community to collect information for the FBI overseas against a non-U.S. person for purposes of a criminal investigation.[7]

Although the FBI has prided itself over the past decade as being a "proactive" law enforcement agency and has, in fact, numerous examples of where it has stopped crimes before they have occurred—especially in the context of undercover operations—it has been primarily a reactive agency. A large percentage of its 11,500 special agents, who are located in 56 major field offices, 400 resident offices and 44 overseas locations, are investigating crimes that have already been committed. These investigations are focused and finite, are subject-specific and prosecution-oriented. In the end, the investigative process and the investigative product will be transparent, and any relevant information, document and witness—including possibly an informant or protected witness—will be exposed to the light of day and open testimony in a criminal courtroom before a judge, a jury and the public-at-large. Unless the FBI intends to use a plea agreement or a lesser sentencing arrangement with a convicted defendant in order to work up to the next level of the criminal "food chain," at the end of the trial, the work of the FBI is generally over, although the case will remain open until any appeal rights have been exhausted.

## Domestic Terrorism Investigations

The late 1960's and early 1970's were a politically and socially turbulent time for the country. The country was involved in a distant war, which a significant number of Americans opposed. The civil rights movement was developing its own momentum, and there was little tolerance for racial intolerance. In addition, there was an increase in urban crime and an increase in violence. According to the FBI, in 1970 alone, there were an estimated 3,000 bombings and 50,000 bomb threats that occurred in the United States. In response, the FBI initiated its now-infamous counter-intelligence program (COINTELPRO) to counteract domestic terrorism and conduct investigations of individuals and organizations that espoused violence, especially against the government. Some COINTELPRO targets, such as the National Organization for Women and several environmental groups were not, however, linked to violent activities.[8]

At the time, the FBI had no specific guidelines for conducting domestic terrorism investigations, and it was not until 1968 that its Special Agents were required to get a judicial warrant in order to conduct electronic surveillance. Congressional hearings in the mid-1970's found that the FBI had monitored, infiltrated, and often internally disrupted lawful civil rights and anti-war organizations, whose members were exercising their protected First Amendment rights. As a result of hearings, in 1976 Attorney General Edward Levi issued one set of guidelines for foreign counter-intelligence investigations and another set for domestic security investigations (which were later superceded in 1983). After the Oklahoma City bombing, the FBI, under Director Freeh, tried to get the self-imposed limits loosened in domestic terrorism matters, but senior officials in the Administration strongly objected and refused to allow them to be amended.

On May 30, 2002, Attorney General John Ashcroft amended these guidelines, which he said "have hampered our ability to fight terrorism." He criticized some of the guidelines, which, he said, "provide limitations and guidance over and above all requirements and safeguards imposed by the Constitution and beyond the legal framework established by federal statutes enacted by Congress." The new guidelines announced by the Attorney General[9] changed the way domestic terrorism investigations were initiated, the length of time they could be open, the type of investigative techniques that could be used and the use that could be made of the information collected. Most notably from a privacy perspective, the guidelines now allow FBI Special Agents to gather information from commercial databases and the worldwide web without having to justify their actions as being part of an ongoing criminal investigation. While the new rules provide more latitude to special agents and more discretion in the field by allowing lower levels of approval, it will remain to be seen whether they have a significant—or any—impact on the FBI's ability to conduct terrorism investigations or prevent terrorist activities.

## Counterterrorism

Although domestic terrorism incidents decreased dramatically in the 1980's, foreign terrorism did not. In 1982, in response to a number of terrorism incidents worldwide, then-Director William Webster made counterterrorism a fourth national priority of the FBI.[10] In 1986 Congress expanded FBI jurisdiction to cover terrorist acts against U.S. citizens in foreign countries. In 1989, the Justice Department authorized the FBI to arrest terrorists, drug traffickers and other fugitives abroad without the consent of the foreign country in which they resided.[11] As crime became more

global and criminal enterprises became more international, the FBI has expanded its presence overseas. In the mid-to-late 1990's, Director Freeh was involved in developing closer international cooperation with foreign law enforcement agencies, expanded the number of Legat (Legal Attaché) offices to 44 countries and created a new Counterterrorism Division.

In June of this year Director Mueller announced the reorganization of the FBI, and one area of significant restructuring and expansion was the Counterterrorism Division. One of the main reasons given for this was the fact that greater collaboration between law enforcement and the intelligence community required more resources. A repeated theme was the need to improve collaboration and information sharing, and one of the methods to accomplish that goal was to duplicate the FBI's Strategic Information Operations Center (SIOC) environment within the Counterrorism Division. SIOC is an inter-agency, collaborative environment where information flows quickly among all participants.

## Disclosure of Information to the Intelligence Community

As noted above, most of the information collected by the FBI—even in domestic terrorism investigations—related to the commission of one or more specific crimes by one or more specific individuals. Unless the investigation dealt with espionage or involved some intelligence equity, the intelligence community was generally not interested, and it especially did not want information about U.S. persons. On occasion the intelligence community was asked to do an archival file search to determine whether it had any information about the suspect that might be of investigative interest.

The information that was shared with the intelligence community was that for which there was a foreign intelligence value. For instance, the FBI can share with the intelligence community information it collects pursuant to an intercept or a search authorized by the Foreign Intelligence Surveillance Court, because it is deemed to be foreign intelligence. However, information obtained during the course of a grand jury investigation or intercepted pursuant to a court-authorized criminal wiretap could not be shared with the intelligence community because of legal prohibitions, even if the content of the intercepted communication related to terrorism.

The FBI's inability to provide these types of terrorism-related information to the intelligence community was the subject of numerous meetings with the Justice Department during the past couple of years, which, before September 11 opposed a statutory fix that would have authorized the disclosure of such information to the Intelligence Community. The Department's principal concern was protecting the integrity of criminal investigations. But the prohibition also protected privacy interests—with the information available to only a small number of persons there was little likelihood that embarrassing personal information developed by a grand jury probe would be leaked to the public. The information disclosure issue was resolved, however, with the passage of the USA PATRIOT Act, which authorized both wiretap and grand jury information to be provided to "any federal law enforcement, intelligence, protective, immigration, national defense or national security official" for the performance of his official duties.[12]

## The Intelligence Community

### Structure

The "intelligence community" is a term defined in Section 3 of the National Security Act of 1947, and over the years that definition has been amended to include new components, the most recent addition being the U.S. Coast Guard. In addition to the Office of the Director of Central Intelligence, it includes: the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency (which includes the Defense Humint Services); the National Imagery and Mapping Agency; the National Reconnaissance Office; the intelligence elements of the military services, the FBI, the Departments of the Treasury and of Energy; the Bureau of Intelligence and Research at the Department of State; and other designated offices, including certain ones at the Department of Defense involved in the collection of specialized national intelligence. Each of these entities has a highly specific mission within the national security arena and a specific role with respect to the collection of intelligence related to national security.

### Mission

The mission of the intelligence community is to support the President, the National Security Council and all U.S. officials who make and execute the U.S. national security policy. This is done in two ways primarily: first, by providing accurate, comprehensive and timely foreign intelligence on national security topics; and second, by conducting counterintelligence activities, special activities, and other functions related to foreign intelligence and national security, as directed by the President. Foreign intelligence, in this context, is defined as "information relating to the capabilities, intentions or activities of foreign governments or elements thereof, foreign organizations, or foreign persons."

### Methodology

The process by which information is acquired, converted into intelligence, and made available to policymakers is called "The Intelligence Cycle." "Information" is raw data from any source, including open source. It may be fragmentary, contradictory, unreliable, ambiguous, deceptive or wrong. "Intelligence" is information that has been collected, integrated, evaluated, analyzed and interpreted. "Finished intelligence" is the final product of the Intelligence Cycle ready to be delivered to the policymaker.

Individually, each member of the intelligence community may collect information in the course of executing its own mission, such as collecting imagery, or communications, or military intelligence. What is critical is that this information be shared and integrated into a common understanding. To facilitate this effort, fusion centers have been created, which provide for multi-disciplinary analysis of priority national security issues, such as nonproliferation, counterterrorism, counterintelligence, international crime and narcotics trafficking. By bringing the best resources of each of the intelligence community components together, by providing complete access and transparency to all-source information and by subjecting the intelligence product to increased, multi-dimensional critique, the best finished intelligence is created for the President and the policymakers.

## Sources and Methods

The collection of foreign intelligence is accomplished through a variety of techniques—the most important of which are referred to as "INTs." Human sources (HUMINT) can be the most productive, depending on the nature of their access to information. They may be witting or unwitting, paid assets or volunteer walk-ins, long-term or one-time. Their level of access and their level of credibility will define the quality and reliability of the information they provide.

Imagery (IMINT), at one time, was the sole province of governments, especially the U.S. Now commercial imagery is available to the buying public, and, in fact, even to the intelligence community. Different types of satellites and aircraft can provide varying qualities of imagery product to meet the needs of the policymaker or the warfighter. Both governmental and commercial imagery is now being used to assist U.S. government agencies, such as the Federal Emergency Management Agency or the Department of Interior, in visualizing the extent of damage from disasters and in planning for the next steps to be taken.

Interception of foreign communications (SIGINT) often gives the best information regarding the plans and intentions of the speaker, his organization or his government. Over the past half-decade, this technique has become challenged by innovations in technology and encryption, as well as the linguistic challenges of new intelligence targets. While there are no constraints on targeting non-U.S. persons outside the United States, if a U.S. person (which includes a "green card" holder) is the target of an electronic intercept overseas because of his suspected terrorist activities, the Attorney General must approve the interception for foreign intelligence purposes, and will do so only for limited periods of time. If part or all of the conversation to be intercepted occurs in the U.S., the Government must show that the target is an "agent of a foreign power"[13] and request the Justice Department to petition the Foreign Intelligence Surveillance Court for electronic surveillance authority—a very time-consuming process.

Other intelligence collection mechanisms and platforms (*e.g.*, MASINT) focus on the more intangible aspects of information and may measure radiation levels, or identify chemical and biological concentrations, or capture electronic emissions. Regardless of the form or the method used, the end product of every technique is "information," and this information is put into the intelligence cycle in order to produce a finished product which has been integrated, analyzed and, to the extent possible, validated, so that policymakers can understand what is happening in important areas of the world and make informed decisions.

An important source of information is foreign liaison relationships, which are forged with foreign intelligence services worldwide. The nature and depth of these relationships vary country-by-country, and often, but not always, reflect the foreign policy compatibility the U.S. Government has with the respective foreign government. Some of these relationships are time-tested and enduring, and others are creatures of necessity and suspicion. In recent years, the CIA's relationship with the Israeli and Palestinian intelligence services became obvious, when Director Tenet was asked to play an overt role in the Wye Accords, because both intelligence services trusted and respected him.

One of the most closely held—and most highly classified—techniques is covert action. A covert action is an activity designed to influence political, economic, or military conditions abroad, where

it is intended that the role of the U.S. government will not be apparent or acknowledged publicly. A proposed covert action reflects a policy decision of and recommendation by the National Security Council (NSC). Covert action is considered when the NSC judges that U.S. foreign policy objectives cannot be fully realized by normal diplomatic means and when military action is deemed to be too extreme.

Covert action can only be undertaken after the President issues a written finding, in which he must find that such an action is necessary to support an identifiable foreign policy objective and is important to the national security of the United States. A presidential finding cannot authorize a covert action that has already occurred, cannot violate the U.S. Constitution or federal law, and cannot be intended to influence U.S. political process, public opinion, policies or media. The National Security Act of 1947 sets forth specific notification requirements, which enable the House and Senate Intelligence Committees to exercise appropriate oversight of the these covert actions.[14]

## The FBI as a Member of the Intelligence Community

Although the FBI is primarily a law enforcement agency, its Counterintelligence Division has long been deemed part of the intelligence community. The Division focuses on activities conducted or sponsored by foreign powers within the United States—the National Security Act defines counterintelligence to be "information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities."[15] During the Cold War, the FBI devoted the vast majority of its counterintelligence resources to monitoring the activities of Soviet Bloc intelligence services within the United States. Monitoring foreign intelligence operations remains an important FBI mission, but, with the end of the Cold War, the FBI's counterintelligence focus has broadened to encompass involvement of foreign states in terrorism, proliferation of weapons of mass destruction, economic espionage, and the targeting of the national information infrastructure.

Even within the FBI, the cultural distinction between the intelligence and law enforcement communities is evident. In contrast to most FBI components, the principal focus of the Counterintelligence Division has not been the arrest and conviction of violators of U.S. law. Because its responsibility encompasses the official actions of sovereign foreign states, the Division has generally deemed its mission to include collection of information about foreign intelligence activities and the prevention and deterrence of unfriendly actions by foreign governments within the United States.

Despite the unique culture and objectives of the Counterintelligence Division, the separation between the FBI's law enforcement and counterintelligence functions has never been airtight. Most notably, counterintelligence investigations have often led to espionage prosecutions. The distinction between the FBI's law enforcement and intelligence community roles will likely continue to blur in coming years with the increased focus of all FBI components on combating international terrorism and increased information sharing between the intelligence and law enforcement communities on terrorism-related matters.

In carrying out its counterintelligence and counterterrorism missions, the FBI often engages in electronic monitoring or covert physical searches, as authorized by the Foreign Intelligence Surveillance Act (FISA).[16] The Act permits the Foreign Intelligence Surveillance Court—comprised of eleven district court judges selected by the Chief Justice of the United States—to authorize surveillance that targets agents of foreign powers. This includes international terrorist organizations, without the need to establish probable cause to believe that criminal activity is or has occurred—the standard which must be met for law enforcement searches or electronic intercept warrants.[17] Courts have allowed evidence gathered pursuant to FISA orders to be used in criminal prosecutions.[18] But a recent decision by the Foreign Intelligence Surveillance court rejected an effort by the Justice Department to increase the access of prosecutors to information gathered under FISA.[19]

Until recently FISA orders could only be issued if the government could demonstrate that the "purpose" of the surveillance was to collect foreign intelligence. This language created problems, particularly in terrorism cases where surveillance might be for the dual purpose of collecting intelligence and obtaining evidence for criminal prosecutions. The USA PATRIOT Act modified FISA to allow FISA orders to be issued where "a significant purpose of the surveillance is to obtain foreign intelligence information." Some critics have challenged the constitutionality of this language, arguing that it allows the government to collect evidence for criminal prosecutions while avoiding the strictures of the Fourth Amendment. Eventually, this issue may need to be decided by the Supreme Court.

FISA does not apply to searches conducted outside the United States, and it is unclear the extent to which Fourth Amendment protections apply to U.S. persons overseas. Currently, intelligence collection that targets Americans overseas is governed by the Reagan-era Executive Order 12333.[20] The Order provides that intelligence agencies may "collect, retain or disseminate information concerning United States persons only in accordance with procedures…approved by the Attorney General."[21] It prohibits "[p]hysical surveillance of a United States person abroad to collect foreign intelligence, except to obtain significant information that cannot reasonably be acquired by other means" and mandates that when intelligence agencies do legitimately target U.S. persons they "use the least intrusive collection techniques feasible."[22] The order envisions that electronic surveillance of U.S. persons overseas will only occur with the approval of the Attorney General and that such approval will only be given if the Attorney General determines that the U.S. person is the agent of a foreign power.[23]

### Disclosure of Information to Law Enforcement

Because of the way information is collected and because of the sensitivity of the intelligence that is produced, both the process and product are classified at various levels. These levels are determined by the extent of damage that would be done to the national security if the source, the method, the information or the analysis were made public. Some sources are single-threaded and identifiable; some operational methodologies are easily compromised; some collection platforms are irreplaceable; and some networks—human and cyber—are very fragile. Consequently, in additional to having the required clearance and in some cases, having authorized access to the specific compartment, everyone who gets access to any piece of classified information, regardless of its level, must also have a "need to know" that piece of information. The two-pronged requirements of required clearance and need-to-know complicate information sharing.

The intelligence community has developed a number of solutions so that "actionable intelligence" can be made available to law enforcement agencies. One approach is simply to downgrade the level of classification by sanitizing or redacting the most sensitive portions of the intelligence. In many instances, law enforcement may not need to know the source of the information or the method used to obtain it, but rather will use it as a "lead" to further evidence. This intelligence, which is generally still at the SECRET level, is passed to a special unit at the headquarters of the federal law enforcement agency, which removes all references identifying the intelligence community as the source of the information. The headquarters unit then transmits the information to the appropriate field office as an investigative lead to be followed-up. If a prosecution results, only the evidence developed by the field office is relevant and admissible, not the lead. At the moment, there is no procedure to make such information routinely available to state and local law enforcement agencies.

Another approach is similar to the FBI's SIOC: all-source Centers, in which cleared federal law enforcement personnel sit side-by-side with intelligence community personnel and have access to the same raw data and finished intelligence. They are able to determine what information needs to be shared with their respective agencies and with what degree of specificity. In some of these Centers, such as the Counterterrorist Center, the Deputy Director is a senior FBI Special Agent, who has transparency to all information and operations.

### Collaboration with Law Enforcement

Director Tenet and Director Freeh made it a priority for the FBI and CIA to cooperate and collaborate with each other. They developed a senior-level group, which met regularly, called the "Gang of Eight." It was composed of both Directors, their General Counsels, their Executive Directors (who ran their respective agencies day-to-day) and the heads of the FBI's Criminal Division and the CIA's Directorate of Operations. A basic premise was that problems of coordination and cooperation were to be identified and solved not ignored. As a result of these meetings, joint training was conducted, tradecraft was shared, specialists were detailed to each other's agency and senior officials were exchanged. An outgrowth was the Chief of Station—Legal Attaché conferences, which were held all over the world. These conferences brought the law enforcement and intelligence counterparts together for a couple of days, and they worked together to resolve scenarios, the goal of which was to ensure that the investigation was not compromised and that the intelligence could be exploited in a timely fashion.

## Conclusion

Cooperation and collaboration between law enforcement and the intelligence community will always be a work in progress; it will never be seamless or perfect. The situation will become more complex and complicated when the new Department of Homeland Security is established because, by law, both the FBI and the CIA will be required to share intelligence (but not necessarily "raw data") with the new Department. Perhaps what both have learned from experience will obviate the need for history to repeat itself.

## Endnotes

[1] Executive Order No. 11396 designates the Attorney General to facilitate and coordinate the criminal law enforcement activities and crime prevention programs of all federal departments and agencies.

[2] Other titles of the U.S. Code also contain criminal prohibitions, some of which are investigated by specific federal agencies: Title 21, chapter 13, contains drug offenses investigated primarily by DEA; Title 26, chapter 53, contains firearm offenses investigated primarily by the Bureau of Alcohol, Tobacco & Firearms; and Title 31, chapter 53, contains Bank Secrecy Act offenses investigated primarily by the Internal Revenue Service.

[3] There is a whole body of rules, procedures and case law applicable to the admissibility and use of certain types of evidence at trial, about which FBI Special Agents must also be knowledgeable. See Federal Rules of Evidence.

[4] Other exceptions would include consent searches, vehicle searches, container searches, inventory searches, border searches, searches at sea, administrative searches.

[5] *See Terry v. Ohio,* 392 U.S. 1, 21 (1968), from which developed what is referred to as the *Terry* stop for questioning and the Terry frisk for weapons.

[6] In order to conduct undercover operations, the FBI needed exemptions from numerous federal contracting, fiscal and property statutes as well as authority to use income to offset expenses of the proprietary so that it could be a self-sustaining business. *See* Public Law 98-411, § 203(b); 98 Stat. 1545, at 1559.

[7] *See* National Security Act of 1947, § 105A, 50 U.S.C.403-5a. This provision was enacted in order to counter the CIA's assertion that it could not collect such information unless the "primary purpose" for such collection was a foreign intelligence one.

[8] Electronic Privacy Information Center, "The Attorney General's Guidelines," http://www.epic.org/privacy/fbi/.

[9] The text of the new guidelines is available at http://www.usdoj.gov/olp/generalcrimes2.pdf.

[10] Director Webster also expanded FBI efforts in the three other priorities: foreign counterintelligence, organized crime and white-collar crime.

[11] It remains to be seen whether this authority will continue to be viable after the decision by the Ninth Circuit Court of Appeals last year in *Alvarez-Machain v. United States,* 96 F.3d 1246 (9th Cir. 2001), where the court held that a Mexican doctor, who had been abducted from Mexico and turned over to the Justice Department to be prosecuted for the torture and murder of a DEA agent, could sue the United States under the Federal Tort Claims Act on a claim of "false arrest" and could sue anyone who had assisted in the abduction, including other Mexicans, under the Alien Tort Claims Act. This case is now scheduled for rehearing en banc by the 9th Circuit. *Alvarez-Machain v. United States,* 284 F.3d 1039 (March 20, 2002).

[12]Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, P.L. 107-56, § 203; 115 Stat. 272, at 278 (2001).

[13] This term is defined in the Foreign Surveillance Act of 1978, § 101(b), 50 U.S.C. § 1801(b).

[14] National Security Act of 1947, § 503(b)-(c), 50 U.S.C. § 413b(b)-(c).

[15] 50 U.S.C. § 401a(3)

[16] Pub. L. 95-511, 92 Stat. 1783 (1978) (codified, as amended, at 50 U.S.C. 1801 et seq.).

[17] During 2001 the Foreign Intelligence Surveillance Court approved a total of 934 FISA intercept or covert search orders. Larry D. Thompson, Acting Attorney General, Letter to L. Ralph Meacham, Director, Administrative Office of the United States Courts, April 29, 2002 available at http://www.fas.org/irp/news/2002/04/fisa01.html. The court modified the language of two of the requested orders, but no request was rejected during the year. In contrast, 1,491 conventional law enforcement wiretaps were authorized during 2001. Administrative Office of the United States Courts, 2001 Wiretap Report, table 2, http://www.uscourts.gov/wiretap01/table201.pdf.

[18] *See, e.g., United States v. Ott,* 827 F.2d 473 (9th Cir. 1987)

[19] *In Re All Matters Submitted to the Foreign Intelligence Surveillance Court,* U.S. FIS Ct., May 17, 2002. *See also,* D. Eggen and S. Schmidt, *Secret Court Rebuffs Ashcroft, Washington Post,* August 23, p. A1.

[20] The full text of Executive Order 12333 is available at http://www.cia.gov/cia/information/eo12333.html#1.9.

[21] E.O. 123333 at ¶ 2.3.

[22] *Id.* at ¶¶ 2.4 & 2.4(d).

[23] *Id.* at ¶ 2.5.

# Legal Authorities for "All-Source" Domestic Intelligence

**By Daniel R. Ortiz**
**John Allan Love Professor of Law and**
**Joseph C. Carter, Jr., Research Professor**
**University of Virginia School of Law**

In the wake of September 11, many have started to rethink the present allocation of the nation's intelligence responsibilities. Some feel that the current structure overly compartmentalizes intelligence functions and unduly restricts the kinds of information certain agencies can receive, thereby hobbling the country's ability to respond to terrorism. Others feel just as strongly that centralizing intelligence authority and easing government access to information would threaten civil liberties. This report takes no position on this important debate. Policy, not law, should drive it. Rather, this report discusses where under existing law Congress could place an all-source authority for the collection or analysis of intelligence on terrorism if it wanted to create one.

Congress has two options. First, it could create a new agency and endow it with all-source authority. The proposed Homeland Security Act, in fact, aims far in this direction. The House bill, for example, charges the Under Secretary for Information Analysis and Infrastructure Protection broadly with:

> (1) Conducting analysis of information, including foreign intelligence and open source information, lawfully collected by federal, state and local law enforcement agencies and by elements of the intelligence community with respect to threats of terrorist acts against the United States.
>
> (2) Integrating information, intelligence and intelligence analyses to produce and disseminate infrastructure vulnerability assessments with respect to such threats.[1]

And it allows the Secretary:

> Access to all reports, assessments, and analytical information relating to threats of terrorism in the United States. . . and to all information concerning infrastructure or other vulnerabilities of the United States to terrorism, whether or not such information has been analyzed, that may be collected, possessed, or prepared by any executive agency, except as otherwise directed by the President[,]. . . [and] access to other information relating to the foregoing matters that may be collected, possessed, or prepared by an executive agency, as the President may further provide.[2]

Although the House bill would not, by itself, grant the Department of Homeland Security full all-source terrorism authority—it does not, for example, grant the Department access to information held by non-executive agencies or lower any bars to obtaining information from the private sector—it does represent a large step in that direction.

Second, Congress could, if it wished, endow an existing agency of government with all-source authority. Because of the current distribution of intelligence powers, only one agency appears a

serious candidate: the Counterterrorist Center (CTC). This organization, created within the CIA in 1986 to produce intelligence on terrorism, includes representatives from intelligence agencies other than the CIA and from various law enforcement and policy agencies. George Tenet, Director of Central Intelligence, has argued that the CTC plays a critical and effective role in counterterrorism:

> [CTC] creates a whole that is greater than the sum of its parts. It harnesses all the operational, analytical, and technical elements devoted to counterterrorism. The results through the years point to the soundness of this idea. The successes of this approach range from the uncovering of Libya's role in the bombing of Pan Am 103 to the thwarting of Ramzi Yousef's attempt to blow a dozen United States airlines out of the sky in the Far East during 1995. Moreover, CTC has worked with the State Department to provide extensive counterterrorist training to our allies. Over 18,000 individuals in 50 nations have been trained in counterterrorism over the past decade. . . . [T]he Department of Justice, the FBI, the Department of State [and] the Department of Defense are [its] customers.[3]

The remainder of this report considers the extent to which the CTC could exercise all-source authority consistent with existing law.[4] It does not address the policy issue of whether all-source authority should be lodged there.

Because the CTC lies within the CIA, it is subject to all the legal constraints governing the CIA itself. Two legal provisions have primary bite: the National Security Act,[5] the statute delineating the CIA's powers and authorities, and Executive Order 12,333,[6] which distributes intelligence functions among the intelligence agencies under that Act and other statutory provisions. The National Security Act defines the CIA's authority through a series of specific grants of power to its Director. Section 403-3(d) states in relevant part that in the Director's capacity as head of the Central Intelligence Agency, the Director shall:

> (1) Collect intelligence through human sources and by other appropriate means, except that the Agency shall have no police, subpoena, or law enforcement powers or internal security functions;
>
> (2) Provide overall direction for the collection of national intelligence through human sources by elements of the intelligence community authorized to undertake such collection and, in coordination with other agencies of the Government which are authorized to undertake such collection, ensure that the most effective use is made of resources and that the risks to the United States and those involved in such collection are minimized;
>
> (3) Correlate and evaluate intelligence related to the national security and provide appropriate dissemination of such intelligence;
>
> (4) Perform such additional services as are of common concern to the elements of the intelligence community, which services the Director of Central Intelligence determines can be more efficiently accomplished centrally;

> (5) Perform such other functions and duties related to intelligence affecting the national security as the President or the National Security Council may direct.[7]

The first three of these powers are particularly relevant to all-source authority. First, § 403-3(d)(1) grants the CIA general authority to "collect intelligence" subject to the important exception that it "shall have no police, subpoena law enforcement powers or internal security functions." Unfortunately, the Act nowhere defines the scope of this "internal security" limitation. This limitation, present ever since the creation of the CIA in 1947,[8] has long been understood as "an integral part of the definition of the CIA's authority. It reflects Congress's general understanding that CIA activities in the United States would be justified only to the extent they supported the CIA's basic foreign intelligence missions."[9] The limitation's intent is to keep the CIA out of the business of domestic law enforcement and internal security, but it also recognizes that the CIA will have to conduct some business on American soil to accomplish its foreign intelligence mission.[10] It aims, in other words, to define the CIA's authority not territorially but functionally. The CIA is to play no role in American domestic matters either here or abroad. After all these years, however, the limitation's precise contours are surprisingly unclear. It has never received specific, definitive judicial interpretation.

The other significant feature of this first collection authority is the kind of information it allows the CIA itself to gather. The authority defines this class of information simply as "intelligence," which the general definitional section of the National Security Act states "includes foreign intelligence and counterintelligence."[11] Luckily, the Act goes on to define these two particular terms in some helpful detail:

> 1. "Foreign intelligence" means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.
>
> 2. "Counterintelligence" means information gathered and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.[12]

In other words, the CIA has very broad collection authority over information with either a *foreign* nexus or a nexus to *international* terrorist activities and no collection authority over purely domestic information or information pertaining solely to *domestic* terrorist activities. Furthermore, as the earlier discussion made clear, even within its broad collection authority, the CIA cannot collect foreign or international terrorist information when it can do so only through engaging in an "internal security function," a small category of information.

Second, § 403-3(d)(2) grants the CIA "overall direction" authority over "national intelligence" collected by any intelligence agency's human sources and, third, § 403-3(d)(3) grants the CIA "correlation and evaluation" authority over "intelligence related to national security." These two separate authorities have a common structure and one that differs from that of the CIA's collection authority in two significant respects. Unlike § 403-3(d)(1), the "overall direction" and "correlation and evaluation" authorities contain no "internal security" limitation. Thus, while the Act bars the CIA from engaging in internal security functions when collecting intelligence, it does not when the CIA

is "providing overall direction for the collection of national intelligence" or "correlat[ing] and evaluat[ing] intelligence related to the national security." This difference seemingly allows the CIA more room to act when directing the collection of intelligence by others or analyzing intelligence collected by them.

The significance of this difference, however, depends in large part on the second structural difference between the agency's "collection" authority and its "overall direction" and "correlation and evaluation" authorities. This difference concerns the scope of the information each authority covers. Whereas the "collection authority" covers general "intelligence," which includes both foreign intelligence and counterintelligence, the other two authorities cover ""national intelligence" and "intelligence related to the national security" instead. These two different terms actually refer to the same category of information. As the Act defines them:

The terms "national intelligence" and "intelligence related to the national security"—

> 1. Each refer to intelligence which pertains to the interests of more than one department or agency of the Government; and
>
> 2. Do not refer to counterintelligence or law enforcement activities conducted by the Federal Bureau of Investigation except to the extent provided for in procedures agreed to by the Director of Central Intelligence and the Attorney General, or otherwise as expressly provided for in this title.[13]

Both terms, then, refer to a particular subcategory of intelligence: that in which more than one federal agency has an interest, but which was not produced by the FBI (unless the Attorney General and the Director of Central Intelligence have agreed to share it beforehand).

These structural differences seem puzzling at first. Why should the CIA's collection authority extend to a wider class of information but be subject to the internal security limitation, while its overall direction and correlation and evaluation authorities extend to a narrower class of information without any similar limitation? In a sense, the CIA's collection authority is both broader and narrower than these other two primary authorities. It covers a broader range of information, but is subject to a limitation that they are not.

On deeper analysis, however, these structural puzzles largely disappear. Both sets of authorities have the same aim—keeping the CIA out of domestic law enforcement and internal security—but accomplish it differently. Whereas the collection authority gives the CIA itself power to broadly seek intelligence provided that it does not do so for domestic purposes, the other two authorities do not restrict the purposes for which it can seek intelligence from other agencies but bar it access to intelligence gathered by the FBI, the agency most concerned with domestic security, unless the Attorney General agrees to provide it. The two different sets of authorities, in other words, structurally restrict the CIA's involvement in the domestic arena but do so differently. The collection authority limits by purpose or function the information on terrorism that the CIA can itself collect, whereas the other two authorities allow the Attorney General to limit the CIA's access to foreign and international terrorist information that the FBI develops in its own law enforcement investigations.

In short, the drafters of § 403-3(d) made the Attorney General a gatekeeper to the CIA. Without his permission, the CIA has no access to foreign and international terrorist information held by the FBI. And, since "national intelligence" and "intelligence related to the national security" are both subsets of "intelligence," a statutory category that does *not* include purely domestic information, the CIA cannot obtain information about purely domestic terrorist activities from the FBI or from other agencies even with the Attorney General's permission.

> The question is how much this structure would impair the exercise of all-source authority within the CIA. The answer depends on whether *general* or merely *foreign* all-source terrorism authority is wanted. The National Security Act would pose significant obstacles to general all-source terrorism authority. It would bar the CIA from either collecting, directing, or correlating and evaluating any information on purely domestic terrorist activities. No amount of creative statutory interpretation, for example, could have shoe-horned the Oklahoma City bombing investigation under any of the CIA's existing authorities. Thus, the CTC could have no all-source authority in these situations unless Congress specifically amended the National Security Act to authorize it.
>
> If the CTC, on the other hand, were seeking only foreign all-source terrorism authority, the answer is more complicated. The collection authority would pose little problem. It allows the CIA to collect information "relating to...international terrorist activities...except that the agency shall have no police, subpoena, or law enforcement powers or internal security functions." The only possible difficulty would arise in a very narrow category of cases. When the agency needed to obtain information on international terrorism that (1) it could get directly itself only through engaging in an "internal security function" and (2) it could not get indirectly through another agency, like the FBI. Unless the courts were to impose a very broad interpretation of the term "internal security function," the first such occasion would seldom arise. And even if the courts did, the second possibility remains—that the CIA might be able to obtain the information indirectly from a domestic law enforcement agency pursuant to its correlation and evaluation authority.

This raises the related issue of whether the definition of the CIA's correlation and evaluation authority might prevent it from effectively exercising all-source international terrorism authority. As mentioned, this authority gives the Attorney General the power to block the CIA's access to international terrorist information developed by the FBI, a not trivial amount of intelligence. If the Attorney General actually refused to share this information, it would pose a significant obstacle. At the extreme, the Attorney General could bar the CIA from nearly all intelligence about "international terrorism activities" held by the FBI. But is this likely? Despite turf-battles between the two agencies, it seems unlikely that the Attorney General would work to defeat the CIA's legitimate needs. Their common boss, the President, can, after all, fire the Attorney General at will or issue an Executive Order setting the terms of how the Attorney General and the CIA should reach agreement. There is no doubt, however, that the restriction of the CIA's "overall direction" and "correlate and evaluate" authorities to "national intelligence" and "intelligence related to the national security" does give the Attorney General potential power to impede all-source international terrorism authority anywhere within the CIA, including the CTC.

Another significant but more easily amended impediment to lodging all-source authority with the CTC is Executive Order 12,333. Issued by President Reagan in 1981, it distributes intelligence collection authority among the various intelligence agencies. Like § 403-3(d), it restricts the CIA's authority to collect certain forms of intelligence but it does so somewhat differently. Section 1.8(a) grants the CIA authority to "[c]ollect, produce and disseminate foreign intelligence and counterintelligence, including information not otherwise obtainable. The collection of foreign intelligence or counterintelligence within the United States shall be coordinated with the FBI as required by procedures agreed upon by the Director of Central Intelligence and the Attorney General."[14] Executive Order 12,333 mirrors the National Security Act in one important respect. It limits both "foreign intelligence" and "counterintelligence" to information with a foreign nexus or a nexus to international terrorism. The executive order states that:

> Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations *conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities*...[and f]oreign intelligence means information relating to the capabilities, intentions and activities of *foreign powers, organizations or persons, but not including counterintelligence except for information on international terrorist activities.*[15]

Section 1.8(a) differs from the Act's collection authority, however, in two important ways. Unlike § 403-3(d)'s collection authority, it (1) covers both direct collection by the agency itself and indirect correlation and evaluation of intelligence collected by other agencies and (2) contains no "internal security function" limitation. This limitation appears in two other sections, which have a somewhat different coverage. The first of these sections, § 1.8(c), covers counterintelligence. It states that the CIA shall:

> [c]onduct counterintelligence activities[, which includes "activities conducted...to protect against...international terrorist activities,"] outside the United States and, without assuming or performing any internal securities functions, conduct counterintelligence activities within the United States in coordination with the FBI as required by procedures agreed upon by the Director of Central Intelligence and the Attorney General.[16]

The second of these sections, § 2.3, contains a somewhat similar provision for foreign intelligence "concerning United States persons," a category that covers "United States citizen[s], . . . alien[s] known by the intelligence agency concerned to be . . . permanent resident alien[s], . . . unincorporated association[s] substantially composed of United States citizens or permanent resident aliens, or . . . corporation[s] incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments."[17] It states that:

> [c]ollection within the United States of foreign intelligence [concerning United States persons] not otherwise obtainable shall be undertaken by the FBI or, when significant foreign intelligence is sought, by other authorized agencies of the Intelligence Community, [including the CIA,] provided that no foreign intelligence collection by such agencies may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons..."[18]

Because of these particular textual differences, the executive order's authorities diverge from the Act's in several respects. First, the Act bars the CIA from performing any internal security function wherever it collects intelligence, whereas Executive Order 12,333 bars it from doing so only within the United States. Under the Executive Order alone, it would be possible for the CIA to perform (1) offshore activities related to an internal security function and (2) activities within the United States not "concerning United States persons" that are related to an internal security function. Since it is hard to imagine an internal security function that does not concern United States persons, this second category may be largely theoretical. The first, however, is real. But under the well-established hierarchy of legal authorities, the National Security Act clearly takes precedence and would restrict such operations.

Second, the Act—through its definitions of "national intelligence" and "intelligence related to the national security"—gives the Attorney General power to control the CIA's access to information gathered by the FBI, whereas Executive Order 12,333 does both something more and less. It does more insofar as it requires coordination with the FBI whenever the CIA collects on American soil (1) counterintelligence generally[19] or (2) foreign intelligence "concerning United States persons" unless it is "significant."[20] Under the National Security Act, on the other hand, the CIA can collect intelligence on American soil without speaking to the FBI whenever the intelligence has a foreign nexus or a nexus to international terrorism.

Executive Order 12, 333 does less insofar as it requires only (1) with respect to counterintelligence collected within the United States that the CIA "coordinat[e] with the FBI as required by procedures agreed upon by the Director of Central Intelligence and the Attorney General,"[21] rather than giving the Attorney General gate-keeping authority over information the FBI holds, and (2) with respect to non-significant foreign intelligence concerning United States persons that the CIA rely on the FBI for collection.[22] In other words, with respect to counterintelligence, the Executive Order requires the Attorney General's agreement not to the sharing of information itself but only to procedures that govern the two agencies' "coordination" and with respect to foreign intelligence concerning United States persons it requires no coordination with the FBI when it comes to "significant information." The executive order, then, appears both to expand the number of occasions when the CIA has to work with the FBI and simultaneously reduce the danger that the FBI could bar the CIA access to its own information. Since the executive order cannot waive any requirement imposed by the National Security Act, however, the latter difference is largely apparent. The Executive Order cannot remove the Attorney General's statutory gate-keeping authority. Despite the Executive Order's different structure, this remains a potential impediment to CTC all-source authority.

In sum, under existing law there are three obstacles—two major and one minor—to the CTC exercising all-source terrorism authority. First, unlike the proposed Department of Homeland Security, whose authority reaches terrorism both foreign and domestic, the CTC, by virtue of its home within the CIA, is strictly limited to gathering and correlating intelligence relating to "*foreign* governments, *foreign* organizations, *foreign* persons, or *international* terrorist activities."[23] It has no authority to collect and analyze information pertaining to purely domestic terrorist activities. The requirement in both the National Security Act and Executive Order 12,333 of a foreign nexus or nexus to international terrorism cannot be stretched so thin and only Congress and the President together can change this. Second, even with respect to information with such a nexus, the CTC's

all-source authority could potentially be impeded by the Attorney General. He can exercise a veto over the FBI giving over such information that it itself has collected. The President, of course, can guide and supervise the Attorney General's discretion either through an Executive Order or through less formal means, like threats of firing. Third, in addition to its structural clumsiness, Executive Order 12,333 forces the CIA to rely on the FBI for one category of information that the National Security Act does not. Under § 2.3(b) of the Executive Order, the CIA cannot itself collect within the United States foreign intelligence concerning United States persons unless it is "significant," a term the executive order nowhere defines. If he wished, the President could override this limitation by issuing another Executive Order.

## Endnotes

[1] Homeland Security Act of 2002, H.R. 5005, 107th Cong. § 201(a)-(2) (2002).

[2] *Id.* § 203.

[3] *Counterterrorism: Special Hearing Before the Senate Comm. on Appropriations*, 105th Cong. 20, 26 (1998) (statement of George J. Tenet).

[4] Because some of the regulations governing the CIA's intelligence activities are unavailable to the public, this Report's coverage is necessarily incomplete.

[5] 50 U.S.C. §§ 401-42 (1994 & Supp. 1999).

[6] Exec. Order No. 12,333, 3 C.F.R. 200 (1981), *reprinted* in 50 U.S.C. § 401 app. at 58 (1994).

[7] 50 U.S.C. § 403-3(d)(1) (1994).

[8] National Security Act of 1947, Pub. L. No. 80-253, 61 Stat. 495 (1947).

[9] Commission on CIA Activities within the U.S., Report to the President 48 (1975).

[10] *Id.* at 52-53 (quoting testimony before closed House hearing).

[11] 50 U.S.C. § 401a(1) (1994).

[12] *Id.* § 401a(2)-(3).

[13] *Id* § 401(a)(5).

[14] Executive Order 12,333 § 1.8(a), 3 C.F.R. 200, 205 (1981), *reprinted* in 50 U.S.C. § 401 app. at 60 (1994).

[15] *Id.* § 3.4(a) & (d) (italics added).

[16] *Id.* § 1.8(c).

[17] *Id.* § 3.4(i).

[18] *Id.* § 2.3(b).

[19] *Id.* § 1.8(c).

[20] *Id.* § 2.3(b).

[21] *Id.* §§ 1.8(a) & (c).

[22] *Id.* § 2.3(b).

[23] 50 U.S.C. § 401a(2) & (3) (1994).

# Domestic Security in the United Kingdom: An Overview

**By Joanna Ensum[1]**
**Task Force Researcher**

This paper aims to give an overview of the parameters and structures defining domestic security arrangements in the United Kingdom. It examines developments since September 11 against the background of British security perceptions and organization since outbreaks of domestic terrorism in the 1970s, and hopes to indicate both potential areas of interest for U.S. agencies and some differences in political and social context.

This paper gives a guided tour of the major features of domestic security intelligence in the United Kingdom, in comparison with those of the United States, and in the shadow of the current threat of international terrorism. It illustrates the three salient points of the current debate: pre-emptive profiling, data warehousing, and agency interactivity.

Britain's intelligence community has grown up piecemeal over the last hundred years in response to successive events and consequent perceptions of the national need. The Diplomatic Service combined intelligence gathering and national representation until the First World War; responsibility for domestic security, including terrorism, was vested in police forces. The structure and the balance of power between the major foreign and domestic intelligence agencies have reflected adaptations in the original system and neither ossified nor allowed one agency to dominate.

## Basic Architecture

The British intelligence community consists in five major independent bodies maintaining a somewhat flexible system of vertical and horizontal links. Although domestic and foreign security agencies are institutionally distinct, the role played by Northern Ireland in their development has interwoven them in a way that has eased the transition into today's multifaceted transnational environment.

The bare bones of British security arrangements are as follows:

- The Security Service [MI5] and the police function as the domestic security agencies and are the responsibility of the Home Office. The Secret Intelligence Service [MI6] and the Government Communications Headquarters [GCHQ] answer to the Foreign Office. The Defence Intelligence Staff is part of the Ministry of Defence [MoD].

- In general, MI6 only does human intelligence [HUMINT] outside the UK. MI5 does HUMINT and technical intelligence collection in the UK in concert with law enforcement agencies. GCHQ does most technical intelligence collection outside the UK.

- The agencies interface with government through the Joint Intelligence Committee [JIC] which forms part of the Cabinet Office and provides Ministers with intelligence assessments both immediate and long term. The JIC is supported by its assessment arm, the Joint Intelligence Organisation [JIO], consisting of the three Agency Heads, Chief of Defence Intelligence and his

deputy DCDI, and senior officials from the Foreign Office, MoD, Treasury, Department of Trade and Industry, Cabinet Office and Home Office, in addition to the JIC Chairman. Representatives from other government departments, including the Northern Ireland Office, HM Customs and Excise, National Criminal Intelligence Service and National Crime Squad, attend meetings as necessary.

- Within the intelligence community, Britain does not have a central analysis agency on the CIA pattern. Agencies are independent and with the exception of GCHQ, conduct their own analysis. The JIC weighs this with input from the Foreign Office, raw SIGINT information and operational sources to produce a single assessment which is then passed outwards. The process is collegial and arrives at assessments by consensus, rather than following the U.S. model of "competing assessments." The system has been criticized for producing "lowest common denominator" assessments devoid of inspirational disagreements. But in practice its operators are adept at "reading between the lines" and the product has an impressive record of accuracy, possibly as a result of this high level inclusion of Foreign Office personnel and others with direct and extensive experience in the field.

- MI5 also reports on domestic security to the Official Committee on Security, also part of the Cabinet Office—which also assesses information collected from the police [Special Branch] and other agencies, with security functions including the Post Office and the MoD Police.

## The Security Context in the UK vs. the U.S.

Many social and political variables shape the context in which the British security agencies work, in which the current operational environment is markedly different to that of the United States. A few points indicate briefly the different liberties and constraints.

The British public have on the whole a more accepting attitude to government "interference" but a more suspicious attitude to commercial involvement in public administration than is the case in the United States. Gun control is almost absolute. Militias have not played a part in political life [with some caveat regarding the paramilitaries in Northern Ireland] and there exists no equivalent to the Posse Commitatus Act. Although British soldiers are not permitted to wear a uniform on the streets unless on active duty, they have been deployed within the UK to deal with civilian emergencies such as the BSE crisis. They are generally not seen as a tool of government control by the public on the UK mainland.

The UK has a large, mainly urban Muslim population, many of whom arrived in the 1950s and 60s as a result of Indian independence and the partition of Pakistan and Bangladesh. Many of whom were the subject of a sharp increase in racism during the 1970s and 80s. These groups have tended politically to focus inward upon community issues. The Blair government has courted the vote of young Muslims with a bi-national identity reacting against the conservative social attitudes of their parents. The government must be careful to avoid racial profiling issues in current terrorism-related activities.

On the side of the Agencies, it should be noted that Whitehall is a very small place, with the exception of the GCHQ facility in Cheltenham. Most Agency central staff work within walking distance of each other. This has been exacerbated by the tendency of the Agencies to recruit from very restricted social group of mainly Oxbridge graduates, which has led to a tight-knit social and professional community that remains suspicious of outsiders. This culture is reinforced by a stringent Official Secrets Act, which in effect guarantees that very little operational or even administrative detail leaks to the outside world. Authorised biographies are sanitized to the point of blandness and operatives who do reveal information face significant penalties. Changes in recruitment practices are underway especially within MI5, but an atmosphere of mistrust appears to prevail.

The British Civil Service as a whole is very ignorant about technology; its managers tend to be accountants or lawyers and there is very little understanding of IT at the top level. In the present landscape of networked databases and automated data organization, the Civil Service leadership has increasing problems in re-conceptualizing information management as technology advances. With the exception of GCHQ, agency staff have in the past been recruited on strength of "character" and analytical skill rather than technical grounds. It has been observed that "the high fliers of [SIS] Intelligence Branch stream were more often versed in the classics than in the science of uranium centrifuge enrichment or anthrax preparation."

Britain has permanent Civil Service which tends to roll on regardless of who is in power. The constitutional independence of the agencies from each other and from central government, together with the opacity of security agency interfaces and their institutional culture, has encouraged an environment in which individuals from government can be kept at a distance. For example, when the Labour government first came to power in 1997, the discovery of MI5 files on leading politicians considered "subversive" in the1970s awoke little protest and incited exaggerated cries that the Intelligence Agencies had the politicians "well under control." U.S. political arrangements help to avoid such "bureaucratic capture."

The development of the UK domestic security sector has to be seen in the context of an evolving European architecture. EU mechanisms such as the Schengen Information System provide a political framework to facilitate the sharing of data within the EU. Current proposals include the extension of databases to include one for "public order offenders," and another registering third country nationals present in the EU at any given time. Both databases would include an EU-wide automated police alert system linked to border crossings and visa issue data. There is therefore ample incentive to consider compatibility issues when designing interactive databases.

## Agency Responsibilities and Capacities

### Security Service (MI5)

MI5 collects intelligence through "the interception of communications; eavesdropping, agents within target organisations; and surveillance. . . . MI5 holds around 20,000 active files, about one third of which relate to foreign nationals—typically members or associates of foreign intelligence services or terrorist groups—leaving approximately 13,000 active files on UK citizens."

The Branches of MI5 are laid out as follows:

- "A" Branch Operations deal with breaking, entering and bugging; technical backup and surveillance devices; A4 "the Watchers" cover surveillance. Their teams the "Mobiles and Statics" employ a wide range of personnel including ex-SAS soldiers.

- "C" Branch is responsible for Protective Security: Whitehall; vetting government contractors, Civil Servants and Ministers; and security against terrorist attacks.

- "K" Branch monitors counter-espionage and runs foreign agents in the UK.

- "S" Branch is the Information Technology department.

- "F" Branch deals in domestic surveillance, excluding terrorism.

- "G" Branch focuses on overseas threats, including counter-terrorism.

- "T" Branch is responsible for domestic counter-terrorism, including threats from Loyalists in Northern Ireland, Welsh and Scottish nationalist extremism. An extensive restructuring in 1992 resulted in a convergence of agencies working on IRA terrorism: T branch, A4 "Watchers" backing police surveillance teams from the Metropolitan Police Special Branch and Anti-Terrorist Unit. This proved very successful and has nearly doubled the number of personnel working directly on IRA terrorism.

## Police

Britain has 55 local Police Forces including the new Police Service of Northern Ireland which replaced the Royal Ulster Constabulary (RUC) in November 2001. The Metropolitan Police ["the Met."] act as a national police force with the remit for counterterrorism operations on the British mainland. Each force has own Special Branch, but intelligence gathering on IRA terrorist operations on the mainland UK is coordinated nationally by the Met Special Branch with added intelligence from MI5. Special Branch activity is divided into roughly two areas of operations: its E3 department operates inside terrorist organisations while the E4 section is responsible for surveillance of paramilitary suspects.

However, the Met's Anti-Terrorist Unit [ATU or SO-13] is staffed from the Criminal Investigation Department CID, whose personnel are trained to collect evidence from known sites of terrorist activity, arms dumps and bomb sites. The new Police Service of Northern Ireland has merged the responsibilities of the CID and Special Branch.

Investigations of IRA mobile cell movements on the mainland cut across force jurisdictions and have in the past lead to competitive behaviour between Chief Constables.

### Government Communications Headquarters (GCHQ)

GCHQ is a single source collector of SIGINT for Government Departments and Military Commands. It is answerable to the Foreign Office and intercepts communications using ECHELON through its Composite Signals Organisation stations in the UK and elsewhere.

The Communications Electronics Security Group of GCHQ protects government communications and is the UK's National Authority for the use of cryptography. CESG does not make equipment, but works with the private sector to supply government needs.

### Secret Intelligence Service (MI6)

MI6 is a single source collector of HUMINT from outside UK territory, running a network of foreign stations, with covert operatives who recruit and run agents and collect information.

SIS has access to CCHQ information and DIS military intelligence. Its Current Intelligence Groups also report to Government Departments and Military Commands in the weekly *Red Book*. The SIS receives direction from the JIC—unlike MI5, SIS is "tasked."

### Defence Intelligence Staff (DIS)

The Defence Intelligence Staff analyses defence related intelligence for the Ministry of Defence, Armed Forces and other Government Departments. It is comprised of operational and staff from all three Services, and has a support staff of intelligence officers. The DIS has been praised for looking outside its defence remit into the wider context of military bodies overseas. But the MoD has not invested resources or prestige in the organization in a way which could match the MI5, MI6 or the Foreign Office Research department.

The agencies have each been criticized at different times for "single-service tribalism" resulting organizationally from the lack of opportunities for outside secondments and reliance solely upon their in-house analytical capacities.

## Cross-Agency Relationships

Again the Northern Irish experience was seminal in developing and institutionalizing relationships between the police, military and intelligence services. The major relationships that were formed in Northern Ireland resulted from the emphasis on HUMINT collection and analysis, which predominated for two reasons: the inadequacy of electronic surveillance technology in the 1970s; and the tight-knit nature both of the communities in which the IRA operated and their operational structure of small independent cells. The current achievements toward security in Northern Ireland—culturally and linguistically "next door" to the UK, but engaged in a conflict of interests and ideology in which small IRA or security force achievements could score major political consequences—for better or worse—indicates the importance of tackling the underlying political issues and studying the situation through the subjective eyes of local elites.

Support for the Security Services from local communities in Northern Ireland was an essential part of the political conflict, as merely acquiring enough informants required not only resources and tenacity but engagement and understanding of a complex environment. This has given particularly the British Army invaluable experience in intelligence-related operations in political conflict zones, including the sharing of operational responsibilities with police, a critical understanding of key concepts in community relations and an appreciation of the legal parameters in conflict-driven societies. This experience showed enormous benefits in Kosovo, where highly developed techniques and procedures for effective intelligence sharing with police enabled joint operations where both effective security and evidence-gathering were necessary.

This contrasts with the prevailing attitude in the United States that SIGINT is the most accurate information as it takes info "right from the enemy's mouth." Context is critical and in practice both tools should dovetail in effective anti-terrorist operations. Complementarity between the two approaches acts as a force multiplier only when there is effective communication between them.

British Security services also developed tentacles into international criminal investigation and intelligence agencies through IRA involvement in transnational crime and weapons trade, especially as the IRA formed links with terrorist organizations in Eastern Europe, the Middle East and Libya after 1972.

## Inter-Agency Services

### National Criminal Intelligence Service (NCIS)

NCIS was set up in 1992 to provide intelligence and analytical backup to the criminal investigation agencies. Its HQ division in London includes an operational support unit, intelligence coordination, policy and research unit and specialist intelligence branch. The International Division manages a network of European Drugs Liaison officers and coordinates with worldwide Customs and Excise Drugs Liaison networks. It also houses the UK branch of Interpol and is thus linked with databases in member countries.

NCIS does not work directly in anti-terrorism intelligence, but acts as a coordination centre for secondary intelligence in the criminal networks.

### National Technical Assistance Centre (NTAC)

NTAC will provide a central facility for the complex processing needed to derive intelligence material from lawfully intercepted computer-to-computer communications and from lawfully seized computer data. It will run a twenty-four hour centre operated on behalf of all the law enforcement, security and intelligence agencies. The NTAC will be operated by the National Criminal Intelligence Service (NCIS) on behalf of the Home Office. The three Agencies will provide the NTAC with both some staff and fund part of its activity, and be fully engaged in its operation as well as customers of its product.

## The Relationship between MI5 and the Police Forces

"…The Service also works closely with the UK's 55 police forces, particularly their Special Branches, and with other law enforcement agencies, such as HM Customs and Excise and the National Criminal Intelligence Service. The Service receives assistance from the police, provides information and assessments to them on the current threats and collaborates closely with them in investigations which may result in criminal proceedings. The Service provides support to the police in two main areas: in the field of serious crime where the Service works exclusively in support of the police and other law enforcement agencies and in Northern Ireland where the Service provides support to the Royal Ulster Constabulary, which has the lead role for intelligence work on terrorism related to Northern Ireland. (The Service has the equivalent role for all aspects of terrorism outside Northern Ireland.)"

The relationship between MI5 and the Police forces raises two issues: that of operational collaboration, and the eternal issue of operational and legal distinctions between intelligence and evidence.

The expansion of MI5 towards policing activities in the 1980s was continued with the1991 takeover of Special Branch responsibilities on the UK mainland. This stemmed from a successful argument in Whitehall in which MI5 stressed the effectiveness of their preference for running agents and the preference of Special Branch for running informers, who offer information but are outside the control of their handlers.

Intelligence operations involving agents were subject to multifarious confusions between different elements of the security forces players until MI5 took overall control in 1992. Co-operation with the Gardai, the Irish Police, was necessary as the IRA General Order no. 8 expressly forbade "any military action against 26 County Forces under any circumstances whatever" although training and operational planning was carried out on Irish territory.

Within Northern Ireland MI5's lack of power to compel the police to make arrests forced a compromise with the Royal Ulster Constabulary by which their Special Branch ran local informer networks relating to the Province, but MI5 dealt with informers who could provide information on IRA campaigns on the mainland. The two agencies under pressure to get results found a mode of operating by which their co-dependency was developed as an investigative tool.

This was helped by the IRA's preference for using English "lily whites" i.e. persons with no criminal record, when setting up safe houses and arms caches on the mainland, whilst directing operatives from Ireland. These factors combined to push counter-terrorism intelligence gathering towards infiltration of IRA GHQ by agents run by MI5, who wanted to destabilize the IRA at a strategic level.

Throughout this period MI5 was able to expand its capacities with the formation of MI5 Counter-Terrorism T Branch and the expansion of A4 section "watchers." At the same time the RUC suffered from allegations of police collusion with Loyalist paramilitaries, and the difficulties of forming a police force equally balanced between Protestants and Catholics.

Operation CATNIP in 1992 raised issues of surveillance versus arresting an operation in the interests of preventing terrorist acts, in this case an explosion in Soho, London. MI5 favoured extended operational surveillance over arrests, in the interests of "little fish catching big fish", but this entails a "measured risk" of incident which in this case resulted in the explosion of a primed device, fortunately without casualties.

The trial of Brian Nelson, a former member of an illegal Loyalist paramilitary group turned MI5 agent, raised legal issues about the role of infiltrated agents, their personal participation in conspiracies to kill people and foreknowledge of crimes. The trial of Patrick Daly in 1992 likewise raised accusations of MI5 liability for the use of "agents provocateurs" to "spur others on."

Partly in order to avoid legal entanglements resulting from accusations of using agents as provocateurs, MI5 has targeted IRA Quartermasters responsible for storing and dispensing weapons, recruiting agents and allowing MI5 to tamper with bomb-making materials to render them ineffective.

A similar struggle later took place over the respective roles of police and the security agencies in the EU. The Special Branch in the Metropolitan Police through its European Liaison Section (ELS) has a dedicated communications system. But it was MI5 who trailed and pinpointed three IRA people in Gibraltar shot dead by the SAS in an MI5-directed operation in 1988.

Agencies also work to differing definitions of "success." Police measure success in terms of convictions, whilst MI5 defined success in terms of disrupting attacks: these two views compete for ministerial approval, especially as MI5 powers are confined to intelligence gathering and arrests must be made by police Anti-Terrorist Units.

### The Relationship between MI5 and the Army

Coordination between the civilian services and the Army has raised different operational and legal issues. The SAS Special Projects Team is now the Army's duty counter-terrorist force. It is available for action at short notice and duty is rotated amongst SAS Regiments.

The Army has run counter-terrorist intelligence operations in Northern Ireland at different times, frequently without consultation with, or indeed the knowledge of other security forces. There were several incidents in which operations got entangled. There is speculation that during the 1970s the SAS established free-ranging intelligence gathering units in the most dangerous areas, which avoided normal military intelligence channels but reported directly to MI5.

The Gibraltar operation in 1988, in which three unarmed men were shot dead by SAS operatives under MI5 coordination, showed the extent of cooperation but also highlighted institutional differences between MI5 and the Army.

The SAS were briefed by MI5 officers who worked to procedures governed by expectations of civilian arrest and the collection of evidence. Misunderstanding at the briefing arose from the soldiers' assumptions based upon their training and military Rules of Engagement; critically, the soldiers left the briefing believing the suspects to be armed and expecting a primed car bomb near the point of

contact. Military practice in Northern Ireland at the time used the SAS when clear intelligence of a forthcoming attack called for the positioning of the soldiers where a "clear kill" could be obtained and the incident could be treated as a military engagement.

In court the question was posed that "the same knowledge—which had allowed them to place SAS troops in the path of an IRA cell—might also have been used to avert a confrontation and make arrests." Previous cases had condoned the use of lethal force in instances in which the soldier believed his own life, or that of a colleague or bystander was in danger. The Army defines this in physical terms—*e.g.* sudden body movements—rather than intelligence terms.

The Gibraltar operation was run by MI5 from London, precluding real-time operational management. The incident also illustrated the clash between the Agencies' preference for observation leading to detecting other operatives over aborting an operation by arrests or confrontation.

## Technical Developments and Issues

The UK is undergoing a revolution in its public administrative architecture. The Blair government aims to introduce database networking technology to achieve "joined-up government" by 2008. Public support for measures using technology to reduce crime in an atmosphere of hostility to benefit abuse, asylum fraud and street crime, resulted in widespread use of monitoring devices, although there are signs that a backlash would be unleashed should the public perceive government monitoring on any pre-emptive basis. At the same time, database technology is expanding to include automated selective correlation of data from civil databases.

The drive towards networked government proceeds up a somewhat steep hill within the intelligence community: the British education system has traditionally seen analytical intellect winning out over excellence in technical ability. GCHQ recruits technicians, but policymakers and agency staff tend not to have technical skills—even to shun them. This has implications for information management: according to one senior administrator, "it was like nuclear weapons, there were no neutral specialists."

The major logistic challenge to the intelligence machinery as a whole remains money. Government can't afford to pay private sector salaries and few companies can afford to make the large investment in security clearances and understanding of specialized government requirements. The Agencies are reluctant to experiment with small or new companies and there is no equivalent to the CIA venture capital fund to expand the industry.

## Data Collection

Private data warehouses are not extensively used by security services in the UK. Generally there is much more commercial data floating around the US than Europe; European companies invest less in database technology, partly for financial and cultural reasons, but partly as a result of EU data privacy directives and their reflection in national legal jurisdictions, i.e. the Data Protection Act in the UK.

The numerous recent developments in surveillance technology have manifested themselves through most walks of private life in the UK:

- Since Intelligence has shown that IRA operatives avoid areas covered by CCTV, it has been estimated that there are more than two million surveillance cameras trained on public places across the UK.

- The London Borough of Newham was the first to use face recognition technology matched to a database. Face matches occur about three times a day and the police are automatically notified. Recognition is easily avoided by changes in appearance. But this does not seem to have dimmed enthusiasm for the technology, which has allegedly produced a 30 percent reduction in crime [at least in the vicinity of the cameras].

- Traffic cameras have been used for some years to automate the issue of speeding tickets in residential communities. The practice is not covert as the cameras are brightly marked, as are the speed measurement marking on the roads. Cameras are also positioned to record the license plates of vehicles entering what is known as "the ring of steel" into the centre of London.

## Data Coordination Issues

Whilst as yet their coordinated utilization by government is confined to specific security operations and subject to warrant provisions, there is growing public concern over "soft" measures that would in effect undermine rights by restricting access to services on political grounds without a criminal process or right of trial. For example, the Home Office proposes to compel airlines to record the name, gender date of birth and home address of each passenger, clearing them on a central database before allowing them to board an aircraft.

The debate is fuelling widespread controversy also over the provision of security through "joined-up government." Whilst civil liberties groups protested over the provisions of the Regulation of Investigatory Powers Act in 2000, Government proposals to extend its provisions and initiate further security measures after the events of September 11$^{th,}$ have drawn much more general criticism in the public as a whole, resulting in several Government backdowns including the extension of RIPA powers under the Anti-terrorism, Crime and Security Act.

New proposals for a national database containing biometric information are the subject of intense controversy and suspicion that the government intends to introduce the dreaded "identity card" through the back door.

## Legal Constraints

There is limited space here for an introduction to the major legislation governing the intelligence community. The points below survey the most sensitive legislative items in the current National Security debate:

- The major legislative measures governing domestic intelligence collection are the Data Protection Acts of 1984 and 1998. These measures limited powers to maintain web logs and email records; and the Interception of Communications Act 1985, which created the offence of

unlawfully intercepting telephone and postal communications. The IOCA made no attempt to regulate bugging or metering of telephone calls, if made with or in pursuit of a warrant or with the consent of the occupant. It gave legal authority for "trawling" of telephone communications via British Telecom to GCHQ and to taps on targeted individuals. It also covered the granting of warrants in the interest of the "economic wellbeing of the United Kingdom", but only outside UK territory. The Act entirely excluded regulation of electronic surveillance.

### Regulation of Investigatory Powers Act 2000 (RIPA)

RIPA allows web log records be kept to aid investigation of minor crimes, tax, health and safety and public order offences. Databases can be accessed by Police, intelligence services, Customs and Excise and the Inland Revenue. Access authorisation can be given internally from an official at a level within that organization designated by the Home Secretary, in cases:

- Judged to be necessary in the interests of national security
- For the purpose of preventing or detecting crime or preventing disorder
- Or in the interests of the economic wellbeing of the UK
- If it is in the interests of public safety, or for the purpose of protecting public health
- Or for the purpose of assessing or collecting any tax, duty or levy payable to a government department
- Or for the purpose in an emergency of preventing death or injury, any damage to a person's physical or mental health
- Or mitigating any injury or damage to a person's physical or mental health
- Or "for any purpose [not listed above]…which is specified for the purposes of this subsection by an order made by the Secretary of State."

The organization Liberty commented, "given such a range of permissible activities it is difficult to think of a situation where interception powers would not be available."

No authorisation would be made by an independent or judicial body. Tribunals would not open to complainant, there would be no provision for public hearing and no reason given if the complaint fails. RIPA provisions specifically exclude access to the High Court to test the legality of decisions made by the Tribunal.

## RIPA Amendment Proposal

Amendments to RIPA were proposed in the spring of 2002 by the Home Office. Measures would be taken to compel ISPs to maintain web logs detailing content, time and destination of email, and websites visited and also to hand over encryption keys. Data would then become available to a wide variety of government bodies, including local government, health services and other relevant agencies.

Parliamentary debate over these draft proposals scheduled for June 18th 2002 was postponed due to public outcry. Research by the UK Information Commissioner found that 73 percent of adults were already either "very concerned" or "quite concerned" about the amount of personal information being held by organisations.

## Anti-Terrorism, Crime and Security Act

Authorises confiscation and freezing orders, greater disclosure of information by public authorities to law enforcement authorities in the UK and abroad and the retention of communications data for use in criminal investigations. It also proposes significant extensions of police powers allowing police to search, fingerprint or photograph detainees without their consent, solely in order to establish their identity.

The Act also provided for detention without trial in the case of non-UK nationals who are suspected of involvement in international terrorism. The provisions are similar to those enacted in the U.S. following the September attacks.

Some concern has been expressed that these provisions contravene Britain's obligations under the European Convention on Human Rights. Civil liberties organizations have also warned against the danger of human rights violations occurring as a result of information transmitted by Europol to third states.

## Bibliography


Martin Dillon, *The Dirty War: Covert Action in Political Conflicts,* Routledge, 1999 (ISBN: 041592281X).

Peter Gill, *Policing Politics: Security Intelligence and the Liberal Democratic State* London: Frank Cass, 1994 (ISBN 0714634905).

Michael Herman, *Intelligence Services in the Information Age: Theory and Practice,* Frank Cass Publications, 2002.

Mark Hollingsworth and Nick Fielding, *Defending the Realm: MI5 and the Shayler Affair,* London: Deutsch, 1999.

Mark Urban, *UK Eyes Alpha,* Faber and Faber, 1996 (ISBN: 0571176895).


## Endnote

[i] Joanna Ensum is an independent researcher on international legal and security issues, based in the UK.

# Information Sharing at the FBI

**By Laura Rozen**
**Senior Associate**

## Introduction and Executive Summary

This memo is focused on information management and information sharing at the FBI in the context of efforts to counter terrorism. It tries to answer four questions:[1]

- How does the FBI (culturally, institutionally) view information?
- How does information move within the FBI? (Who reports where? Where is information currently held)?
- Through what (organizational) channels is information shared between the FBI and other agencies (intelligence community, law enforcement)?
- What initiatives exist and are planned to facilitate FBI information sharing and data warehousing, both internal, inter-agency, and what it may acquire from the private sector (airlines, financial industry, etc.)?[2]

Developing an information sharing strategy at the FBI has become one of the bureau's urgent priorities in the aftermath of September 11; in particular as Congressional investigation into the failure to prevent the September 11 attacks has uncovered major breakdowns in FBI communications, both between FBI field offices and the FBI Headquarters (FBI HQ) and to other field offices; and between the FBI and other agencies, such as the CIA and the FAA.

The information technology solutions the FBI is in the process of implementing to facilitate information sharing within the Bureau and inter-agency coincide with an important new, genuine and incomplete transformation of the Bureau's sense of mission, purpose and philosophy about its role in protecting U.S. security. More important than the technological upgrades is the new recognition among FBI leadership that the types of crimes the United States faces from terrorists are too lethal to be treated as a traditional law-enforcement issue. In the face of catastrophic terrorism, prosecuting already-committed crimes is not sufficient. Far more important is preventing them in the first place. It's hard for a culture steeped historically in rewards for gathering evidence that wins prosecutions to determine how to operate in a new value system, where a scuttled terrorist operation may not lead to a prosecution at all (or much public recognition or credit).[3] There are also important legal issues of concern, about what rules should give guidance to the FBI in carrying out a mission that is beyond pure prosecution-minded law enforcement, that are addressed by other memos.

Operationally, it's not clear how an organization guided by a sense of itself as a law enforcement agency, now being asked—and trying—to retool itself into a terrorism-prevention agency, can be both. While FBI officials point out that the FBI has always had a domestic intelligence and coun-

terterrorism role, further discussion suggests that the culture of the FBI has historically favored prosecution-minded law enforcement and crime fighting.

Finally, it's not clear what role the FBI will be asked to play in the larger reorganization of the government for homeland security that is still being determined. But in recent testimony before the Senate Governmental Affairs Committee, FBI Director Robert Mueller has suggested that his agency's 11,500 field agents are "superb" collectors of intelligence, who have much experience working on the ground and interacting closely with the country's 650,000 law enforcement officers, police and sheriffs.[4] Mueller has announced his commitment to beef up the bureau's admittedly weak in-house intelligence analysis abilities—for starters, by creating an Office of Intelligence, a school of intelligence analysis at the FBI Training Academy and by borrowing CIA analysts. He has also indicated that the FBI is accelerating technical efforts to facilitate its information dissemination abilities, chiefly the FBI's technical ability to electronically transmit raw intelligence reports to the CIA and other agencies, including presumably to the proposed Department of Homeland Security's intelligence analysis center. Since that seems to be the direction things are going, it will be important to resolve not just technical feasibility issues, but the legal issues surrounding the admissibility of information that has been disseminated upward as intelligence, that may be desired to be used as "evidence," at least in terms of guidance given to FBI field agents.

### New Team Leading FBI Information Sharing Initiatives

The new focus on information sharing at the FBI is reflected in a number of recent appointments, drawing on information-architecture specialists from the private sector and intelligence community. The two most important of these for the Task Force's purposes are the new FBI Chief Information Officer (CIO), Darwin A. John,[5] appointed just this July, and Kenneth M. Ritchhart, appointed in March to head data/information management at the FBI's Information Resources Division.[6]

Ritchhart, formerly head of the Defense Intelligence Agency's (DIA) Joint Intelligence Virtual Architecture, is tasked with coming up with the vision for how the FBI should organize and make accessible all the information already in the FBI's hundreds of legacy databases, information it is acquiring from other agencies, and from private industry, and making it all work in real-time, and within the confines of the law and security concerns.[7]

Also in March, Mueller appointed Sherry Higgins, a former CIO of Lucent, as the FBI's advisor on the Trilogy Systems, which is the major agency-wide upgrade already underway of the Bureau's hardware, software, inter-office networking and automated case-system, described in detail below.

Another key figure is Robert J. Jordan, who heads the FBI's Information Sharing Task Force.

## I. How is information viewed by the FBI?

### " Evidence" vs. "Intelligence"

Director Mueller has identified two main tensions for the FBI between its traditional practices of federal law enforcement and the new priority of terrorism prevention: the Bureau has historically been very focused on prosecuting (past) crime, and therefore has become very reactive, rather than

pro-actively preventing criminal or terrorist acts. Secondly, he is concerned about the way people at the Bureau tend to view information as potential evidence, rather than as intelligence.[8]

"We must change how we look at information," Director Mueller told a House Appropriations subcommittee in June,[9] "so that we not only consider its case-related value, but also its relevance to the larger, strategic view of a group or organization."

The primary historic mission of the Federal Bureau of Investigation—to investigate and solve federal crimes, with an eye towards prosecution—is the main reason the organization's structure and culture have lent themselves towards hoarding and compartmentalizing of information, and not processing it in a way that makes it easily accessible and analyzable by the variety of people and agencies that would find it of use for intelligence and counterterrorism purposes. The bureau's mission has historically favored information gathered for the sake of prosecution, *e.g.* evidence, and its legal requirement of being held secret, over information gathered for intelligence's sake. The information-management tools the agency has acquired—a series of some 200 databases that for the most part cannot talk to each other or be easily searched or disseminated to other agencies—reflect the larger organizational structure and practice.[10] It has become a cliché among FBI veterans that technology is not the problem, but a symptom or reflection of the larger culture itself.

## Culture of Information "Hoarding"

A former bureau agent describes a culture at the FBI and in law enforcement more generally where information is viewed as a "jewel," something to hold onto, and not share; and where turf consciousness and fear of a scuttled case have in the past fostered FBI reluctance to share information even in inter-agency bodies supposed to facilitate just that, such as the Joint Terrorism Task Forces (JTTF).

"Maintain the integrity of the investigation," the former Bureau counterterrorism official describes the cultural mantra.[11] "If I've written a report about say the Popular Front for the Liberation of Palestine, am I going to give that to the New York Police Department? What are they going to do with it? I don't know what other people are going to do with it."

"A key question you are always asking yourself as you investigate a case and do surveillance is, 'when do you go overt?'" he continued. "There's a question of not knowing the impact of dissemination of that information. Who can I trust or not, to not blow my case?"

The reluctance to share information that could blow a case is much in evidence. Indeed, a Task Force member has recounted how the FBI had been pursuing a domestic bioterrorism suspect believed to have a jar of anthrax in his car through Las Vegas, Nevada. The FBI had failed to notify any public health officials about the case until after they had apprehended the suspect, because they didn't want anyone getting in the way of catching their suspect in the act, even at the cost of hospitals and public health officials being entirely unprepared for what could have been a catastrophic health emergency should the suspect have crashed or not been arrested.[12]

## II. How Does Information Move Within the Bureau?

It's useful to understand the basics of how information has typically moved through the Bureau, and the organizational structure itself. The FBI has 28,000 employees, 10,000 of whom are assigned to FBI Headquarters (FBI HQ). Ten thousand of the Bureau's 11,500 field agents are distributed across 56 field offices, 400 smaller satellite offices (known as resident agencies), four specialized field installations, and 40 foreign liaison posts.[13]

### View from the Kansas City field office

An agent at the FBI field office in Kansas City helps describe how investigation, reporting, and information-flow from a field office through the Bureau typically work. "It depends on what kind of case it is: bank robbery, white-collar crime, drugs, organized crime, terrorism, etc.," an agent from the KC field office explains.[14] "If you're an agent, you're assigned to a squad and that's what you work for a given amount of time. Each squad has a supervisor, and that supervisor is in charge of all valuations that squad covers.

- "In Kansas City, we have one squad that does international terrorism. In a smaller office, like Springfield, Missouri, the supervisor for terrorism may also be handling cases of hate crimes, or something else."

- "So if you're an agent assigned to investigate international terrorism in Kansas City, your squad supervisor will review what you write up. When you have a reporting requirement, your report will go to the office of origin (OOO)—the field office where the investigation originated and to the unit at FBI HQ that covers that type of investigation (radical Islamic fundamentalism, Osama bin Laden, etc.)."

- Each of the FBI's 56 field offices operates somewhat on its own. There's a lot of autonomy in what they do. But they do also report back to DC, and there are certain things Washington has to approve. For instance, you couldn't initiate an under-cover operation or a drug buy without approval from Washington. That said, all investigative programs are run by the local field office itself.

Where are data from cases investigated locally stored? Where is it distributed?

- Cases are stored in the local (field office) file/database, and reports are uploaded into the bureau-wide computerized Automated Case System (ACS), the bureau's legacy case/investigation system (described below).

- "Whether the investigation is terrorism, or anything else, agents do global searches on the ACS. If they are investigating XYZ company in Kansas City, and if that comes up with a matching case in Chicago, it's the job of the investigating agent in Kansas City to contact the other agent who handled the case and find out what happened there. It's very easy to pick up the phone. We'll know from the ACS system who's got a case and who's done something."

Are there issues about what information can be shared? And what is "admissible" if it's been shared, or more widely disseminated with other agencies?

- **Field Document 302 (FD 302):** "The 302 is documentation relative to evidence—a witness interview, review of documents, surveillance logs, etc. Once it's in a FD-302 and entered in the ACS, that's it. That's the document that will be used in court. That document can still be used even if it goes to another agency. The chain of custody isn't an issue once the 302 is entered into the system, no one else can change its contents. Once it's entered, the 302 is cement."[15]

It is worth noting that it is largely up to the discretion and initiative of the original investigating agent if and where else to send his report onto inside the Bureau, *e.g.* if he or she should send it on to other field offices that in the course of his investigation he determined may find the information in his report relevant. There is no systematic bureau-wide reporting to other field offices.[16]

## Work Flow

A former FBI and Department of Justice official explains: [17]

- Typically, FBI agents don't view themselves as gathering information for customers, even when they're gathering what constitutes foreign intelligence information. They are working an investigation, either a criminal investigation or a Foreign Counterintelligence Investigation (FCI), which includes both espionage and foreign terrorism cases.

- Important information gathered pursuant to an investigation is supposed to be shared with HQ program managers, who are supposed to approve certain sensitive techniques, make any linkages among separate investigations, and provide general oversight. This would include making determinations about whether an FCI case that involves following suspected terrorists should be turned into a criminal case for the purpose of putting the suspect in jail rather than just gathering more intelligence. It's also HQ that would typically be responsible for determining whether and what info gathered in a terrorism investigation should be shared with other intelligence agencies such as CIA or NSA, or with policymakers such as those in the White House, NSC, etc.

- So a flow chart would have an agent in a field office reporting to his Supervisory Special Agent (SSA) who heads his CT squad; that SSA reporting to a Unit Chief in the Counterterrorism Division at HQ; and the Unit Chief reporting to a Section Chief (*e.g.*, for the International Terrorism Operations Section), who reports to the Assistant Director for the CT Division, who reports to the Executive Assistant Director Counterterrorism and Counterintelligence, who reports to the Director. That seems like a long chain, but the decisions about sharing intelligence information with other agencies or policymakers would normally be made at the Unit or Section Chief level.

## III. Through what channels is information shared between the FBI and other agencies (intelligence community, law enforcement)?

Robert Jordan, the head of the FBI's Information Sharing Task Force, testified to the Senate Judiciary Committee in April 2002 about information sharing initiatives at the Bureau. He identified the following as the main inter-agency bodies where information is shared between the bureau, other law enforcement, intelligence and government agencies:

### Joint Terrorism Task Forces (JTTFs):

- "There are currently…JTTFs in each of the FBI's 56 field offices," Jordan testified.[18] "…The creation of 21 new JTTFs this year is resulting in an expanded level of interaction and cooperation between FBI Special Agents and their Federal, state and local counterparts, as well as an enhanced flow of information between the participating law enforcement agencies. Among the full-time federal participants in JTTFs are the INS, the US Marshall's Service (USMS), the Secret Service, the FAA, the Customs Service, the Bureau of Alcohol Tobacco and Firearms (ATF), the State Department, the US Postal Inspection Service, the IRS, and the US Park Police, state and local police and other agencies are heavily represented."

- Director Mueller has also proposed the creation of a National Joint Terrorism Task Force at FBI headquarters to "complement task forces established in local FBI field offices and to improve collaboration and information sharing with other agencies."[19]

- In addition to the city-level JTTFs, there are six Regional Terrorism Task Forces (RTTFs) that operate on an *ad hoc* basis.[20] "FBI Special Agents assigned to counterterrorism matters meet with their federal, state and local counterparts in designated alternating locations on a semi-annual basis for common training, discussion of investigations, and to share and discuss intelligence," Jordan testified. "The design of this non-traditional terrorism task force provides the necessary mechanism and structure to direct counterterrorism resources toward localized terrorism problems within the U.S."[21]

### Terrorism Watch List (TWL)

- The Terrorism Watch List (TWL) serves "as the FBI's single, integrated listing of individuals of investigative interest that will be accessible throughout the law enforcement and intelligence communities," Jordan testified. It replaces the "stop-gap system previously resident within NCIC [the National Crime Information Center]."[22]

- The TWL will "consist of a compendium of names based on information identified through the FBI and JTTF investigations, US Intelligence Community reporting, and Department of Defense intelligence gathering, as well as information provided by cooperating foreign governments…"

- The TWL will be divided into three distinct categories. The first category includes names of individuals for whom formal criminal charges or indictments have been issues (*e.g.* the 22 individuals on the Most Wanted Terrorism List). The second category includes the names of individuals of investigative interest to the FBI. The third category includes the names of individuals provided by the Intelligence Community and cooperating foreign governments.

- TWL is designed "to assist both the intelligence and law enforcement communities in their investigation of terrorist groups/ individuals and…to alert officers or agents should a person of interest in a terrorism matter be encountered by another agency," Jordan testified. "TWL staff will coordinate within the FBI's Criminal Justice Information Services (CJIS) Division to ensure the utilization of appropriate NCIC files. This capability will provide all state and local agencies ready access to this information. Information in the TWL will also be shared with the U.S. Government agencies that operate comparable tracking systems," such as the State Department's TIPOFF program, which is designed to stop terrorists from getting visas or entering the U.S. at a point of entry.[23]

- While the FBI has created a watch list of known and suspected terrorists which is accessible on the NCIC database, there is not yet as of this writing a comprehensive, consolidated multi-agency terrorism watch list that draws on the resources of the State Department, CIA, NSA, etc.[24]

### Connecting FBI with State, Local Law Enforcement

- Director Muller has named Louis Quijas, chief of police of High Point, North Carolina, to be FBI Assistant Director for Law Enforcement Coordination. Quijas "has as his single mission fully exploiting state and local law enforcement support through enhanced information sharing and ensuring that state and local law enforcement have a strong voice within the FBI."[25]

### The CIA Counterterrorism Center (CTC)

- At the CIA Counterterrorist Center (CTC), one of the two deputies is from the FBI, and a CIA official plays the same role at the FBI's Counterterrorism Center. CIA has also lent staff to the FBI to contribute to Counterterrorism analysis and to the nascent Office of Intelligence within the Counterterrorism/Counterintelligence Division.[26]

- CTC brings together case officers from the Directorate of Operations with analysts from the Directorate of Intelligence. Other agencies represented include NSA and National Imagery and Mapping Agency (NIMA) personnel. "CTC's Operations group includes two sets of skills—a 'tool box' group of scientists and engineers, who design and assemble special devices, and a group of case officers familiar with running agents."[27]

### National Infrastructure Protection Center (NIPC)

- The NIPC's mission is "to serve as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infra-structure."[28]

- "A central part of the NIPC's mission has been to share actionable information with other agencies and the public; to analyze information from all sources (criminal investigations, intelligence, open sources, industry data); and to bring all relevant agencies into the Center through the detailing of employees. So CIA, NSA, DoD, Commerce, Energy and even Canadian and UK government representatives were included, some with senior management positions."[29]

- The outreach and analysis and warning functions are slated to be moved to the Department of Homeland Security (DHS), leaving just the investigations at the FBI. So even though NIPC was a pioneer effort to do what the FBI is trying to do more broadly now (be interagency, do prevention first, issue effective warnings, and do better analysis), the FBI is willingly ceding its analytical capacity in the cyber attack area.[30]

## IV. What initiatives exist and are planned to facilitate FBI information sharing and data-warehousing?

### Hardware, software, case-system upgrade

Currently, the FBI is in the midst of a massive, agency-wide, 36-month, $379 million upgrade of its office computer systems network, called the Trilogy Program.[31] The upgrade is long overdue, as has been much reported.

Trilogy is upgrading from a system of 56k-modem-connected offices, where agents don't have email or Internet-access, or the capacity to electronically send photos (even of September 11 hijackers—those had to be over-nighted), and a record-keeping system that is based on paper reports that are uploaded by agents to the Bureau's legacy "Automated Case Support" (ACS) system.

### Automated Case System (ACS)

- The ACS investigative case-load system, circa 1995, is so cumbersome that agents reportedly sometimes fail to enter their paper reports at all. Some FBI squads are reportedly six months backed up in entering paper reports. The backlog in reports filed and difficulty retrieving information filed led the FBI's John Kerr to tell the *Wall Street Journal*,[32] "In many cases, we don't know what we know."

- As for data-mining? According to a recent *Wired* report,[33] it's done by hand, by "1,000 of the bureau's 28,000 employees, who sift by hand through information collected by field agents."

### Trilogy

- The Trilogy Program, expected to go on-line by January 2004, some aspects before, will provide all FBI agents and staff with desk top (Dell) computers running Web-based (Microsoft Office) products, high-speed connections linking all FBI offices to FBI HQ and to each other, and five user-specific software applications to allow each employee to access, organize and analyze information.[34]

- Trilogy is also the internal upgrade of the bureau's case files, the ACS. It will consolidate data from the FBI's five main investigative applications to reduce "stovepiping," into a single virtual knowledge database.

- Some FBI officials have also described a **"Virtual Case File"**—part of a larger data warehousing project, which involves the contribution of databases of other government agencies, that's underway.

## Most Important Existing Databases and Data-Sharing Networks

### National Crime Information Center (NCIC 2000)

- The **NCIC 2000** is a real-time database system comprised of 17 databases able to be accessed in real-time by 80,000 authorized users, mostly law enforcement. NCIC 2000 contains information on outstanding warrants, wanted persons, watch lists, criminal records, stolen property, license plate numbers, drivers license numbers, digital mug shots, fingerprints, missing persons, stolen guns, etc.[35]

- If a police officer stops someone for speeding and does a check on his driver license, he will connect to NCIC 2000 and be able to pull up any outstanding warrants, check the missing persons file, watch lists, etc.

- The FBI maintains NCIC 2000, based in Clarksburg, West Virginia, but most of the information on it is submitted by local law enforcement agencies. NCIC is the evolution of the National Crime Information Center system that has been around since 1967. In the 1990s the FBI spent almost $200 million to upgrade it. The system runs on three IBM mainframes capable of processing 2.5 million transactions a day.[36]

- The **Violent Gang Terrorist Organization File** (**VGTOF**) is part of the NCIC 2000.[37]

### Law Enforcement On-line (LEO):

- Web-based private "Intranet" for law enforcement officials, the FBI, etc. Unclassified. A kind of virtual law enforcement community space, where law enforcement officials can "chat" on the web with other law enforcement professionals on subjects of interest and concern, patterns they're observing, other law enforcement related issues. Maintained by the FBI Criminal Justice Information Services division. Who can use it? Law enforcement, FBI and other interested agencies, by accessing the LEO intranet site.

- "The information provided to law enforcement agencies, as well as appropriate private entities, will be approved by FBI HQ, the Program Assistant Special Agent in charge, and the US attorney," explained Chicago FBI Special Agent in Charge Patrick Daly. "The LEO system will facilitate communication regarding terrorist matters, not only between law enforcement agencies, but also with other appropriate agencies in the public and private sectors. Federal and local law enforcement agencies have joined to determine the capabilities and resources of each agency that could be utilized in a WMD incident or in other types of emergencies."[38]

- The **Regional Information Sharing Systems** (**RISS**) network connects six regional law enforcement/anti organized crime "nodes" on a secure system, enabling them to "share intelligence and coordinate efforts against criminal networks that operate in many locations across jurisdictional lines. Typical targets of RISS activities are drug trafficking, terrorism, violent crime, cybercrime, gang activity, and organized criminal activities."[39]

### InfraGard

- Part of the **National Infrastructure Protection Center (NIPC)**[40], which is slated to be moved to the proposed Department of Homeland Security.

- "InfraGard is an information dissemination and intelligence gathering initiative. Its mission is the protection of the eight critical infrastructures of the United States. The eight critical infrastructures were identified by the National Infrastructure Protection Center…as a result of Presidential Decision Directive 63, signed in May of 1998."[41]

- An information sharing and analysis alliance between government, first responders, and the private sector at the city level that provides formal and informal channels for the exchange of information about infrastructure threats and vulnerabilities. Key information about nine categories of vital city infrastructure, such as water systems, power grids, key landmarks, etc. is studied and stored on a database, accessible to first responders.[42]

### Integrated Intelligence Information Application (IIAA)

- FBI has recently developed an FBI-wide and DOJ-wide capability to electronically share case information.[43]

- Real-time collection system that houses over 33 million records—derived from many different sources including the Department of State and INS—provides analytical support for Counterintelligence and Counterterrorism programs.

- Multiple programs have been written to standardize incoming data arriving in different formats and to package the responses to accommodate the requesters' needs.

## Most important database and data-sharing networks, prospective/in development

### Secure Counter Terrorism Operational Prototype Environment (SCOPE)[44]

- "That is the core of 'connect the dots.' The end result will be a prototype that allows the Bureau to pull data from other agencies, interviews from witnesses, (anything that can legally be obtained) and access and analyze all content."[45]

- This will be ready to go on-line when Trilogy is finished, within 18 months. Being spearheaded by Kenneth M. Ritchhart, the FBI's new information technology manager, formerly program manager of the Joint Intelligence Virtual Architecture at the Defense Intelligence Agency.

- "Rithchart is looking at all the material in Counterintelligence, in Counterterrorism, mission data (photos taken with a guy who may have been investigated, information about people not subject of investigation but which the bureau wants to keep), and administrative data."

- Phase I of SCOPE solves FBI's internal info-sharing problem. Later phases address inter-agency info-sharing and what may be acquired from the private sector.

## Current and Prospective Use of Private Industry Databases by the FBI

### ChoicePoint

- The FBI purchases files of information on individuals from ChoicePoint Inc., a publicly held Alpharetta, Georgia company, among others.

- According to a *Wall Street Journal* report on the FBI's use of ChoicePoint, the company "specialize[s] in doing what the law discourages the government from doing on its own—culling, sorting and packaging data on individuals from scores of sources, including credit bureaus, marketers and regulatory agencies…The FBI's Investigative Information Services unit, which helps agents obtain information on individuals for their investigations, relies heavily on ChoicePoint's services…"

- FBI agents also can go to a dedicated Web intranet site for help in conducting their own searches.[46]

### Terrorism Financing Database

Following September 11, the FBI created the terrorism financing database to centralize financial information collected from government agencies and private financial institutions on suspects of the September 11 terrorist attacks.[47] They have since expanded this database to include financial data on all terrorist investigations. Among other things, they conduct link analysis of records in this database to identify associations among existing suspects and to identify new possible suspects.[48]

### Critical Private Industries[49]

The FBI is not connected in real time to private sector databases at this time, although it is exploring the legal options and industry willingness for doing so. One system reportedly under consideration would link government databases to airline reservation systems, credit agencies, etc., to create a network capable of tracking an individual's purchases, living arrangements, travel, and other info. [50]

Before that is created, the FBI is using its standard operating procedure to go to a court and get permission to search suspects' account histories, travel history, acquire phone and financial and bank records, etc. In national security cases, the court gives the FBI tremendous leeway. [51]

In an interview with Abt Associates and the Markle Task Force, the FBI identified the following private industries as holding information key for terrorist investigations:

- Travel Industry (*e.g.*, airlines, rail, rental car)

- Communications Industry *(e.g.*, cell, land line, Internet) [They noted that pre-paid phone cards are a problem for them.]

- Financial Industry (*e.g.*, banks, credit cards, and money transmitters, casinos and brokerage firms). [The FBI mentioned the particular challenge that the money transmitter industry poses as it is an easy means of transferring funds with little to no audit trail.]

- Services Industry (*e.g.,* insurance, pharmaceuticals, weapons, chemicals, precursors)

## Endnotes

[1] Many thanks to Abt Associates' Anne-Marie Bruen, Mitretek's Robert Clerman, Steve Pomerantz, Craig Janus, and Larry Pantzler, former FBI officials Harvey Rishikof, Michael Vatis, Drew Richardson, Steve Pomerantz, and FBI press officers Paul Bresson and Jeff Lanza for insights; and Bruce Berkowitz and Ryan Coonerty for comments on drafts. None of them is however responsible for errors that may be included.

[2] Legal issues involved with these data sharing issues are being addressed by other memos and will not be addressed here.

[3] For instance, former FBI legal counsel Harvey Rishikof has proposed the creation of a new court for terrorism, in an opinion piece in the *New York Times,* June 8, 2002 http://www.nytimes.com/2002/06/08/opinion/08RISH.html?todaysheadlines=&pagewanted=print&position=top "What we need is a specialized, secure and protected federal court dedicated to matters involving domestic and international security…A specialized federal security court could accommodate the particular challenges of prosecuting terrorism cases without undermining constitutional principles. We already have specialized courts in the federal system, for bankruptcy, patents, copyrights, tax matters and international trade. In the arena of national security, the Foreign Intelligence Surveillance Act in 1978 also established a Foreign Intelligence Surveillance Court…"

[4] Statement for the Record of Robert S. Mueller, III, Director Federal Bureau of Investigation on Homeland Security, Before the Senate Committee on Governmental Affairs, June 27, 2002, http://www.fbi.gov/congress/congress02/mueller062702.htm

[5] July 8, 2002, Source: FBI press release. www.fbi.gov/pressrel/pressrel02/mueller070802.htm. The new CIO Darwin John was formerly information/communications director at the Church of Jesus Christ of Latter Day Saints in Utah. As such, Director Mueller pointed out when announcing John's appointment, John managed a popular genealogy data-warehouse/website consisting of 900 million names that draws some eight million hits a day.

[6] FBI press release, http://www.fbi.gov/pressrel/pressrel02/mueller031102.htm

[7] Mitretek, interview with Markle Task Force staff, June 10, 2002.

[8] Mueller testimony to House Appropriations Committee, June 21, 2002, *ibid.*

[9] Statement of Robert S. Mueller, III Director Federal Bureau of Investigation on A New FBI Focus before the Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies, Committee on Appropriations House of Representatives, June 21, 2002. http://www.fbi.gov/congress/congress02/mueller062102.htm

[10] John R. Wilke, "How Outdated Filing Hampers FBI Effort to Fight Terrorism," Wall Street Journal, July 9, 2002. http://online.wsj.com/article_print/0,,SB1026164881307136720,00.html

[11] Interview with former FBI counterterrorism official by Markle Task Force staff, June 10, 2002.

[12] Comments by a task force member to a Markle working group meeting, June 27, 2002. News reports back up the account, see "Local Officials Felt Ignored in Scare," Las Vegas Review Journal, February 25, 1998, http://www.lvrj.com/lvrj_home/1998/Feb-25-Wed-1998/news/7021270.html:

"Clark County's chief health officer found out about last Wednesday's seizure of suspected military-grade anthrax from an ambulance company employee. Up to that point, Dr. Otto Ravenholt said he had no idea what kind of threat the Federal Bureau of Investigation was trying to diffuse at a Henderson business complex. 'So far, I've never had any real contact from the FBI,' Ravenholt said Tuesday. 'I think they got caught up in doing it themselves'…Local emergency agencies that assisted the FBI are questioning whether police officers, firefighters and local residents were jeopardized by the lack of information the FBI made available during the hours a biological threat appeared real."

[13] Source: www.fbi.gov). An organization chart of FBI headquarters is available at http://www.fbi.gov/aboutus/todaysfbi/hqorg.htm (A thousand or so field agents are assigned to FBI HQ at any given time, but the HQ itself has little investigative capacity, instead relying on field offices.)

[14] Phone interview of FBI KC field office press office with Markle staff researcher, July 22, 2002.

[15] "Classified information is a different story. The only classifying authority is in Washington (at the FBI),"July 23, 2002.

[16] The highly compartmentalized nature of the Bureau, and the lack of systematic/technically facilitated dissemination of investigation information, was of course evinced by the now infamous fate of the Phoenix memo, the eerily prescient July 10, 2001 memo by Phoenix FBI special agent Kenneth J. Williams, warning of "a possible effort by Usama bin Laden to send students to the U.S. to attend civil aviation universities and colleges." Williams' 3-page memo "was transmitted electronically to FBI headquarters," the *Washington Post* reported, "distributed to two counterterrorism units there and sent to the counterterrorism team in New York…The Phoenix memo was never shared with the CIA or any other agency." Source: Bill Miller and Dan Eggen, "FBI Memo Author Did Not Envision Sept. 11: Phoenix Agent Who Marked Warning 'Routine' Finishes Congressional Testimony ," *Washington Post,* May 23, 2002. http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A60179-2002May22

[17] Source: Former FBI official email with Markle Task Force staff, July 23, 2002.

[18] Statement for the Record of Robert J. Jordan, FBI, on Information Sharing Initiatives, before the US Senate Committee on the Judiciary, Subcommittee on Administrative Oversight and Courts, April 17, 2002. http://www.fbi.gov/congress/congress02/jordan041702.htm

[19] Mueller, "A New Focus," June 21, 2002, http://www.fbi.gov/congress/congress02/mueller062102.htm

[20] Source: Jordan testimony, *ibid.*

[21] Source: Jordan testimony, *ibid.*

[22] Source: Jordan testimony,*ibid.*

[23] Information on TIPOFF from a speech given by John G. Arriza, Director Tipoff Watch Program, State Department, to the Information Sharing for Homeland Security conference, Philadelphia, August 21, 2002.

[24] Source: interviews by the Markle Task Force staff.

[25] Source: Jordan testimony, *ibid.*

[26] For a much more detailed description and analysis of the work of the CTC, see Stephen Marrin's "Homeland Security and the Analysis of Foreign Intelligence," in this report.

[27] Source: Association of Former Intelligence Officers (AFIO) http://www.afio.com/sections/wins/1998/notes37.html

[28] Source: A message from Ron Dick, Director of the National Infrastructure Protection Center, www.nipc.gov/about/about.htm

[29] Source: former FBI/NIPC official, email with Markle Task Force staff, August 20, 2002.

[30] Source: former FBI/NIPC official, *ibid.*

[31] The Trilogy contracts were awarded in May and June 2001, but some aspects of the upgrade, such as Windows-based desktops for all agents, and high speed connections networking offices, are supposed to be completed by the end of 2002. The rest of Trilogy is expected to go on-line in the next 18 months. Sources: FBI, Mitretek.

[32] John R. Wilke, "How Outdated Filing Hampers FBI Effort to Fight Terrorism," *Wall Street Journal,* July 9, 2002. http://online.wsj.com/article_print/0,,SB1026164881307136720,00.html

[33] McHugh, Josh, "Rewiring The FBI: The FBI's $379 million upgrade won't solve the agency's problems," *Wired*, October 2001. http://www.wired.com/wired/archive/10.01/mustread.html?pg=2

[34] Sherry Higgins, Project Management Executive for the Office of the Director Federal Bureau of Investigation on FBI Infrastructure, Statement before the Senate Judiciary Subcommittee on Administrative Oversight and the Courts, July 16, 2002. http://www.fbi.gov/congress/congress02/higgins071602.htm (Dell computer hardware, Windows 2000, Microsoft Office software, e-mail, and eventual access to a secure internal "intranet": Source: "Rewiring the FBI," *Wired, ibid.*)

[35] Interview with FBI press office, July 18, 2002.

[36] "Rewiring the FBI," *Wired, ibid.*

[37] Source: Mitretek, interview with FBI.

[38] Statement of Patrick J. Daly, Assistant Special Agent in Charge, Chicago Division, FBI, on Counterterrorism, July 2, 2002.

[39] Source: http://www.iir.com/RISS/

[40] For more on NIPC, see section III of this paper, or www.nipc.gov

[41] Source: North Texas Joint Terrorism Task Force, at https://secure.fbiern.org/ntjoint/index1.php

[42] Daly, *ibid*: "Threat assessment teams identify…key infrastructure components…Information pertinent to the specific venue, i.e., ingress, egress, utility information, key personnel, storage of hazardous material, etc…obtained and entered into a database at the City of Chicago Emergency Communications Center. In the event of a terrorist incident or threat, this information can be retrieved by a first responder."

[43] Source: Robert J. Jordan testimony, *ibid.*

[44] Legal issues/privacy concerns involved with these data sharing issues are not addressed here.

[45] Source: Mitretek.

[46] Source: Glenn R. Simpson, "Big Brother-in-Law: If the FBI Hopes to Get The Goods on You, It May Ask ChoicePoint—U.S. Agencies' Growing Use Of Outside Data Suppliers Raises Privacy Concerns," *Wall Street Journal,* April 13, 2001.

[47] Abt Associates and Markle Task Force interview with FBI, April 24, 2002.

[48] Source: Abt Associates:

"The FBI obtains information from private financial institutions in the following manner:xlix (1) FBI sends out a "Financial Control List" (a list of persons suspected of being involved with terrorists or terrorist organizations) to every U.S. bank (including foreign offices of U.S. banks) and 50 foreign countries. (2) The list contains up to the following information for each person: name, address, date of birth, phone number, SSN, passport #. Banks are asked to check their records for any transactions involving the people or addresses on the list. If a bank gets a hit, they notify the FBI. (3) The FBI then provides the bank with a subpoena to provide the FBI with information on all transactions involving the suspect(s). The FBI will reimburse the bank for expenses they incur for extracting this information."

[49] Source: Abt Associates.

[50] Source: Electronic Privacy Information Center (EPIC), http://www.epic.org

[51] Source: interview with FBI press office, July 20, 2002.

# Limitations upon Interagency Information Sharing: The Privacy Act of 1974

**Sean Fogarty**
**Task Force Researcher**
**University of Virginia School of Law**

**and**

**Daniel R. Ortiz**
**John Allan Love Professor of Law and**
**Joseph C. Carter, Jr., Research Professor**
**University of Virginia School of Law**

## Introduction and Executive Summary

In his address to America proposing the creation of a Department of Homeland Security, President Bush announced that this new department will "review intelligence and law enforcement information from all agencies of government" in an effort to improve national security. The major provisions of the Privacy Act of 1974 appear, however, to prevent government agencies from sharing an individual's personal information with other agencies for uses other than those for which it was originally obtained. At first glance, in other words, the President's proposal appears to run right up against existing law. As Professor Lillian Bevier has argued, however, the Privacy Act is something of a "paper tiger."[1] In practice, its many exemptions greatly relax the protections its central provisions grant. That is particularly the case here.

This report seeks to summarize the purposes of the Privacy Act and the protections it offers individuals. It describes how the law constrains—and does not constrain—government agencies from disclosing information they collect on individuals in the course of carrying out their authorized objectives. These constraints provide numerous safeguards designed to protect an individual's privacy. The text of the Privacy Act, for instance, broadly prohibits any federal agency from disclosing any record contained in a system of records, without written consent of the individual to whom the record pertains.

The Act's many exemptions, however, greatly weaken these safeguards. Three in particular would make it possible for government agencies to share information on individuals with a central counterterrorism intelligence agency. First, the Act contains an exemption for legitimate civil and criminal law enforcement activity. By itself, this exemption would allow much transfer of relevant information to an intelligence agency that aimed to prevent unlawful terrorist acts. Second, the Act's "routine use" exemption allows an agency to share an individual's personal information with other agencies if that sharing (1) is listed as a routine use for that agency in the Federal Register and (2) is compatible with the purpose of the initial information gathering. Past cases indicate that these two burdens are fairly easily met. Third, an exemption for foreign counterintelligence found in the Computer Matching Act (which amended the Privacy Act in 1988) legitimizes information sharing through data matching among agencies for national security purposes.

## Privacy Act of 1974

The Privacy Act of 1974 represented Congress's first broad effort to provide individuals protection against governmental invasion of their privacy in personal information.[2] The Act tried to balance an individual's right to control the use and dissemination of her own personal information and the government's legitimate need to gather and use that same information. In general, the Privacy Act: (1) prohibits disclosure by Federal agencies of any record contained in a system of records, except pursuant to a written request by or with the prior written consent of the individual to whom the record pertains; (2) requires agencies which keep record systems to keep account of disclosures of records and to inform the subjects of such disclosures when they occur; (3) allows subjects of records to see and copy their records, establishes a procedure for amendment of such records, and permits judicial review of agency refusals to amend; (4) requires that any information held be relevant to the agency's official purposes and be accurate, that agencies publish annually a notice of the existence, character, and accessibility of their record systems, and that they take appropriate safeguards to maintain the confidentiality of such records; and (5) allows recordkeeping agencies to promulgate rules on all these subjects.

The provision of the Privacy Act most relevant to this report, 5 U.S.C. § 552a(b), proscribes the sharing of personal information between agencies. It states that "no agency shall disclose any record which is contained in a system of records by any means of communication to any person, *or to another agency,* except pursuant to a written request by, or with prior written consent of, the individual to whom the record pertains."[3] This section then lists a series of exemptions allowing disclosure of records under certain circumstances. The exemptions provide the primary means through which agencies can legally pass an individual's private information amongst themselves.

### Interpretation of 5 U.S.C. 552a(b)

The first critical question in interpreting § 552a(b) is what constitutes an "agency." "Agency," according to the Act itself, means "each authority of the Government of the United States, whether or not it is within or subject to review by another agency," not including Congress or the courts.[4] The courts have interpreted this general definition a number of times. Generally speaking, the courts look primarily at the degree of government control in determining whether or not a particular entity is an "agency," but they can disagree on the bottom line.[5] One court, for example, found that the Federal Home Loan Mortgage Corporation was an agency subject to the Privacy Act primarily because it had a federal charter and a presidentially appointed board.[6] Another court, however, refused to find a federally chartered production credit association to be an agency under the Act.[7] As a consequence of this second ruling, the personal information of individuals held by the credit association could legally be turned over to any federal agency without the threat of liability under the Privacy Act.

Courts have also found that the following special entities do not constitute agencies under the terms of the Privacy Act: an individual government employee,[8] state and local government agencies,[9] the White House Office and those components of the Executive Office of the President whose sole function is to advise and assist the President,[10] grand juries,[11] and national banks.[12] Thus, an individual has no recourse under the Privacy Act when these entities share his personal information with an agency of the federal government.

The Privacy Act's definitions of "records" and "system of records" also limit an individual's ability to restrict the dissemination of his personal information. The Act dictates that "no agency shall disclose any record which is contained in a system of records." It defines "record" as "any item, collection, or grouping of information about an individual that is maintained by an agency…that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual."[13] Additionally, the Act defines "system of records" as a "group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."[14] When reading these definitions back into the text, courts have found that many records containing sensitive personal information are beyond the reach of the Act.[15] For instance, the D.C. Circuit Court held that a "system of records" subject to the Privacy Act only exists when personal information *is actually retrieved* from a database by a personal identifier, not when it *can be retrieved* by a personal identifier.[16] Thus, databases that have not yet yielded individualized records by personal identifier upon the agency's request are not covered by the Privacy Act. Smaller sources of personal information have proven equally unprotected by the Act. A number of courts have held that private notes written by government agents are not considered a "system of records" when kept in personal files and are consequently exempt from the Act.[17]

The courts' strict interpretation of the entities and information covered by the Privacy Act has reduced the scope of the Act's protections against disclosure of personal information, but this reduction is small compared to that achieved through the Privacy Act's numerous exemptions and the Computer Matching Act of 1988.

### Specific Exemptions to 5 U.S.C. 552a(b)

The Privacy Act contains several different kinds of exemptions. One broad type permits disclosure to certain groups within the federal government. Under 5 U.S.C. 552a(b), an agency can disclose its records on an individual to officers and employees within the agency itself, the Bureau of the Census, the National Archives, Congress, the Comptroller General, and various consumer protection agencies. Additionally, the information contained in an agency's records can be disclosed for "civil or criminal law enforcement activity if the activity is authorized by law."[18] This exemption allows an agency, for example, to share its records with the FBI if the records indicate that a law has been broken or could be in the future. And some federal agencies have created enforcement divisions within the agency in order to qualify for the law enforcement exemption to the Act.[19]

The broadest and most controversial exemption is for disclosure pursuant to a "routine use."[20] Under this exemption, federal agencies are permitted to disclose personal information without the consent of the individual so long as the nature and scope of the routine use was previously published in the Federal Register and the disclosure of data was "for a purpose which is compatible with the purpose for which it was collected."[21] Although the exemption was initially inserted to allow for routine information exchange in "housekeeping measures," the potential for abuse was recognized immediately. Despite this recognition and public criticism, agency use of the routine use exemption has steadily expanded.

Under the Act, an agency's "routine use" must be "compatible" with the purpose for which the data was originally collected. But what does "compatibility" require? According to the Office of

Management and Budget (OMB), "compatibility" covers uses that are either (1) functionally equivalent or (2) necessary and proper.[22] The courts, however, have disagreed with some requiring a tighter nexus and some little nexus at all. In a leading case, the Third Circuit took the stricter approach. It criticized an agency for equating "compatibility" with "relevance" to the entity receiving the information and stated that "[t]here must be a more concrete relationship or similarity, some meaningful degree of convergence, between the disclosing agency's purpose in gathering the information and in its disclosure."[23] In a more recent case, the D.C. Circuit took a quite different view. It held that "compatibility" required merely that "a proposed disclosure would not actually frustrate the purposes for which the information was [originally] gathered."[24] It did, however, suggest that its decision depended in part on the identity of the entity to which the information was being disclosed. Luckily, in the law enforcement context, the compatibility rules are clearer. Agencies may—regardless of the original purpose of collection—disclose information for the purpose of investigating or prosecuting possible violations of the law.[25] The compatibility requirement, then, creates little difficulty for routine uses related to terrorism.

Lack of an effective oversight mechanism within the government has also led agencies to push the "routine use" exemption. Although OMB is assigned the task of overseeing agency compliance with the Act, it has done little more than issue guidelines outlining how the Act should be implemented.[26] Additionally, Congress—though considered the major check on agency abuse of routine use determinations—has limited power to oversee agency implementation of routine uses. When a change to a routine use is proposed, the Privacy Act requires that the agency submit a report to House and Senate subcommittees for review.[27] Based upon this report, Congress can recommend changes to the proposed routine use, but it has no actual power—short of legislation—to directly shape it. The agency must then decide whether or not to heed Congress's advice—and many do not. The CIA, for example, proposed one of the broadest of routine uses—one covering all of its systems of records to allow disclosure "whenever necessary or appropriate to enable the CIA to carry out its responsibilities."[28] Congress objected to the rule as overly broad and made a series of recommendations to narrow it. The CIA ignored them, however, and published the routine use as planned. While this type of circumvention has continued for most of the Privacy Act's life, the trend very recently may be toward a slightly narrower construction of the exemption.[29]

Based upon past applications of the routine use exception, it seems likely that future government initiatives promoting increased interagency information sharing to protect national security will meet with little resistance. A routine use need only meet the two aforementioned requirements to be valid: (1) compatible with the purpose of the information collection and (2) published in the Federal Register. A transfer of all information gathered on federal employees for security clearance by an agency to an intelligence agency, like the CIA, would easily satisfy the compatibility requirement, as increasing security is a common goal between them. The Department of Labor, in fact, already lists this type of routine use in the Federal Register. It states that personnel investigation records may be disclosed "[t]o the intelligence agencies of the Department of Defense, the National Security Agency, the Central Intelligence Agency and the Federal Bureau of Investigation for use in intelligence activities."[30] Broadening this routine use to encompass other information that could be useful to counterterrorism intelligence authorities does not appear to be a particularly drastic step given current interpretations of the exemption.

Legislative and judicial challenges to routine use determinations, moreover, are quite rare. Only once has Congress overturned a class of routine uses and claimants must clear high hurdles in court in order to successfully attack one.[31] First, only the injured individual has standing to sue the federal agency responsible for the wrongful disclosure. Second, the claimant must prove that the agency acted willfully or intentionally in disclosing personal information from a record contained in a system of records. Finally, the individual must prove that he suffered an identifiable adverse effect. Only once an individual has jumped these hurdles, will a court reach the issue of the routine use itself and determine whether the disclosure was permissible. A litigant who makes it this far, however, should not rejoice, as she is then faced with overturning an agency determination to which the courts accord much deference.[32]

## Amendment to the Privacy Act: The Computer Matching Act

In today's age of information, data mining has the potential to become one of the government's most powerful tools for analyzing information on terrorism. Congress, however, has restricted the kinds of data mining federal agencies can do. In 1977, the Department of Health, Education and Welfare initiated Project Match to identify federal employees fraudulently receiving welfare payments. In order to further the project, several different federal agencies listed computer matching as a routine use and allowed personal information in their system of records to be disclosed in pursuit of finding waste and fraud. Over the next decade, such computer matching became pervasive. In a 1986 study, the Office of Technology Assessment reported that in 1984, eleven cabinet level departments and four independent agencies conducted 110 separate computer matching programs, consisting of 700 total matches and involving seven billion records.[33] At this time, the House Government Operations Committee determined that:

> the Privacy Act presents only a few procedural barriers to matching and those barriers are easily overcome. The committee is not aware of any computer match that could not be conducted because of Privacy Act disclosure rules. The Office of Technology Assessment found that the "Privacy Act as interpreted by the courts and the OMB guidelines offers little protection to individuals who are the subjects of computer matching."[34]

This widespread disclosure of information across agencies prompted Congress to act in 1988. To address these problems, Congress amended the Privacy Act by passing the Computer Matching Act, which precluded government agencies from treating computer matching as a routine use in most cases. Congress, however, explicitly excluded "matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of Federal personnel."[35] And although these terms are not defined anywhere in the Privacy Act itself, the National Security Act does offer a definition of counterintelligence as "information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities."[36] Thus, so long as an agency lists something like "analyzing information to improve national security or prevent terrorism" as a routine use for the agency's information, a counterterrorism intelligence agency should be able to data mine the agency's records. The compatibility hurdle will pose little problem because of its law enforcement exemption. Only the congressional notification requirement might make such action cumbersome. But once the agency notifies Congress and publishes notice of this general routine use in the Federal Register, all is done.

## Endnotes

[1] Lillian R. BeVier, *Information about Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection,* 4 Wm. & Mary Bill of Rts. J. 455, 481 (1995).

[2] Todd Roberts Coles, *Comment: Does the Privacy Act of 1974 Protect Your Right to Privacy? An Examination of the Routine Use Exemption,* 40 Am. U.L. Rev. 957, 969 (1991).

[3] Privacy Act of 1974, 5 U.S.C. § 552a(b) (1988).

[4] 5 U.S.C. § 551(1).

[5] Courts consider the extent of day-to-day governmental supervision, the existence of federal reporting requirements and federal chartering, and the presence of federal employees when determining whether there is sufficient government control to call the entity an "agency."

[6] Rocap v. Indiek, 539 F.2d 174 (D.C. Cir. 1976).

[7] U.S. v. Haynes, 620 F. Supp. 474 (M.D. Tenn. 1985).

[8] Petrus v. Bowen, 833 F.2d 581 (5th Cir. 1987).

[9] Perez-Santos v. Malave, 23 Fed. Appx. 11 (1st Cir. 2001); Ortez v. Washington County, 88 F.3d 804 (9th Cir. 1996).

[10] Flowers v. Executive Office of the President, 142 F. Supp. 2d 38 (D.D.C. 2001).

[11] Standley v. Department of Justice, 835 F.2d 216 (9th Cir. 1987).

[12] U.S. v. Miller, 643 F.2d 713 (10th Cir. 1981).

[13] 5 U.S.C. § 552a(a)(4).

[14] *Id.* at (a)(5).

[15] BeVier, *supra* note 1, at 482.

[16] Henke v. United States DOC, 83 F.3d 1453 (D.C. Cir. 1996).

[17] Bowyer v. United States Dep't of Air Force, 804 F.2d 428 (7th Cir. 1986); Chapman v. NASA 682 F.2d 526 (5th Cir. 1982).

[18] 5 U.S.C. § 552a(b)(7).

[19] Coles, *supra* note 2, at 980.

[20] 5 U.S.C. § 552a(b)(3).

[21] Id. at (a)(7).

[22] OMB Guidelines, 52 Fed. Reg. 12,900, 12,993 (1987).

[23] Britt v. Naval Investigative Service, 886 F.2d 544, 547-50 (3rd Cir. 1989).

[24] United States Postal Serv. V. Nat'l Ass'n of Letter Carriers, 9 F.3d 138, 144 (D.C. Cir. 1993).

[25] OMB Guidelines, 40 Fed. Reg. at 28,953, 28,955; 120 Cong. Rec. 36,967, 40,884 (1974) (remarks of Congressman Moorhead).

[26] In many instances, the OMB guidelines themselves suggest "routine uses" that appear to be incompatible with the Privacy Act's protections.

[27] 5 U.S.C. § 552a(r).

[28] Coles, *supra* note 2, at 988.

[29] *See* Pontecorvo v. FBI, No. 00-1511, slip op. at 13-15 (D.D.C. Sept. 30, 2001) (denying agency summary judgment and ordering discovery to determine whether the agency "overstepped [the] explicit restrictions" contained in its routine use) at http://www.usdoj.gov/04foia/1974condis.htm#routine; Memorandum on Privacy and Personal Information in Federal Records, 34 Weekly Comp. Pres. Doc. 870 (May 14, 1998).

[30] 67 F.R. 16816 (2002); *See also* 64 FR 30106 (1999) (Routine uses for the Department of Education).

[31] Coles, *supra* note 2, at 992-96.

[32] Dep't of the Air Force, Scott Air Force Base, Ill. v. FLRA, 104 F.3d 1396 (D.C. Cir. 1997).

[33] Coles, *supra* note 2, at 982.

[34] H.R. Rep. No. 100-802 at 5 (1988), *reprinted in* 1988 U.S.C.C.A.N. 3107, 3111.

[35] 5 U.S.C. 552a(a)(8)(B)(vi).

[36] 50 U.S.C. 401a(3) (2001).

# Federal Legal Constraints on Electronic Surveillance

**By Jeffrey H. Smith**
**Partner, Arnold & Porter**

**and**

**Elizabeth L. Howe**
**Summer Associate, Arnold & Porter**

## Executive Summary

The goal of constitutional, statutory, and regulatory restrictions on the power of government agents to conduct searches and seizures is to strike a balance between the privacy rights of individuals and public safety. In the wake of September 11th, some have criticized these restrictions as impeding the ability of law enforcement and intelligence organizations to gather the information necessary to prevent terrorist attacks and identify threats to national security. As new models of information-collection, dissemination, and analysis are considered, one of the primary challenges will be to devise a system that both satisfies this demand for improved information-gathering and includes sufficient means of protecting individual privacy rights.

This report does not take a position on the appropriate balance between individual privacy rights and national security interests. Rather, this report outlines the existing legal constraints imposed by the U.S. Constitution, federal statutes, and Department of Justice guidelines regarding the government's search and seizure power, particularly the ability to conduct electronic surveillance. This report also asks, but does not resolve, the question of whether the existing legal framework can adequately addresses the difficult and novel issues created by evolving technologies and new national security concerns.

Fourth Amendment jurisprudence establishes that government agents wishing to conduct electronic surveillance within the U.S. of American citizens or permanent resident aliens for a domestic law enforcement purpose generally must obtain a warrant from a court issued pursuant to a finding of probable cause. These Fourth Amendment protections also extend to American citizens subjected to electronic surveillance by the U.S. government in a foreign location. On the other hand, the Supreme Court's Fourth Amendment jurisprudence has not addressed the extension of similar protection to targets of U.S. government surveillance conducted for a "foreign intelligence" purpose (a term defined below), even if the target is a U.S. citizen and the surveillance is carried out on American soil.[1]

Reflecting Fourth Amendment jurisprudence's distinction between government actions taken for domestic law enforcement and "foreign intelligence" purposes, two different statutes apply to electronic surveillance: Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), and the Foreign Intelligence Surveillance Act of 1978 ("FISA"). Title III outlines the procedures required for conducting searches and seizures for domestic law enforcement purposes, while FISA pertains to "foreign intelligence" activity by the government. The USA PATRIOT Act's recent

amendments of these statutes, such as broadening the definition of "foreign intelligence" to include international terrorism, have reduced some of the barriers to electronic surveillance by the government and thus caused some critics to question the constitutionally of these statutes.

Electronic surveillance by the FBI is also regulated by guidelines issued by the Attorney General. The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (the "General Crimes Guidelines") primarily pertain to investigation of organizations originating in the U.S. The Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (the "Foreign Intelligence Guidelines") govern investigations of foreign powers, international terrorism organizations with foreign origins (*e.g.*, al Qaeda), and their agents (including U.S. and non-U.S. persons).[2] Both sets of guidelines pertain to investigations that occur on U.S. soil and investigations that may involve U.S. persons. However, in the international terrorism context, the General Crimes Guidelines seem to apply when the investigation is for a law enforcement purpose, while the Foreign Intelligence Guidelines are used for intelligence investigations. It is unclear which guidelines would apply to an investigation that serves both law enforcement and intelligence objectives. Little information is available regarding the Foreign Intelligence Guidelines since they are classified, but the General Crimes Guidelines are publicly available and the subject of considerable debate. Recent revisions to the General Crimes Guidelines by Attorney General John Ashcroft, including expansion of the permissible types of Internet-based investigations and increased authority for FBI agents to attend public events and meetings, have received much attention and criticism.

## A Note on Terminology

In Fourth Amendment jurisprudence, three distinctions are important. They are:

### 1. U.S. Persons v. Non-U.S. Persons

U.S. citizens and permanent resident aliens (commonly referred to as "U.S. persons") often receive greater protection than is afforded to non-U.S. persons. For instance, FISA requires that the government obtain a court order if foreign intelligence communications of a U.S. person are likely to be intercepted; however, if the surveillance will only intercept communications of non-U.S. persons, the government can conduct the surveillance for up to one year without a court order, provided that the Attorney General certifies that only foreign powers will be targeted and that the required minimization procedures will be followed.[3]

### 2. Electronic Surveillance Conducted within the U.S. v. a Foreign Country

Legal distinctions often rest on whether electronic surveillance activity is being conducted on U.S. soil or in a foreign country. While Congress has enacted statutes such as Title III and FISA to address surveillance conducted within the U.S., Congress has not passed any statutes limiting electronic surveillance performed by the U.S. government in a foreign country.[4] For example, FISA governs the collection of "foreign intelligence," which is defined as "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities."[5] Even though FISA focuses on "foreign intelligence," FISA only applies to surveillance performed within the U.S. In other cases, how-

ever, a surveillance target's rights do not hinge on the location of the surveillance. For instance, the Fourth Amendment applies to U.S. citizens targeted for surveillance by the U.S. government even when the surveillance takes place in a foreign country.

### 3. Law Enforcement v. Intelligence

The final distinction used in the regulation of electronic surveillance is one of law enforcement versus intelligence. When the government conducts electronic surveillance to gather information for eventual use as evidence at a criminal proceeding, the government's actions are "law enforcement" and fall within the reach of Title III. On the other hand, when the intent is to collect "foreign intelligence" or to prevent an action from occurring that would jeopardize national security, it is "intelligence" and FISA applies. Although surveillance with respect to international terrorism involves aspects of both "law enforcement" and "foreign intelligence," courts have treated international terrorism as falling within the category of "foreign intelligence" when the investigation only incidentally collects law enforcement information.[6]

## Constitutional Restrictions: The Fourth Amendment

The Fourth Amendment serves as the primary constitutional mechanism for limiting governmental invasions of individuals' privacy. Enacted in reaction to abuses committed under British colonial rule, the Fourth Amendment provides that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[7]

The Fourth Amendment does not function as an absolute bar to government action, but rather only restrains government action deemed "unreasonable." The primary remedy for violation of the Fourth Amendment is exclusion of the improperly obtained evidence and any further evidence gathered based on the improperly obtained evidence.[8]

The Fourth Amendment covers two types of government action: "searches" and "seizures." In the absence of textual definitions, the Supreme Court has defined a "search" as the infringement of an individual's reasonable expectation of privacy and a "seizure" as the meaningful interference with an individual's possessory interest in property.[9] The Supreme Court, since 1967, has held that electronic surveillance qualifies as a "search" under the Fourth Amendment.[10]

### I. Requirements of the Fourth Amendment

The Fourth Amendment contains two basic elements: (1) a reasonableness requirement for searches and seizures, and (2) restrictions on the issuance of warrants. The Constitution does not define "unreasonable searches and seizures," so courts decide whether a search or seizure is reasonable on a case-by-case basis considering previous caselaw and the totality of the facts and circumstances.[11] Courts balance the degree of intrusion into a person's privacy with the governmental interests asserted; thus, the Fourth Amendment includes the flexibility to expand the scope of permissible

invasions of privacy when the public interest demands and to contract the range of reasonable government action when the threat to the public interest recedes. For example, in *Skinner v. Railway Labor Executives' Association,* the Supreme Court found that the Fourth Amendment rights of railroad workers were not violated by mandatory drug and alcohol testing conducted in the absence of a warrant or particularized suspicion because the interest in railroad safety justified the intrusion into the workers' privacy.[12]

Whether a particular search or seizure is reasonable may also turn on whether the government agents involved have complied with the Fourth Amendment's warrant requirement.[13] Compliance with the Fourth Amendment generally requires obtaining a warrant prior to a search or seizure, but the Supreme Court in interpreting the Fourth Amendment has carved out exceptions to the requirement of a warrant, including (1) search or seizure of items in the "plain view" of a law enforcement officer,[14] (2) searches conducted incident to valid arrests,[15] and (3) searches involving national security.[16]

If one of the exceptions to the warrant requirement does not apply, then the government agent wishing to conduct the search or seizure must obtain a warrant. The Fourth Amendment only provides for issuance of a warrant if "probable cause" exists. Probable cause is a flexible standard that adjusts in light of the totality of the circumstances of a particular case, but probable cause generally is found when the facts and circumstances known to the government agent are sufficient to warrant a person of reasonable caution to believe that an offense has been or is being committed.[17] The Fourth Amendment also requires that a warrant describe with particularity the place of the search and the persons or items to be seized.

## II. The Fourth Amendment as Applied to Electronic Surveillance

In the 1967 case *Katz v. U.S.,* the Supreme Court held that electronic surveillance can qualify as a search or seizure to which Fourth Amendment protections apply, but later Fourth Amendment jurisprudence has more specifically defined the reach of the Fourth Amendment.[18] The Supreme Court's holding in *Katz* case only addressed the question of electronic surveillance of a U.S. person for a law enforcement purpose, and the Court explicitly left open the possibility that the Fourth Amendment might not apply to surveillance conducted for national security (or "intelligence") purposes. Five years later, the Supreme Court considered the issue of surveillance for intelligence-gathering and held that the Fourth Amendment did apply when the targets of the surveillance lacked ties to a foreign power.[19]

### A. Electronic Surveillance for Domestic Law Enforcement

Prior to 1967, electronic surveillance (at that time, only wiretapping) did not fall within the scope of activity covered by the Fourth Amendment. In 1928, the Supreme Court in *Olmstead v. U.S.* ruled that the protections of the Fourth Amendment did not apply to electronic surveillance when no physical invasion of the target's personal space occurred and that words were not tangible things capable of being seized.[20] Forty years later, the Supreme Court reversed course with its decision in the *Katz v. U.S.*, holding that the protections of the Fourth Amendment do extend to cases of electronic surveillance conducted for domestic law enforcement purposes in which no physical intrusion has occurred.[21] The *Katz* opinion represented a doctrinal shift by the Court away from a focus

on property rights (i.e., whether there was a physical invasion of the target's personal space) to one of privacy protection; as the Court noted, the Fourth Amendment "protects people, not places."[22] In his dissent to the *Olmstead* decision, Justice Brandeis foreshadowed this transition in Fourth Amendment doctrine, cautioning that constitutional protections must keep pace with technology in order to prevent invasions of individual liberty: "To protect [the right to be let alone], every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[23]

In his concurrence to the *Katz* opinion, Justice Harlan established a two-part test,[24] which the Supreme Court has subsequently adopted,[25] for determining whether a sufficient privacy interest exists to merit Fourth Amendment protection: (1) the person subjected to the search or seizure must have a "subjective" (actual) expectation of privacy, and (2) the person's subjective expectation of privacy must be one that society is prepared to recognize as "reasonable." The application of the "reasonable expectation of privacy" test to interception of electronic communications has raised some concern because courts might base their determinations on technological distinctions unknown to the average computer user but which arguably reflect different subjective expectations of privacy. As a result, individuals could have misplaced expectations of privacy for electronic communications such as e-mail.[26] For instance, a court might extend Fourth Amendment protection to one individual's e-mail communications because he or she uses highly sophisticated encryption software while denying similar protection to an e-mail user unwittingly employing a low-grade encryption program that is automatically installed as part of the e-mail software.

**B. Electronic Surveillance for Intelligence Purposes**

The *Katz* court also noted, but left unresolved, the possibility that the Fourth Amendment might not apply to electronic surveillance conducted for domestic national security purposes. Five years later, the *Supreme Court in United States v. United States District Court for the Eastern District of Michigan* (commonly referred to as the *Keith* case) answered this question by rejecting a domestic national security exception to the Fourth Amendment.[27] In *Keith*, three defendants accused of conspiring to bomb a U.S. government building challenged the use of electronic surveillance without a warrant. Even though the government conducted the surveillance for the purpose of intelligence, not criminal law enforcement, the Court still held that the surveillance violated the Fourth Amendment because the defendants did not have a connection to a foreign power.

The *Keith* decision still leaves open the question of whether, as a matter of constitutional law, Fourth Amendment protections apply to U.S. or foreign organizations that do have connections to foreign powers or their agents.[28] Although the Supreme Court has not addressed the applicability of the Fourth Amendment to electronic surveillance conducted for a "foreign intelligence" purpose, several circuit courts have acknowledged the existence of a foreign intelligence exception to the warrant requirement for searches conducted within the U.S. which target foreign powers or their agents.[29] Circuit courts have also indicated that the protections provided by FISA (at least prior to its amendment by the USA PATRIOT Act[30]) satisfy any constitutional requirements that might apply in the context of conducting surveillance of domestic organizations with foreign connections.[31] A district court has also found a foreign intelligence exception to the warrant requirement with respect to activities conducted overseas when probable cause existed to believe that the U.S. citizen targeted was an agent of a "foreign power." [32]

## Statutory Restrictions

Following the Supreme Court's main decisions outlining the constitutional limitations on electronic surveillance, Congress enacted additional statutory restrictions that codified and extended the protections afforded by the Fourth Amendment. The Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"),[33] passed in response to the Supreme Court's ruling in *Katz*, sets forth the statutory guidelines for obtaining a warrant to conduct electronic surveillance for domestic law enforcement purposes. FISA[34] sets forth the procedures the government must follow in obtaining warrants to conduct foreign intelligence surveillance within the U.S.

Although the statutory framework established by Title III and FISA rests on a distinction between electronic surveillance for the purpose of domestic law enforcement versus foreign intelligence, these lines are not as clear in the post-September 11th conception of national security. Thus, one question to consider is whether this statutory framework remains the appropriate one for regulating the use of electronic surveillance. As Senator Patrick Leahy has observed, with the passage of the USA PATRIOT Act, the United States is "enter[ing] new and unchartered territory by breaking down traditional barriers between law enforcement and foreign intelligence."[35]

### I. Law Enforcement Surveillance in the United States: Title III of the Omnibus Crime Control and Safe Streets Act of 1968

One year following the Supreme Court's ruling in *Katz* that wiretapping falls within the scope of activity governed by the Fourth Amendment, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act ("Title III") to detail further the limits applying to wire, oral, and electronic surveillance by the government for the purpose of domestic criminal investigations.

#### A. Title III Generally

Title III limits the ability of law enforcement officials to conduct electronic and other surveillance in a number of ways. First, Title III only permits surveillance for certain specified offenses.[36] However, this bar has been lowered over time by the marked expansion of the list of enumerated offenses.[37] Second, a law enforcement officer wanting to conduct wire or oral surveillance must first obtain the approval of a senior Justice Department official. However, any government attorney may approve an application for interception of electronic communication.[38] After receiving such approval, a law enforcement officer must then apply for a court order authorizing the surveillance. Before issuing a court order a judge must find probable cause that: (1) an enumerated offense is being, or will be, committed and that a wiretap will obtain particular communications concerning that offense; (2) law enforcement officials have exhausted all reasonable and normal investigative procedures and (3) the facilities intercepted are or will be used in the commission of the offense or are leased to, listed in the name of, or commonly used by the person named by the court order.[39] Title III's requirement of a probable cause finding is one of the key features that distinguishes electronic surveillance conducted pursuant to Title III as opposed to FISA. When issuing a court order, the judge must specify, among other things: (1) the identity of the person whose communications are to be intercepted; (2) the nature and location of the facilities to be intercepted; (3) the type of

communication to be intercepted and the offense to which it relates; and (4) the period of time for which the interception is authorized.[40]

The judge issuing the court order also has the discretion to require completion of periodic reports regarding the surveillance.[41] Title III also includes a "minimization" requirement, which mandates that the law enforcement officer must conduct the surveillance in a manner that reduces the interception of communications beyond the scope of the court order.[42] Unlike FISA intercepts, Title III surveillance requires that, within a reasonable time after the completion of the surveillance, the government must notify the target of the surveillance that such monitoring has occurred.[43] In keeping with the Fourth Amendment, the judicial remedy for violation of Title III is excluding the improperly obtained information as evidence.

### B. Use of Roving Wiretaps under Title III

In 1986, Congress amended Title III with its passage of the Electronic Communications Privacy Act (ECPA).[44] Under the amended Title III, judges are permitted to issue court orders authorizing "roving wiretaps," in which government agents target their surveillance on a particular individual rather than on a particular telephone or other communication device.[45] In 1998, Congress lowered the standard for obtaining authorization for a Title III roving wiretap by no longer requiring that a target have the intent to thwart electronic surveillance by the government, but rather only that the target's behavior had such an effect. Title III does require that law enforcement must determine that the target actually used the particular device to be monitored or was "reasonably proximate to the instrument through which such communication will be or was transmitted."[46]

### C. Use of Pen Registers and Trap-and-Trace Devices under Title III

The ECPA also amended Title III to allow for the use of pen registers and trap-and-trace devices. Pen registers and trap-and-trace devices allow a government agent to obtain the telephone numbers that a particular telephone dials or from which it receives calls.[47] A government attorney, law enforcement officer, or investigative officer may apply for an order for use of a pen register or trap-and-trace device.[48] ECPA states that such an order shall be approved so long as the government certifies that the "information likely to be obtained is relevant to an ongoing 'criminal investigation.'"[49] The Supreme Court has found that the use of pen registers and trap-and-trace devices to obtain telephone numbers dialed or received by a telephone line does not constitute a search under the Fourth Amendment. According to the Supreme Court, individuals do not have a reasonable expectation of privacy in telephone numbers because telephone companies routinely record telephone numbers for the purpose of billing.[50] The Supreme Court has also explained that the low expectation of privacy also stems from the fact that the content of telephone communications are not revealed by pen registers and trap-and-trace devices.[51]

## II. Foreign Intelligence Surveillance in the U.S.: Foreign Intelligence Surveillance Act of 1978 (FISA)

Whereas Title III covers electronic surveillance conducted for domestic law enforcement purposes, the Foreign Intelligence Surveillance Act of 1978 (FISA) governs surveillance conducted for the purpose of gathering foreign intelligence. Congress enacted FISA in 1978 amidst concerns that the

dearth of effective judicial or statutory restraints on foreign intelligence gathering had opened the door to increased use of electronic surveillance conducted without a warrant and with little or no actual connection to national security and foreign intelligence.[52]

### A. FISA Generally

In some circumstances, FISA permits the government to conduct electronic surveillance without first obtaining a court order. The electronic surveillance must be of "means of communication used exclusively between or among foreign powers," which FISA defines as including foreign governments, groups engaged in international terrorism, and foreign-based organizations not substantially composed of U.S. persons. There also must not be a substantial likelihood that the surveillance will intercept communications to which a U.S. person is a party.[53] The Attorney General must submit a certification to this effect to the Foreign Intelligence Surveillance Court (FISC), but this certification remains sealed unless the government chooses to request a court order or the target of the surveillance challenges the legality of the surveillance.[54] Unlike Title III surveillance targets, however, the subjects of FISA searches do not receive notice of the surveillance upon completion of the monitoring, so FISA targets may never learn that their privacy interests have been compromised.[55] FISA allows surveillance conducted pursuant to Attorney General certification (as opposed to a court order) for up to one year. If the government wishes to conduct surveillance of a foreign power for more than one year, the government must apply for a FISC court order according to the procedures described below.[56]

If a government agent wishes to undertake electronic surveillance of a U.S. citizen or permanent resident alien ("U.S. person") for foreign intelligence purposes, FISA requires the agent to obtain a court order issued by the FISC. Originally, the FISC was composed of seven district court judges selected by the Chief Justice of the Supreme Court, but the USA PATRIOT Act's recent amendment of FISA increases the number of judges on the FISC to eleven.[57] A single FISC judge determines whether to grant or deny the government's request for a court order.[58] If the FISC judge denies the government's request, the government may appeal the decision to a three-member "court of review" composed of federal district court and appellate judges. If the court of review denies the government's request, the government can petition the Supreme Court to review the case.[59] FISC proceedings are conducted in secrecy to protect national security interests.[60] Since the targets of FISA-based searches, unlike Title III targets, do not receive *ex post* notification of the surveillance, FISC decisions are rarely challenged by surveillance targets.

To issue a warrant under FISA, a FISC judge must find probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power. Since FISA imposes a lower probable cause threshold than Title III for issuance of a warrant, information obtained under a FISC warrant for foreign intelligence purposes cannot be used for domestic law enforcement as a matter of constitutional law.[61] The recent amendment of FISA by the USA PATRIOT Act, however, has blurred the lines between warrants obtained under Title III and FISA by changing the language from *the purpose* to *a purpose,* thus broadening somewhat the scope of activity for which a FISA warrant may issue.

Previously, a government agent could only receive a FISA warrant if he or she demonstrated that "*the* purpose of the surveillance is to obtain foreign intelligence information" (emphasis added).

The USA PATRIOT Act, however, changes this standard and permits warrants to issue if "*a* significant purpose of the surveillance is to obtain foreign intelligence information" (emphasis added).[62] The Administration argued that such a change was necessary because the previous language forced the government to make a decision at the outset of an investigation as to whether the investigation would be for law enforcement or intelligence. As a result, an increasing number of investigations were conducted within the Title III framework, causing less foreign intelligence to be collected.[63] This resistance to foreign intelligence collection has been cited by some Administration officials as a reason why the FBI denied agent requests to conduct surveillance of Zacarias Moussaoui, the so-called "twentieth" September 11th hijacker.[64] On the other hand, some critics have argued that a government agent wishing to conduct electronic surveillance for the primary purpose of investigating criminal activity, and only secondarily for the collection of foreign intelligence, will bypass the constitutional requirement of heightened probable cause required for domestic law enforcement by obtaining a warrant under FISA.[65]

In addition to securing a warrant from the FISC, a government agent seeking to conduct electronic surveillance of a U.S. person must follow certain "minimization procedures" established by the Attorney General. These minimization procedures require the adoption of techniques designed to "minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting U.S. person consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[66]

### B. Roving Wiretaps under FISA

The USA PATRIOT Act amends FISA to allow the use of roving wiretaps, in which government agents conduct electronic surveillance of a particular individual, as opposed to a specific telephone line. FISA adopts the same "effect of thwarting surveillance" standard for approving roving wiretaps used in gathering foreign intelligence as used in the Title III context, but FISA does not include a provision parallel to Title III's requirement that law enforcement must determine that the target actually used the particular device to be monitored or was "reasonably proximate to the instrument through which such communication will be or was transmitted."[67]

### C. Pen Registers and Trap-and-Trace Devices under FISA

FISA also allows the use off pen register and trap-and-trace surveillance techniques, which enables the source of a communication to be identified. The recently enacted USA PATRIOT Act extends the use of these processes to Internet communications such as e-mail.[68] Some critics have argued, however, that simply extending FISA's pen register and trap-and-trace regulations to Internet communications fails to address the technological distinctions between forms of communications, distinctions which have important legal significance.[69]

The statutory authorization for use of pen registers and trap-and-trace devices only extends to identifying the "source" of a communication, not the "content" of the communication itself.[70] In the context of telephone communications, pen register and trap-and-trace technologies record the telephone numbers of the persons involved in a conversation but do not intercept any content of the conversations themselves. Since telephone companies routinely record the telephone numbers dialed to and from a telephone user for billing purposes, courts have held that telephone users have

a lower expectation of privacy in the telephone numbers they dial than in the content of their telephone conversations. As a result, government agents wishing to obtain the telephone numbers dialed by a surveillance target through the use of pen register or trap-and-trace technologies do not have to make a showing of probable cause, but rather only must certify that the information obtained may be relevant to an ongoing criminal investigation.

In contrast, the distinction between "source" and "content" information is not as clear in the context of Internet communications. For instance, the subject lines of e-mails frequently reveal at least some information regarding the substance of the e-mail. However, e-mail headers listing the sender and recipient of an email also commonly include e-mail subject lines. Since the USA PATRIOT Act does not define the term "content," it is unclear whether the subject line of an e-mail should be treated as "source" information along with the other information listed in an e-mail header, or whether individual parts of the header should be separately labeled as "source" or "content" information.[71]

### D. Physical Searches under FISA

Since 1994, FISA has also permitted government agents to conduct unconsented physical searches in addition to electronic or other surveillance.[72] FISA defines a "physical search" as "any physical intrusion within the United States into premises or property (including examination of the interior of property by technical means) that is intended to result in a seizure, reproduction, inspection, or alteration of information, material or property."[73] FISA permits physical searches when the Attorney General certifies that there is no "substantial likelihood" that a U.S. person will be involved or, if a U.S. person will be the target of a physical search, when the FISC issues a court order authorizing the search. Government agents acting under either Attorney General certification or FISC court order must adopt procedures designed to minimize the intrusion into the target's privacy and the collection of information not pertaining to foreign intelligence.[74]

## III. Electronic Surveillance outside the U.S.: Executive Order 12,333

Congress has not imposed statutory limits on electronic surveillance conducted outside the U.S., but Executive Order 12,333 does speak to the targeting of U.S. citizens in "intelligence" activities conducted abroad.[75] Executive Order 12,333 issued by President Reagan in 1981 and still in force, governs the "intelligence" activities of the U.S. government and vests in the Attorney General considerable responsibility for monitoring such activities and ensuring the "protection of constitutional rights." Section 2.5 of Executive Order 12,333 requires that if a U.S. citizen or resident alien is targeted for surveillance by the U.S. operating overseas, the Attorney General must find probable cause to believe the U.S. person to be targeted by the surveillance is an agent of a foreign power.[76] Thus, before a government agent can use intrusive means to target U.S. citizens overseas for intelligence purposes, he or she must obtain prior authorization from the Attorney General.

Courts recognizing a "foreign intelligence" exception to the warrant requirement have noted in their decisions the need to obtain prior authorization from the President or the Attorney General. In discussing this authorization requirement, courts have made frequent reference to Section 2.5 of Executive Order 12,333. However, the courts have not addressed whether the Fourth Amendment would require such authorization in the absence of Executive Order 12,333.[77]

## The Attorney General's Guidelines

In addition to the Fourth Amendment, Title III and FISA, guidelines issued by the Attorney General also limit the ability of the FBI to conduct electronic surveillance. In essence, the Attorney General's guidelines are intended to be "operational roadmaps. . . ,clear in authority and clear on the limitations" of particular investigative techniques used by FBI agents that may be intrusive upon individuals' First Amendment, Fourth Amendment, and other privacy rights.[78]

### I. History of the Attorney General's Guidelines

Prior to the creation of the first Attorney General's guidelines in 1976, concerns had been mounting that the FBI was using its investigative powers to infringe upon the First Amendment rights of the NAACP, suspected Communists, etc. These fears were confirmed by the findings of the Church Committee, convened by the U.S. Senate to investigate alleged abuses by the FBI. The following year Attorney General Edward Levi responded by issuing the FBI Domestic Security Guidelines. In 1980, Attorney General Benjamin Civiletti broadened the scope of the guidelines and renamed them the General Crimes, Racketeering, and Criminal Intelligence Guidelines. Attorney General William French Smith weakened the restrictions imposed on the FBI by lowering the threshold for conducting a full investigation to a "reasonable indication" of criminal activity and by creating a new category of investigation, the "limited preliminary inquiry." Subsequent Attorneys General have made minor modifications to the guidelines, with the most significant changes being instituted in May 2002 by Attorney General John Ashcroft.[79]

### II. Structure of the Guidelines

The Attorney General's guidelines are provided in two separate documents:

(1) "The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations," and (2) the "Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations."[80] While investigations under both sets of guidelines may involve U.S. persons and occur on U.S. soil, the General Crimes Guidelines are understood to apply to investigations of organizations originating in the U.S. (*e.g.*, white supremacists), whereas the Foreign Intelligence Guidelines govern investigations of foreign powers, international terrorism organizations with foreign origins (*e.g.*, al Qaeda), and their agents (including U.S. and non-U.S. persons).

However, this distinction is less clear following Attorney General Ashcroft's addition of a section to the General Crimes Guidelines entitled "Counterterrorism Activities and Other Authorization," which authorizes the use of certain modes of investigation with respect to terrorists, both foreign and domestic in origin.[81] In the international terrorism context, a different line seems to be drawn between the General Crimes and Foreign Intelligence Guidelines in the context of international terrorism; namely, the General Crimes Guidelines appear to govern the law enforcement aspects of international terrorism investigations, while the Foreign Intelligence Guidelines seem to pertain to intelligence-oriented investigations. The Foreign Intelligence Guidelines apply to "all . . . *intelligence* investigations of international terrorism conducted by the FBI pursuant to Executive Order 12333" (emphasis added).[82] However, the General Crimes Guidelines' new section on "Counterterrorism

Activities and Other Authorizations," which regulates investigations of "terrorist acts against the United States and its people," describes the activities governed by that section as "law enforcement activities."[83] This suggests that the difference between the General Crimes and Foreign Intelligence Guidelines with respect to international terrorism is whether the activity is conducted for a law enforcement or intelligence purpose. However, as previous courts have noted in the Fourth Amendment context, international terrorism activities can simultaneously serve law enforcement and intelligence purposes.[84] It is unclear which guidelines the FBI would apply in such a situation. For instance, the FBI might, as a rule, choose one set of guidelines over the other in cases of overlap, or the FBI might follow the set of guidelines applying to the predominate purpose of the investigation.

Both the General Crimes and Foreign Intelligence Guidelines address issues such as: (1) the FBI's use of particular investigation techniques; (2) what findings must be made before such techniques may be authorized; (3) the purposes for which such investigations may be conducted; and (4) the extent to which information obtained may be recorded and disseminated. The guidelines also include provisions for minimizing the extent of the FBI's intrusion into the privacy of a target, particularly if the target is a U.S. person.

## III. Revision of the Guidelines

The new General Crimes Guidelines issued by Attorney General Ashcroft in May 2002 contain a number of revisions that have been challenged as too intrusive into individuals' privacy and undermine individuals' comfort in speaking freely and openly regarding political or religious subjects.[85] First, the new guidelines expand the ability of the FBI to use the Internet in its investigations by allowing the FBI to conduct "topical research," in which online searches are executed using broad search terms such as "anthrax." Concerns have been raised that topical searches might be conducted using political or religious terms, such as "Palestinian rights." In addition, FBI agents may now "surf" the Internet as any member of the public might, including visiting chat rooms, public Websites and bulletin boards, even in the absence of any indication of criminal activity. The guidelines also authorize the FBI to "mine" privately-owned commercial databases, such as those used by telemarketers, without requiring the government agent to demonstrate a suspicion of criminal activity. Finally, the new guidelines permit FBI agents to visit any place and attend any event open to the public for the purpose of detecting or preventing terrorist activity, even if the FBI lacks any evidence of criminal activity.

Considerably less is known about the Foreign Intelligence Guidelines than the General Crimes Guidelines since the Foreign Intelligence Guidelines are classified and are publicly available only in a highly redacted form. Thus, it is difficult to ascertain what changes, if any, should be made to the Foreign Intelligence Guidelines. However, one aspect of the Foreign Intelligence Guidelines that may be the subject of revision is the applicability of the Foreign Intelligence Guidelines to international terrorism investigations. In light of the recently expanded role of the General Crimes Guidelines in the international terrorism context, it is unclear how the FBI will decide which guidelines to follow when an international terrorism investigation serves both law enforcement and intelligence purposes.

## Endnotes

[1] *See U.S. v. Bin Laden,* 126 F. Supp. 2d 264, 271-72 (S.D.N.Y. 2000) (observing that "[n]o court has considered the contours of [the foreign intelligence] exception when the searches at issue targeted an American citizen overseas," although "[c]ircuit courts . . . have affirmed the existence of a foreign intelligence exception to the warrant requirement for searches conducted within the United States which target foreign powers or their agents").

[2] *See* Jerry Berman and James X. Dempsey, *CDT's Guide to the FBI Guidelines: Impact on Civil Liberties and Security—The Need for Congressional Oversight,* June 26, 2002, at 10.

[3] 50 U.S.C. § 1802 (2002).

[4] See Center for Democracy & Technology, *The Nature and Scope of Governmental Electronic Surveillance Activity,* Sept. 2001, *available* at http://www.cdt.org/wiretap/wiretap_overview.html.

[5] *See* Charles Doyle, The USA PATRIOT Act: A Legal Analysis, CRS Rpt. RL31377 (Apr. 15, 2002), at 12, *available* at http://www.fas.org/irp/crs/RL31377.pdf (quoting Section 902 of the USA PATRIOT Act).

[6] *See Bin Laden,* 126 F. Supp. 2d at 278 (noting that foreign intelligence collection with respect to international terrorists often uncovers evidence of crimes, but that that courts have still treated such activity as "foreign intelligence" if the collection of evidence of criminal activity was only "incidental" to foreign intelligence collection). In the USA PATRIOT Act, Congress formally recognized "international terrorism" as within the scope of "foreign intelligence" activity by amending the definition of "foreign intelligence" to include "information relating to . . . international terrorist activities." *See* Doyle, *supra* note 5, at 12 (citing section 902 of the USA PATRIOT Act).

[7] U.S. CONST. amend. IV.

[8] *See Weeks v. U.S.,* 232 U.S. 383 (1914) (establishing the "exclusionary rule," which provides that information or items obtained pursuant to a violation of constitutional rights should be excluded from evidence); *see also Mapp v. Ohio,* 367 U.S. 643 (1961) (extending the exclusionary rule to constitutional violations committed by state government agents). In some contexts, individuals sustaining a violation of their Fourth Amendment rights may receive monetary damages. *See Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics,* 403 U.S. 388 (1971).

[9] *See U.S. v. Jacobsen,* 466 U.S. 109, 113 (1984).

[10] *See Katz v. U.S.,* 389 U.S. 347 (1967).

[11] *See Chimel v. California,* 395 U.S. 752, 765 (1969).

[12] 489 U.S. 602 (1989). Government agents have even been permitted to enter private residences-which are afforded the "most stringent protection" under the Fourth Amendment-without a warrant if exigent circumstances, such as the threat of a suspect's escape or the possible destruction of evidence, are present. *U.S. v. Martinez-Fuerte,* 428 U.S. 543, 561 (1976); *see Minnesota v. Olson,* 495 U.S. 91, 100 (1990).

[13] *See U.S. v. U.S. Dist. Ct. for the E. Dist. of Michigan,* 407 U.S. 297, 315 (1972).

[14] *See Coolidge v. New Hampshire,* 403 U.S. 443 (1971).

[15] *See U.S. v. Edwards,* 415 U.S. 800 (1974).

[16] The national security exception has been narrowly drawn to apply only in instances of immediate and grave peril to the nation and must be invoked by special authorization of the Attorney General or the President. The national security exception is available only in cases of foreign security, not domestic security, and the contours of the exception are more specifically outlined by statute. *See infra* discussion of Title III of the Omnibus Crime Control and Safe Streets Act (concerning domestic law enforcement) and the Foreign Intelligence Surveillance Act (governing foreign intelligence gathering); 68 AM. JUR. 2D *Searches and Seizures* § 104 (1993)

[17] *See Brinegar v. U.S.,* 338 U.S. 160, 175-76 (1949); Carroll v. U.S., 267 U.S. 132, 162 (1925).

[18] 389 U.S. 347 (1967).

[19] *U.S. Dist. Ct. for the E. Dist. of Michigan,* 407 U.S. 297.

[20] 277 U.S. 438 (1928).

[21] 389 U.S. 347.

[22] *Id.* at 351.

[23] 277 U.S. at 478 (Brandeis, J., dissenting).

[24] 389 U.S. at 361 (Harlan, J., concurring).

[25] *California v. Ciraolo,* 476 U.S. 207, 211 (1986).

[26] *See* Maricela Segura, *Is Carnivore Devouring Your Privacy?*, 75 SO. CAL. L.REV. 231, 254 (2001).

[27] 407 U.S. 297.

[28] *Id.* at 321-22.

[29] *See Bin Laden,* 126 F. Supp. 2d at 271-72.

[30] H.R. 2975, 107th Cong. (2001).

[31] *U.S. v. Duggan,* 743 F.2d 59, 73 (2d Cir. 1984); *U.S. v. Cavanagh,* 807 F.2d 787, 790 (9th Cir. 1987).

[32] *See Bin Laden,* 126 F. Supp. 2d at 277-78.

[33] 18 U.S.C. §§ 2510-2522 (2002).

[34] 50 U.S.C. §§ 1801-1863 (2002).

[35] *See* Jennifer C. Evans, *Hijacking Civil Liberties: The USA PATRIOT Act of 2001,* 33 LOY. U. CHI. L.J. 933, n.230 (2002) (quoting 147 Cong. Rec. S10992 (daily ed. Oct. 25, 2001)).

[36] *See* 18 U.S.C. § 2516 (listing the offenses for which surveillance may be conducted under Title III).

[37] *See* James X. Dempsey, *Communications Privacy In the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy, available* at http://www.cdt.org/publications/lawreview/1997albany.shtml (reprinted from 8 ALBANY L.J. SCI. & TECH. (1997)).

[38] *See* 18 U.S.C. § 2518; Evans, *supra* note 35, at 953.

[39] *See* Segura, *supra* note 26, at 243 (citing 18 U.S.C. § 2518).

[40] *See* 18 U.S.C. § 2518.

[41] *See* Segura, *supra* note 26, at 244 (citing 18 U.S.C. § 2518).

[42] *See id.* at 243 (citing 18 U.S.C. § 2518).

[43] *See id.* at 244 (citing 18 U.S.c. § 2518).

[44] *See* 18 U.S.C. §§ 1367, 2521, 2701-2711, 3121-3127 (2002).

[45] *See* Sharon H. Rackow, *How the USA PATRIOT Act Will Permit Governmental Infringement Upon the Privacy of Americans in the Name of 'Intelligence' Investigations,* 150 U. PA. L. REV. 1651, 1683 (2002) (citing 18 U.S.C. § 2518).

[46] *Id.* (quoting 18 U.S.C. § 2518).

[47] *See* Segura, *supra* note 26, at 244-49.

[48] *See id.* at 248.

[49] *See The Fourth Amendment and the Internet: Testimony Before the Subcomm. on the Constitution of the House Comm. on the Judiciary* (2000) (testimony of James X. Dempsey, Center for Democracy and Technology), *available* at http://www.cdt.org/testimony/000406dempsey.shtml (citing 18 U.S.C. § 3122-3123)

[50] *See* Segura, *supra* note 26, at 247 (citing *Smith v. Maryland,* 442 U.S. 735 (1979)).

[51] *See id.* at 247-48 (citing *U.S. v. New York Telephone,* 434 U.S. 159 (1977)).

[52] *See* Rackow, *supra* note 45, at 1661-66 (explaining the origins of FISA).

[53] *See* 50 U.S.C. § 1801 (defining "foreign power"); 50 U.S.C. § 1802 (conditions in which Attorney General certification is sufficient for use of electronic surveillance); Rackow, *supra* note 45, at 1667-68.

[54] *See* Rackow, *supra* note 45, at 1671-72 (citing 50 U.S.C. § 1802).

[55] *See id.* at 1669-70.

[56] *See* 50 U.S.C. § 1802.

[57] *See* Doyle, *supra* note 5, at 14.

[58] *See* 50 U.S.C. § 1803(a).

[59] *See* 50 U.S.C. § 1803(b).

[60] *See* Rackow, *supra* note 45, at 1668-69.

[61] *See* Evans, *supra* note 35, at 956; Rackow, *supra* note 45, at 1670-71, According to the Center for Democracy and Technology, the FISC has denied only one warrant request in twenty-two years. *See* Rackow, *supra* note 45, at 1671 (citation omitted).

[62] Rackow, *supra* note 45, at 1674-75 (quoting 50 U.S.C. § 1804(a)(7)(B); H.R. Res. 3162, 107th Cong. § 218 (2001) (enacted)).

[63] *See Terrorism Investigation and Prosecution: Hearing Before the Senate Comm. on the Judiciary,* 107th Cong. (2001) (statement of Attorney General John Ashcroft) ("[I]f we don't have the capacity of having a single purpose, of having purposes other than the foreign intelligence purpose, we find that we might have to discontinue in order to prosecute some of these coverages."); *see also Protecting Constitutional Freedoms: Hearing Before the Senate Comm. on the Judiciary, Subcomm. on the Constitution, Federalism, and Property Rights,* 107th Cong. (2001); *The Justice Department's Counterterrorism Proposal: Hearing Before the Senate Select Comm. on Intelligence,* 107th Cong. (2001); Neil A. Lewis, *F.B.I. Inaction Blurred Picture Before Sept. 11,* N.Y. TIMES, May 27, 2002 (describing the FBI's "play-it-safe" approach to FISA warrants following FISC scrutiny of FISA affidavits filed by FBI agents to the FISC).

[64] *See* David Johnston and Philip Shenon, *A Nation Challenged: F.B.I. Curbed Scrutiny of Man Now a Suspect in the Attacks,* N.Y TIMES, Oct. 6, 2001, at A1(citing an anonymous senior Justice Department official).

[65] *See* Evans, supra note 35, at 972, 975-76; *Protecting Constitutional Freedoms, supra* note 63; *The Justice Department's Counterterrorism Proposal, supra* note 63.

[66] 50 U.S.C. § 1801(h)(1).

[67] *See* Rackow, *supra* note 45, at 1683-84.

[68] *See* Doyle, *supra* note 5, at 17; Evans, v note 35, at 971-72.

[69] *See* Evans, *supra* note 35, at 977-78.

[70] *See* Pub. L. No. 107-56, §216(a)(3) (2001).

[71] *See* Electronic Commerce and Privacy Group, *Summary and Analysis of Key Sections of USA Patriot Act of 2001, at 6-7, available* at http://www.piperrudnick.com/publications/PublicationBody.asp?pubID=1118281152001.

[72] *See* Evans, *supra* note 35, at n.145 and accompanying text (citing 50 U.S.C. § 1823).

[73] 50 U.S.C. § 1821(5).

[74] *See* 50 U.S.C. § 1823.

[75] Center for Democracy and Technology, *supra* note 4.

[76] *See* Exec. Order No. 12,333 § 2.5 (1981), *available* at http://www.fas.org/irp/offdocs/eo12333.htm.

[77] *See Bin Laden,* 126 F. Supp. 2d at 279-80.

[78] Neil A. Lewis, *Traces of Terror: Civil Liberties,* N.Y. TIMES, June 13, 2002, at A33 (quoting Assistant Attorney General Viet D. Dinh).

[79] *See* Berman and Dempsey, *supra* note 2, at 1-2, 5-6; Electronic Privacy Information Center, *The Attorney General's Guidelines,* June 26, 2002, available at http://www.epic.org/privacy/fbi.

[80] *See The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations,* May 30, 2002, *available* at http://www.usdoj.gov/olp/generalcrimes2.pdf; *Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations,* May 25, 1995, *available* at http://www.usdoj.gov/ag/readingroom/terrorismintel2.pdf (portions redacted).

[81] *See* Berman and Dempsey, *supra* note 2, at 10.

[82] *Guidelines for FBI Foreign Intelligence Collection, supra* note 80, at 1. *See also Guidelines on General Crimes, supra* note 80, at Preamble (General Crimes Guidelines "do not limit activities carried out under other Attorney General guidelines [i.e., the Foreign Intelligence Guidelines] addressing such matters as investigations and information collection relating to international terrorism, foreign counterintelligence, or foreign intelligence.").

[83] *Guidelines on General Crimes, supra* note 80, at 21, 23.

[84] *See Bin Laden,* 126 F. Supp. 2d at 278.

[85] *See id.* at 6; *Guidelines on General Crime, supra* note 80, at 6, 21-23.

# Federal Legal Constraints on Profiling and Watch Lists

**By Eric Braverman**
**Senior Researcher, The Legal Project**

**And**

**Daniel R. Ortiz**
**John Allan Love Professor of Law and**
**Joseph C. Carter, Jr., Research Professor**
**University of Virginia**

## Introduction and Executive Summary

Controversy has long followed both profiling and watch lists—commonly used and important law enforcement mechanisms. Prior to September 11, most of this controversy focused on traffic stops and drug arrests, where many feared that police were employing suspect racial criteria in profiling decisions. September 11 intensified this controversy. On the one hand, the terrorist attacks made many feel that government should make more and freer use of these mechanisms and focus them more directly on groups associated with terrorism in the public mind. On the other, many came to fear more deeply that the government would invidiously focus these law enforcement techniques on a few traditionally disfavored groups. The stakes, in other words, grew higher on both sides of the controversy.

This report takes no position on the wisdom of profiling and watch lists either generally or in specific contexts. Rather, it describes the existing legal constraints on both practices. They are few but sometimes powerful. The Fourth Amendment has some bite in profiling. It prevents the government from conducting the most intrusive searches and seizures—of someone's house, for example—on the basis of a statistical profile alone. It does, however, allow the government to conduct less intrusive searches and stops on the basis of predictive and specific statistical profiles. The Fourth Amendment, on the other hand, has no application to the government's use of watch lists. Since they represent neither a search nor a seizure, the two independent triggers for Fourth Amendment analysis, watch lists escape this strand of constitutional analysis entirely.

The Equal Protection Clause, by contrast, has some purchase—and the same purchase—on both profiles and watch lists. Unlike the Fourth Amendment, which looks to see whether a particular government action is warranted by adequate suspicion, the Equal Protection Clause looks to see whether the government has impermissibly relied on certain suspect factors, like race, ethnicity and national origin, in deciding to take that action. Any government use of these factors—particularly in a formal, written profile or in a written policy statement governing the preparation of a watch list—will cause some constitutional difficulty. Whether such use is ultimately permissible will depend on (1) whether the policy was informal or written, (2) the particular context of the decision and (3) what other, non-suspect factors might have supported it. Finally, profiling and watch lists employed by private actors are *effectively* subject to many of these same constraints.

## Profiling

### Restraints on Government

#### The Fourth Amendment

The Fourth Amendment represents the primary constitutional constraint on governmental investigations and creates quite high stakes for law enforcement. If the police violate the Fourth Amendment in conducting a search or seizure, a court will often suppress any evidence discovered and any further evidence to which the "tainted" evidence led.[1] The text of the amendment itself gives only some guidance to police. It provides:

> the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

In giving the text content, the courts have read the two triggers—"searches" and "seizures"—broadly. Government interference with a person's reasonable expectation of privacy can represent a "search" for Fourth Amendment purposes, just as "meaningful interference with an individual's possessory interests"[2] in property or any interaction with a person where the person reasonably believes he is not "free to leave" can be a "seizure."[3] Much routine law enforcement work, in other words, comes under Fourth Amendment scrutiny.

The text poses one central interpretive difficulty—the relationship between its first clause, which seems to establish a reasonableness requirement, and the second, which seems to require a warrant supported by "probable cause." The two appear to point in different directions—the first granting the police much discretion, the second much less. The courts have tended to read the Warrants Clause back over the first. Thus, most significant types of searches and seizures require a warrant and many of those that do not still require probable cause. The courts have found many situations, however, where the reasonableness standard governs instead and have applied a balancing test to them. In these cases, the Court has judged the reasonableness of searches and seizures by weighing the government's interest in the specific manner of investigation against the people's interest in the general security of persons and property. So even though the background principle states that warrantless searches and seizures are unreasonable per se, the courts have allowed the government in many cases a lesser burden of proof.

The least of these burdens requires no individualized suspicion at all. This standard applies (1) to searches incident to a lawful arrest, (2) to certain routine searches and seizures that occur at particular places, such as regular searches at international borders or at fixed, discretionless sobriety checkpoints on the highways[4] and (3) to other specific searches and seizures—like inventory searches, regulatory searches (*e.g.,* fire, health, and safety searches) and routine x-ray scans of airline passengers at airports. In the latter two categories, the courts generally require only that the government agents who define the scope of the search or seizure be different from those who execute it. In the first category, the courts do not even require that. In none of these cases, do the agents have to obtain a warrant or produce any individualized evidence of suspicion. Thus, in these cases,

profiling is generally unproblematic.[5] Using a profile in this particular context would not cause difficulty, for the government may conduct its search without any individualized suspicion.

The strictest standard of proof is that mentioned in the Fourth Amendment itself: "probable cause." It requires well-grounded suspicion that a particular individual committed a crime or that a particular place contains evidence of one. It generally applies when a government search or seizure intrudes deeply into an individual's reasonable expectations of privacy. A search of a house or a full custodial arrest, for example, ordinarily requires probable cause. By itself, a profile, which identifies targets by matching them up against a list of general statistical factors, cannot meet this requirement. As further discussion shows, however, it can authorize less intrusive government intervention, which in turn can uncover evidence amounting to probable cause.

Profiling can make the greatest difference in the intermediate cases, where the courts generally require "reasonable suspicion" of criminal activity to authorize government action. While "reasonable suspicion" does require some individualized basis for suspicion, it demands less than "probable cause." This reasonable suspicion standard applies to much of the everyday work of law enforcement, including non-routine searches at international borders (such as strip searches), protective sweeps, and, most famously, so-called "*Terry* stops"—investigatory detentions in which the police stop an individual for a short time, ask him questions, and even conduct a limited frisk ("pat-down") of his body to search for weapons.

"Reasonable suspicion" requires at bottom that the government "point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant" the particular intrusion at issue.[6] In *Terry v. Ohio,* for example, a policeman suspected two men of casing a store for theft because he watched them approach a shop window, study it, and then confer with each other down the street *twelve independent times.* He stopped the men and, when they did not give their names, frisked the outer layers of their clothing and found concealed weapons. The Supreme Court found no Fourth Amendment violation. The suspects' repeated visits to the store window, withdrawals for discussion, and later evasiveness furnished the necessary reasonable suspicion. On balance, the Court held, such facts were sufficient under the Fourth Amendment to support both the limited search and brief seizure.

What kinds of factors can establish reasonable suspicion? The police may establish such suspicion from personal experience, common sense, and information possessed by the law enforcement community in general so long as it is relatively specific. At the one extreme, if a person reports being robbed on a particular street corner by a white man in yellow pants who then fled the scene in an orange Pinto, the police reasonably may stop any white man wearing such pants in that kind of car in the neighborhood. At the other, however, they cannot arrest someone for a crime merely because they have certain "inarticulate hunches" or non-individualized suspicions that that person committed it.[7] Profiles can operate anywhere in between. A profile, like a crime report, can be quite specific and predictive or, like a vague hunch, quite general and unpredictive. The legal approach is clear even if it is not susceptible of precise articulation. The more a particular profile leans towards predictive specifics, the more likely it will provide reasonable suspicion. While parking ten feet from a known drug lair will, by itself, not furnish reasonable suspicion for a stop—even when most of

that hideaway's customers are known to park nearby—parking near a known drug lair, spending a short amount of time inside, emerging with a paper bag, and then leaving the scene evasively will.

Similarly, the police may not stop an airline passenger because of his race, even if he is known to come from a drug-source city. Such evidence *by itself* will fail to satisfy reasonable suspicion. On the other hand, such evidence does not weaken other evidence that is independently sufficient to support reasonable suspicion. The Fourth Amendment, in other words, neither prohibits the government from relying on broad, generic profile elements, even suspect ones like race, nor credits such factors. They simply make no difference. Such broad generic elements, however, can sometimes lead to more supportive and specific ones. It is usually true, for example, that the police cannot stop a person simply because he appears to fall in a broad group. But if the police first notice a person on this ground, choose to watch him, and later see other evidence supporting individualized suspicion, then they can stop him. This principle has significant practical bite. Together with the two Fourth Amendment doctrines discussed next, it allows the government to justify some otherwise impermissible searches or seizures, even ones based on race or ethnicity.

### Intent Matters Not

In *Whren v. United States,*[8] the Supreme Court held that the Fourth Amendment does not look into a police officer's actual reasons for performing a search or seizure. In this case, a policeman in a drug-infested area turned to follow a car that had stopped at an intersection for an unusually long time. When the car sped away at an unreasonable speed, the policeman pulled the car over and found bags of cocaine in the defendant's hands. The defendant argued that since a reasonable police officer would not have followed him merely to enforce the traffic laws, his search violated the Fourth Amendment. The police officer's reason, he argued, was a mere pretext and indeed it seems clear that the officer did not stop the car primarily because it was speeding. A unanimous Supreme Court, however, held that subjective motivation makes no difference to Fourth Amendment analysis. Instead, a court is to look at all the objective evidence available and decide whether that evidence was sufficient to establish the necessary individualized suspicion for the stop—here a routine traffic stop. Making an officer's actual intent irrelevant effectively shields police who informally employ troubling profile elements, such as race, from Fourth Amendment sanction. As the Court stated explicitly in *Whren*, while "the Constitution prohibits selective enforcement of the law based on considerations such as race[,] . . . the constitutional basis for objecting to intentionally discriminatory laws is the Equal Protection Clause, not the Fourth Amendment."[9]

### Bootstrapping Suspicion

A recent Supreme Court case illustrates how a small amount of suspicion, can grant police broad powers under the Fourth Amendment. In *Atwater v. City of Lago Vista,*[10] the Court ruled that the Fourth Amendment does not prohibit police from making full custodial arrests for non-jailable misdemeanors. In this case, a police officer stopped a motorist for a seatbelt violation—a non-jailable offense—arrested her, and drove her off to jail to await appearance before a magistrate, who later released her on a $310 bond. Atwater argued that although the police had probable cause to stop her for driving without a seatbelt, they had no reason to arrest her for any jailable offense. The Court, however, found no Fourth Amendment violation. The probable cause for the non-jailable seatbelt violation furnished probable cause for the detention itself. This doctrine reaches far, for it

allows an officer who has sufficient suspicion that a person has committed a crime—no matter how small—to arrest him. As the dissent in the case pointed out, an officer may thus "justif[y] a full arrest by the same quantum of evidence that justifies a traffic stop—even though the offender cannot ultimately be imprisoned for her conduct."[11]

Taken together, *Whren* and *Atwater* give law enforcement officials great leeway in informal profiling *under the Fourth Amendment.* Under *Whren*, an officer may stop someone he suspects for any reason, including race or national origin, so long as he can later provide other sufficient grounds for individualized suspicion. Once an officer has stopped a suspect, he then notices that the suspect has committed any crime, even a non-jailable misdemeanor, he may under *Atwater* then proceed to take the suspect into full custodial arrest. At the extreme, then, the *Whren* and *Atwater* principles suggest that a law enforcement officer could focus on a suspect for an ordinarily impermissible reason, like race, wait until that person engages in suspicious activity, and then perform a stop and frisk. If the officer then discovers evidence of any criminal activity—no matter how small the crime—he could take the suspect into full custody.

In short, the Fourth Amendment imposes meaningful constraints on profiling in only some cases. It does not allow a statistical profile by itself to justify the most intrusive searches and seizures, like the search of a home or a full custodial arrest. In the intermediate category of less intrusive stops and searches, however, it requires only that the profile generate plausible, predictive individualized suspicion. And, of course, as *Atwater* shows, a profile that justifies less intrusive preliminary stops and searches can sometimes be "stretched" to justify the most intrusive ones.

## Equal Protection

Although the Fourth Amendment operates as the most prominent constitutional constraint on governmental investigations generally, another constitutional provision has particular bite in profiling. The Equal Protection Clause of the Fourteenth Amendment, which applies to states and localities, and its Fifth Amendment analogy, which applies to the federal government, severely restrict the use of certain factors in profiling. Thus, even if a profile establishes adequate suspicion to authorize a search or seizure under the Fourth Amendment, the Equal Protection Clause might forbid it nonetheless because the profiling factors themselves are impermissible.

There are two general differences between how equal protection and the Fourth Amendment apply in profiling. First, the Equal Protection Clause sweeps more broadly than does the Fourth Amendment. Unlike the Fourth Amendment, which by its terms applies only to "searches and seizures," the Equal Protection Clause applies to all government conduct. By commanding that the government "no[t] deny to any person within its jurisdiction the equal protection of the laws," the Clause reaches all exercises of government power. The Fourth Amendment, for example, does not apply to a profile used to identify people for informal government investigation short of searches and seizures, but the Equal Protection Clause does and could possibly invalidate it.

Second, unlike the Fourth Amendment, which asks whether government has enough information to take a particular action (is a particular governmental intrusion warranted under the circumstances?) equal protection asks whether the government can even consider certain information in

making a decision (was the decision based on impermissible factors?). In other words, whereas the Fourth Amendment regulates the outputs of government decisionmaking, equal protection regulates its inputs instead.

### Protected Classes and Levels of Scrutiny

By definition, all laws discriminate. Whenever it creates a category, the law treats those inside the category differently than those outside it. Speeding laws, for example, visit penalties on people who drive over a certain speed and none on those who do not. They necessarily create a favored and a disfavored class. Equal protection, then, cannot possibly foreclose any and all discrimination because it would leave no laws standing—good or bad. It must do something less and the Supreme Court has interpreted it only to require some justification from the government for any differences in treatment.

The Supreme Court has recognized, moreover, that we have no reason to be equally suspicious of all forms of discrimination. Some differences in treatment, like that of speeders, likely reflect valid purposes, whereas others, like laws burdening racial minorities, likely do not. The Court has thus developed a three-tiered framework which scrutinizes governmental action harder the more likely it reflects invidious purposes. Laws burdening groups, like speeders, whom we have little reason to believe the government would disfavor for bad reasons, get an easy pass; laws burdening some long-disfavored cultural groups, on the other hand, receive a harder look.

The courts apply so-called "reduced scrutiny" to most laws. This level of review requires the government to show that its action bears *a rational relationship to a legitimate state interest.*[12] Although the words "rational" and "legitimate" might suggest weak but still meaningful review, the courts have defanged this test almost completely. In addition to accepting asserted governmental purposes that actually played no role in the government's decision, the courts have themselves occasionally hypothesized purposes that might lie behind the government's action and have not required much in the way of real fit between a law's asserted purpose and the law itself. The courts have, in fact, approved dramatically underinclusive classifications on the ground that the government does not have to address a problem comprehensively but can take "one step at a time"—even if it never goes beyond the first step.[13] Gerald Gunther famously summed up this standard of review as "minimal. . . in theory and virtually none in fact."[14]

The courts apply so-called "intermediate scrutiny" to government actions that classify on the basis of sex or illegitimacy. Although sometimes inconsistently described, intermediate scrutiny generally requires that government action bear *a substantial relationship to an important governmental interest.*[15] It thus scrutinizes both the government's ends and its means more closely than does reduced scrutiny and has led the courts to strike down much governmental action. The courts have, however, also found that some laws resting on these same classifications, like statutory rape laws imposing different penalties on men and women and laws requiring men but not women to register for the draft, pass this level of review.

Finally, the courts apply so-called "strict scrutiny" to governmental actions based on a few traditionally suspect classifications, most notably race, national origin and ethnicity.[16] (Religion, although not an official suspect classification, receives similar treatment under the First

Amendment.[17]) As the name implies, strict scrutiny bites harder than the other two forms of review. It requires that the government action bear *a necessary relationship to a compelling state interest.*[18] In fact, it requires such a high showing that invalidation is almost automatic. Only one case burdening a traditionally disfavored group has survived strict scrutiny in the Supreme Court. And that case, *Korematsu v. United States,*[19] which upheld the detention of American citizens of Japanese descent living on the West Coast at the beginning of World War II, is now notorious. As Gerald Gunther pithily put it, this level of review is "'strict in theory' and fatal in fact."[20] In practice, nothing ever satisfies it.

### Implications for Profiling

How seriously does equal protection actually constrain profiling? First, it is clear that any written profile using a suspect classification—*e.g.*, race, ethnicity, or national origin—will face strict scrutiny. Thus, a government agency using a formal written profile that employs one of these factors will have to show that the profile bears a necessary relationship to a compelling state interest. The state interest, national security, will pose little problem. It is difficult to imagine a state purpose more compelling than that. The means, however, will likely pose difficulty. The government will have to argue *at least* that without the ordinarily impermissible factor the profile would have little, if any, predictive validity. The government cannot simply show that legitimate targets of investigation disproportionately exhibit the trait and others do not. The Supreme Court has found such arguments lacking under even intermediate scrutiny.[21] The government will also likely have to show that no other, non-suspect factors could take the suspect factor's place and that the overall profile actually performs a critical national security function.

Using an informal, unwritten profile that employs a suspect factor is subject to somewhat different analysis. In these cases, a government agent typically employs a list of factors in the back of her head to help exercise discretion in selecting people for individual investigation. Drug courier profiles are the primary example. The government can defend the agent's action in these cases by showing that a suspect factor, even if present, made no difference in the particular decision under review. Once someone shows that a government agent used race, for example, in selecting him for investigation, the government can argue that the other, permissible profiling factors by themselves would have led to the same decision to investigate.

Given the discretionary nature of law enforcement, courts cut government officials much evidentiary slack in this inquiry and have upheld many informal profiling decisions posing equal protection questions. *United States v. Weaver*[22] is a good example. In this case, race was the "[n]umber one" factor that led a law enforcement officer to stop a suspect.[23] Still the court found no equal protection violation. It found that the other factors the officer relied on, particularly the suspect's rapid walking, his inability to produce a copy of his plane ticket, his lack of identification, and his nervousness, would have led to the same decision. This same type of defense, however, is unavailable for formal, written profiles. Asserting it in this context would require the government to argue that the suspect profiling factors never make a difference to any decision taken under the profile. But if that were the case, the suspect factors should *never* have been included in the profile to begin with. Harmless error cannot stretch so far.

Using profiling factors related to but not identical with suspect factors is more complicated still. The Supreme Court has long held that government can employ a non-suspect classification that has a discriminatory effect on a protected group so long as the government does not intend that burden.[24] A discriminatory effect alone, in other words, does not offend equal protection; a discriminatory intent is needed. A law burdening the poor, for example, certainly has a discriminatory effect on African-Americans since, as a group, they are poorer than whites. Such a law would not violate equal protection, however, unless the government enacted it precisely in order to burden African-Americans. In upholding a Massachusetts veterans' preference that effectively excluded nearly all women from many state jobs, the Court described how strictly this intent requirement operates:

> "Discriminatory purpose"... implies more than intent as volition or intent as awareness of consequences. It implies that the decisionmaker, in this case a state legislature, selected or reaffirmed a particular course of action at least in part "because of," not merely "in spite of," its adverse effects upon an identifiable group.[25]

And, in a footnote, the Court made clear that a "legitimate" state policy would negate any intent: "[w]hen, as here, the [law's disproportionate] impact is essentially an unavoidable consequence of a legislative policy that has in itself always been deemed to be legitimate... the inference [of discriminatory intent] simply fails to ripen into proof."[26] This approach to intent allows the government to employ a non-suspect classification that in practice targets many members of a suspect class so long as the government can assert a legitimate reason for using the non-suspect classification itself. The government cannot, however, hope to circumvent the law by simply employing a non-suspect classification as a proxy for a suspect one. The intent requirement will catch it and the vise of equal protection will press hard.

The intent requirement thus gives the government wide, but not complete latitude in deciding what factors to use in profiling. Although the government cannot easily employ racial, ethnic and religious factors, it can employ other related factors that it has reason to believe will improve predictive validity. So, for example, although the government cannot use descent from any particular ethnic or racial group as a written profiling factor without proving that such a factor was "necessary" to protect national security, a very high burden, it could use such factors as associating with a country known to harbor terrorists, visiting particular countries where terrorist groups are known to be and using banks or other institutions associated with terrorist groups without any difficulty. As a practical matter, equal protection will likely pose no great obstacles to effective law enforcement.

## Profiling by Private Actors

Although the Fourth Amendment and equal protection regulate only acts of government, the courts and Congress have effectively extended many of their requirements to private actors. First, the courts have held that when private actors carry out public functions under government command, authorization, or direction, they are subject to the same restraints as government.[27] Thus, if the government orders an airline to inspect luggage and profile passengers, the airline becomes a public actor for purposes of the Fourth Amendment and equal protection. Its private status offers it no shield. The precise contours of this rule, however, are extremely murky. All that can be safely said is that the more closely the action resembles a traditional governmental function and the more

direction the government exerts over private actor's exercise of it, the more likely it is that courts will consider the private actor an agent of the government.

Second, Congress has passed many laws regulating discrimination in private behavior. Although it would be impossible to list, let alone discuss, them all, many of them reach profiling by private actors in certain contexts. Many of these laws are narrow. 49 U.S.C. § 40127(a), for example, provides that an "air carrier or foreign air carrier may not subject a person in air transportation to discrimination on the basis of race, color, national origin, religion, sex, or ancestory." Some, like Title VII of the Civil Rights Act of 1964,[28] prohibit discrimination in a single substantive area—in its case, employment. And some stretch very broadly. The two broadest are 42 U.S.C. § 1981 and Title VI of the Civil Rights Act of 1964.[29]

Section 1981 provides sweeping protections against private discrimination in all forms and stages of contract, including performance. It states, in relevant part:

> All persons within the jurisdiction of the United States shall have the same right in every State and Territory to make and enforce contracts. . . as is enjoyed by white citizens. . . For purposes of this section, the term "make and enforce contracts" includes the making, performance, modification, and termination of contracts, and the enjoyment of all benefits, privileges, terms, and conditions of the contractual relationship . . . The rights protected by this section are protected against impairment by nongovernmental discrimination and impairment under color of State law.[30]

The courts have interpreted it, just like the Equal Protection Clause, to reach only intentional discrimination. It thus imposes roughly the same restraints on profiling within private contractual relationships, like travel, that equal protection imposes on governmental actors generally.

Likewise, Title VI of the Civil Rights Act of 1964[31] and its implementing regulations prohibit recipients of federal funds from discriminating on the basis, among others, of race, color or national origin. Thus, any private entity receiving money from the federal government, which covers much of the private economy, falls under this prohibition, which the courts have interpreted to reach somewhat beyond intentional discrimination. Together with § 1981, Title VI forms the basis for most law suits against airlines for inappropriate passenger profiling after September 11.[32]

## Watch Lists

Posting watch lists, the practice of publicly or semi-publicly identifying certain people as dangerous or suspected of criminal activity, poses somewhat different issues than does profiling. The Fourth Amendment, for example, has no purchase here. Posting this type of information—whether on a billboard, a "most wanted" list, or over the internet—does not constitute either a search or seizure, the triggers for Fourth Amendment analysis. On the other hand, equal protection plays out the same here as before. Since equal protection applies to all governmental action, not just searches and seizures, it restricts the grounds on which the government can pick whom to include in a watch list. Just as the government cannot use race as a formal written profiling factor, it cannot use it as a formal written factor in determining whom to include on a watch list. And just as the

government can sometimes use race in informal unwritten profiling—so long as it can explain the ultimate decision in a particular case on non-suspect grounds—so too it can use it in informal unwritten watch list decisions. The equal protection analysis plays out identically in both cases.

No other constitutional provision exerts much force in this area. At one time individuals whom police departments wrongly included on public watch lists claimed that the action violated their constitutional due process rights. They asserted that by wrongly damaging their reputation in the community the department's action represented a deprivation of liberty or property without due process of law. The Supreme Court, however, quickly held that reputation does not represent a liberty or property interest for due process purposes and thereby closed down this line of challenges.[33] Although the Court has left open as a theoretical matter whether wrongful inclusion on a watch list might violate a constitutional privacy interest, the test it would apply in such cases would clearly validate any reasonable governmental program designed to address terrorism.[34] Since the privacy test balances the injury to individual privacy against the government's interest, legitimate national security needs would tip the balance in any reasonable program's favor.

Likewise, the Federal Tort Claims Act forecloses liability under tort law when the federal government includes someone on a watch list. 28 U.S.C. § 2680(h) broadly exempts the federal government from liability for informational torts—slander, libel, and misrepresentation, in particular—and any plaintiff who attempted to recharacterize a tort to evade this exclusion would very quickly run into § 2680(a), which even more broadly exempts the government from liability for any "discretionary function." In short, watch lists escape any regulation from this sometimes powerful restraint on federal administrative action.

Two administrative mechanisms do exist through which a person on a watch list can seek to challenge and correct the information underlying his inclusion. Both the Privacy Act[35] and a newly enacted provision known unofficially as the "Data Quality Act"[36] give persons the right to seek and obtain correction of certain information agencies hold about them. Neither provision, however, allows a person to seek an injunction against use of the information or damages from the government for any injuries stemming from its use. These provisions, then, the first little-used and the second not-yet-tested, do not restrict the government's use of watch lists.

In short, little law constrains watch lists. Congress has specifically ousted the potentially available tort law remedies and has legislated no statutory controls. The only relevant statutes allow for review and correction of the underlying data but no remedy for the posting itself. Finally, the only constitutional provision with any bite in the area is the Equal Protection Clause and it restricts only the types of factors the government can use in putting a watch list together.

## Endnotes

[1] This evidence is commonly referred to as the "fruit of the poisonous tree." *See* Florida v. White, 526 U.S. 559 (1999).

[2] United States v. Jacobsen, 466 U.S. 109, 113 (1984).

[3] United States v. Mendenhall, 446 U.S. 544, 554 (1980).

[4] *See* Michigan Dept. of State Police v. Sitz, 496 U.S. 444, 454 (1990).

[5] Checkpoints are different. They are permissible only when the police have no discretion, as when they stop every car, every fourth car, or cars randomly.

[6] Terry v. Ohio, 392 U.S. 1, 21 (1968).

[7] *Id.* at 22.

[8] Whren v. United States, 517 U.S. 806, 813, 817-818 (1996).

[9] *Id.* at 813.

[10] Atwater v. City of Lago Vista, 532 U.S. 318, 324, 354 (2001)

[11] *Id.* at 361 (O'Connor, J. dissenting).

[12] Ambach v. Norwock, 441 U.S. 68, 80 (1979).

[13] Cleland v. National College of Businesses, 435 U.S. 213, 220 (1978).

[14] Gerald Gunther, *The Supreme Court 1971 Term-Foreword: In Search of Evolving Doctrine on a Changing Court: A Model for a Newer Equal Protection,* 86 Harv. L. Rev. 1, 8 (1972).

[15] Personnel Administrator v. Feeney, 442 U.S. 256, 273 (1979).

[16] Although the Supreme Court has nominally treated alienage as a suspect classification, its treatment varies greatly depending upon context. The Court seems to scrutinize seriously state and local action but not actions authorized by Congress. Federalism concerns, as much as equal protection, seem to explain these cases. In any event, equal protection extends only to legally resident aliens and does not even robustly extend to them in public employment.

[17] *See* Hobbie v. Unemployment Appeals Com., 480 U.S. 136, 141 (1987).

[18] *See* Eu v. San Francisco County Democratic Cent. Comm., 489 U.S. 214, 222 (1984).

[19] Korematsu v. United States, 323 U.S. 214 (1944).

[20] Gunther, *supra* note 14, at 8.

[21] Craig v. Boren, 429 U.S. 190, 201-203 (1976).

[22] United States v. Weaver, 966 F.2d 391 (8th Cir. 1992).

[23] *Id.* at 394 n.2.

[24] Village of Arlington Heights v. Metropolitan Hous. Dev. Corp., 429 U.S. 252 (1977); Washington v. Davis, 426 U.S. 229 (1976).

[25] Personnel Adm'r v. Feeney, 442 U.S. at 279.

[26] *Id.* at 279 n.25.

[27] *See* Edmonson v. Leesville Concrete Co., 500 U.S. 614 (1991).

[28] 42 U.S.C. §§ 2000e-2000e-7.

[29] 42 U.S.C. §§ 2000d-2000d-17.

[30] 42 U.S.C. § 1981.

[31] 42 U.S.C. § 2000d.

[32] *See* Chowdhury v. Northwest Airlines Corp. available at http://www.aclu.org/court/chowdhury.pdf.

[33] Bishop v. Wood, 426 U.S. 341 (1976); Paul v. Davis, 424 U.S. 693 (1976).

[34] Whalen v. Roe, 429 U.S. 589 (1977).

[35] 5 U.S.C. § 552a(d).

[36] Consolidated Appropriations Act, 2000, Pub. L. No. 106-554, § 515, 2000 U.S.C.C.A.N. (114 Stat. 2763) 29, 30.

# The Regulation of Disclosure of Information Held by Private Parties

**By Stewart A. Baker**
**Partner, Steptoe & Johnson, LLP**

## Introduction

The attacks of September 11 have raised again the question of what information our government should be able to gather about individuals as it fights terrorism. This paper examines current legal rules on government access to information held by third parties like telephone companies, Internet service providers ("ISPs"), and credit card companies.

The way lawyers and judges think about privacy has been conclusively shaped by the Fourth Amendment to the U.S. Constitution. That amendment guarantees the privacy of citizens by confirming their right to be "secure in their persons, houses, papers, and effects against unreasonable searches." This right is protected by requiring that searches be approved in advance by independent judges who issue search warrants on the basis of sworn statements stating the "probable cause" for the search.

As new technologies emerged—and offered new sources of information about citizens—privacy advocates sought to squeeze law enforcement access to the new information into this standard "search" model. After decades of uncertainty, for example, in 1967, wiretapping a phone call was declared to be a search requiring prior judicial approval and probable cause.[1] Congress then ratified and elaborated on the process for obtaining a wiretap order in Title III of the *Omnibus Crime Control and Safe Streets Act* of 1968.[2]

The effort to shoehorn new technologies into the "search" framework had its limits, however. One problem for privacy advocates was that the Fourth Amendment's privacy protection is personal—limited to the person who controls the "houses, papers, and effects." If police call on a suspect and want to search his house, they need a warrant. But if they call on his mother and want to search a suitcase he left with her, they can do so with her consent, not her son's. Similarly, if they call on his employer and want to search his work desk, they only need the employer's permission. What is more, even if the employer refuses to cooperate, a simple subpoena, not a search warrant, is usually sufficient to give the government access to things or information in the hands of a third party.

Privacy advocates have been reluctant to allow the government unregulated access to such data, and they have persuaded Congress to impose a series of slightly haphazard limits on government access to third-party records. As laid out in this paper, Congress has imposed special limits on government's access to electronic communications data, to financial records, to cable and video records, and to educational records. Most of these enactments are derived from the "search" model and offer some kind of watered-down Fourth Amendment protection. That is, the government is allowed access to information in a third party's hands if the government can obtain some kind of legal process (*e.g.*, a subpoena or court order) based on some kind of predicate set of facts (*e.g.*, the data is "relevant to an ongoing investigation.")

How much privacy protection is provided by these laws is open to question. A subpoena is easy to obtain; the FBI, for example, has statutory authority to issue its own. Relevance to an ongoing investigation is also easy to establish. If the government has even a casual interest in a citizen's affairs, it can fairly easily establish the predicates and obtain the orders necessary to gather large amounts of data about the citizen.

A few efforts have also been made to establish a broad set of principles that will prevent the government from maintaining large databases about individuals. These efforts include the *Privacy Act of 1974*,[3] which requires special justification for the creation of such databases, as well as the *Guidelines* first adopted by Attorney General Edward Levi in 1976, which restricted the ability of the Federal Bureau of Investigation to survey public records and commercial databases.[4] These initiatives were a response to scandals about government agencies collecting clippings about the activities of domestic dissidents. But in the Google age, when any person can create a private clippings file about anyone else, the scandal seems a bit musty—as relevant to our lives as the question whether a king of England can marry an American divorcee. In point of fact, Moore's Law has democratized the database business, and as data has become cheaper, many private actors have compiled extensive databases on individuals.

The effort to prevent construction of one large government database has succeeded to a degree. But King Canute could have succeeded to the same degree by building a sand castle with elaborate moats. The tide of data continues to flood in; it is simply spread across many smaller databases, often in private hands. Nevertheless, this information is still available to government investigators when they can identify the person whose information they want.

But the imposition of a Fourth-Amendment "search" model on government access to this data does have costs for investigators. In fact, legal restraints seem to pose a significant problem for the use of more sophisticated technologies—particularly when technologies that might help us identify terrorists early, as opposed to convicting them after they've killed people. Data mining and pattern recognition tools, as used by private industry, do not require that the companies identify in advance all of the customers who might be interested in a product—or those engaged in credit card fraud. Instead, the data is analyzed to identify patterns that may lead to the identities of potential customers as well as potential fraudsters. These programs can sift a vast amount of data, looking for previously unidentified individuals who share a profile with the company's targets.

Using data mining techniques to isolate suspicious behavior in masses of privately-held data—data about mostly innocent people—does not fit the typical "search" model. Instead, the government usually will have to process the data for suspicious patterns before it will even know whether further investigation is warranted.

Allowing such processing may well be important to the antiterror campaign. It also raises privacy issues that cannot be ignored. What this review suggests, however, is that a rote invocation of the privacy solutions adopted over the past quarter-century is unlikely to provide a particularly useful answer—either for the government or for privacy advocates.

The conflict between the traditional Fourth-Amendment "search" model and the new tools provided by information technology is one of the themes of this paper. The paper also looks at other legal issues likely to slow government's ability to use such tools when data is in the hands of private parties. Two are particularly noteworthy. First, the owners of the databases in question are not in the business of carrying out antiterrorism investigations. Some cooperation can be obtained by invoking the obligations of citizenship, but as the demands of data processing for antiterrorism grow, these companies will expect government to fund the necessary investment in personnel and technology. Second, private companies do not have sovereign immunity; they can be sued for providing information improperly to government investigators. The fear of liability must be addressed in any initiative on this issue. This fear is particularly powerful where the data is multinational in scope (as practically all the data worth examining soon will be). Data protection laws in other countries can threaten even cooperation by U.S. companies with the U.S. government.

## Gathering Information from Third Parties

Generally speaking, there are three types of "legal process" that the government can use to gather information held by third parties. The easiest form of process for the government to obtain is a subpoena. Many agencies—like the Federal Bureau of Investigation and the Internal Revenue Service—have been given the authority to issue administrative subpoenas in order to conduct their official responsibilities. Grand juries also have the authority to issue subpoenas to gather information relevant to an investigation.

In some cases, the government may also obtain a search warrant. The Fourth Amendment provides that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." As a result of these Constitutional requirements, search warrants are more difficult for the government to obtain than a mere subpoena. A judge must review the information already collected by the government and conclude that there is "probable cause" to justify the search. The warrant must also specify the items that are to be seized.

Finally, the government may obtain various court orders, as authorized by Congress in particular statutes. The procedures by which the government can obtain these orders vary greatly. Some court orders—like a Title III wiretap order—require a higher standard of proof and are harder to obtain than a search warrant. Other orders require the government to show "specific and articulable facts" that reasonably suggest that information is relevant to an investigation[5] —a lower standard than the "probable cause" that the government must demonstrate to receive a search warrant. All of these court orders, however, require a higher standard of proof and are more difficult to obtain than subpoenas.

### Grand Jury Subpoenas

As a general rule, the government can obtain most types of information held by third parties (*e.g.*, a suspect's bank or travel agent) with a grand jury subpoena. The Supreme Court has held that when someone "reveals his affairs to another"—for example, by opening a bank account or booking an airline ticket—the individual "takes the risk … that the information will be conveyed by that

person to the Government."[6] The Court has generally concluded that individuals do not have a Fourth Amendment "expectation of privacy" in most information they share with third parties. As a result, the government does not have to obtain a search warrant when accessing such information; instead, in most cases, a subpoena should be sufficient.

As noted above, compared to search warrants and other court orders, a grand jury subpoena is fairly easy for the government to obtain. Whereas a search warrant requires a judge to evaluate the evidence already gathered by the government and conclude that the government has "probable cause" to believe that a suspect is engaged in a crime, in order to obtain a subpoena, the government merely needs to show that the information being sought is relevant to an investigation. Grand jury subpoenas typically will contain "gag orders," forbidding the third party from discussing the subpoena or the information obtained by the government. Because grand juries are fairly unrestricted in the scope of their investigations, grand jury subpoenas have proven very effective vehicles by which the government can collect information for criminal and even counter-terrorism investigations.

However, even long-lived investigations and grand juries eventually come to an end. Also, in order to obtain a subpoena, the government must demonstrate a relevance to a particular investigation. As a result, subpoenas do not provide a particularly strong basis for programs where the government may want to filter large sets of data prospectively in order to detect possible terrorist actions. It is difficult to see how a subpoena could support the weight of such a program.

## Special Rules for Particular Information

Although, as a general rule, a grand jury subpoena is sufficient for the government to obtain most information held by third parties, Congress has adopted special rules restricting the government's ability to obtain certain types of information. Perhaps the most fully-developed area of law concerns the government's surveillance of communications. Similar restrictions have been adopted for financial records, video rental records, cable subscriber records, and educational records.

### Communications

The government's ability to collect information about a suspect's communications—*e.g.*, phone calls, e-mails, faxes—are governed by two sets of federal laws.[7] The use of government surveillance in criminal investigations is regulated by Title III of the *Omnibus Crime Control and Safe Streets Act of 1968 and the Electronic Communications Privacy Act of 1986* ("ECPA").[8] National security investigations are governed by the *Foreign Intelligence Surveillance Act of 1978* ("FISA").[9] Both sets of laws have been frequently amended. The most recent, substantive changes were adopted last October as part of the *USA PATRIOT Act.*[10]

Over time, the laws governing criminal and national security investigations have been amended by Congress to become increasingly similar. Nevertheless, there are some differences. For example, unlike criminal wiretap orders—which can be issued by any federal court and even state courts—FISA surveillance orders are only issued by a special federal court: the Foreign Intelligence Surveillance Court. This court consists of eleven, secretly designated federal district court judges from around the country. Only federal agencies can obtain FISA orders; state and local law enforcement agencies cannot.

## Obtaining Communication-Associated Information

There are various categories of communication-associated information that the government can obtain from a telecommunications carrier or Internet service provider. The least invasive category of information is basic subscriber information, which is statutorily defined as including: a customer's name, billing address, phone number (or subscriber number), type and length of service, local and long distance telephone connection records (or records of session times and durations) and means of payment (such as a credit card number or bank account number). Such information can be obtained under a subpoena.[11] The Federal Bureau of Investigation is also given special authority to request such information without a subpoena if the Director of the Bureau (or his designee) provides written certification that the information is relevant to a counter-terrorism or counter-intelligence investigation.[12] Ironically, although an Internet service provider faces potential liability if it discloses such customer data to the government without a subpoena, FBI certification or other proper authorization, it is free to distribute such information to private entities without restriction.[13]

The government may also obtain a "pen register order," authorizing it to collect—in real time—signaling information about all communications initiated by a particular subscriber.[14] For example, with a pen register in place, whenever a suspect places a call, the telecommunications company will notify the government of the phone number that the suspect is calling. Similarly, if the order is served on a suspect's Internet service provider, the provider will notify the government of the e-mail addresses to which the suspect is sending messages. A "trap and trace order" authorizes the government to collect such information for in-coming communications (*e.g.*, the phone number of the party that is calling the suspect). Neither a pen register nor a trap and trace order, however, allows the government to monitor the actual content of the communication; the government is not authorized to listen to the phone call or read the e-mail. In order to obtain a pen register or trap and trace order, the requesting government agent must certify that the information is relevant to an investigation.

In order to obtain more detailed information about an individual's communications—such as location information associated with a particular cell phone—the government must either obtain a search warrant or a special court order, known as a "section 2703(d) order."[15] A 2703(d) order allows the government to collect all sorts of transactional information about a suspect's communications, but—like pen register and trap and trace orders—it does not allow the government to access the contents of those communications. For example, the government can learn the specific location where a suspect last used his cell phone but cannot monitor the actual phone call that was placed. Before a court can issue a 2703(d) order, the government must present "specific and articulable facts" that reasonably suggest that the requested information is relevant to an investigation.[16]

## Accessing the Contents of Communications

In addition to collecting information about a suspect's communications, the government may also monitor the content of such communications. First, the government may access stored communications held by a third party.[17] For example, the government may obtain copies of the e-mails stored in a suspect's AOL or Yahoo e-mail account. If the communications have been stored with

the third party for 180 days or less, the government must obtain a search warrant to access the communications. If the communications have been stored for more than 180 days, the government can either obtain a search warrant, a section 2703(d) order or a subpoena. However, if the government uses a subpoena or section 2703(d) order, they must also notify the suspect of the communications being collected. (This notice can be delayed by a court). No notice is required if the government uses a search warrant to access the stored communications.

Second, the government may also wiretap a communication—*e.g.*, intercept the contents of a phone call or e-mail in real time. In order to conduct such live surveillance, the government must obtain either a Title III or FISA court order.[18] Because wiretapping is the most invasive form of surveillance the government can conduct, these orders are extremely difficult to obtain—even more difficult than a search warrant. Before the government can even apply to a court to obtain such an order, there is a lengthy and detailed internal review process, which concludes only when the Attorney General or his designee approves the request for an order. The government must then provide "probable cause" to justify the order.

### Financial Records

Congress has adopted a similar, although less restrictive, legal regime to regulate the government's ability to access financial records. Broadly speaking, it is easier for the government to obtain financial records than to intercept communications.

In 1976, the Supreme Court ruled in *United States v. Miller* that individuals have no Fourth Amendment "expectation of privacy" in records maintained by their banks. The Supreme Court noted that "a depositor takes the risk, in revealing his affairs to another, that the information will be conveyed to the government" and that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party. . . even if the information is revealed on the assumption that it will be used for a limited purpose and the confidence placed in the third party will not be betrayed."[19]

In response to *Miller*, Congress adopted the *Right to Financial Privacy Act* of 1978 ("RFPA")[20] to provide a detailed set of rules about how the government can access records held by financial institutions. Essentially, RFPA requires that the government either obtain an administrative or grand jury subpoena, search warrant, or the customer's permission before the government can collect a customer's records from a financial institution.[21]

One of the specific requirements added by Congress is prompt notification of the customer. If the government obtains the information pursuant to a subpoena, a copy of the subpoena must be delivered to the customer, along with a notice informing the customer how to object to the government's request, within ten days. If the government obtains a search warrant, such notice does not have to be provided for 90 days. More importantly, if the court is convinced that notice would result in endangering the life or physical safety of any person, flight from prosecution, or destruction or tampering with evidence, the court may delay this notice by 180 days (and may extend the delay for periods of up to 90 days each).[22] However, these restrictions do not apply to the Secret Service in its protective functions and to foreign intelligence activities and investigations related to international terrorism.[23]

Under RFPA, if banks suspect that a customer is engaged in criminal activity, they are permitted to voluntarily disclose limited information—the name of the account holder and the suspected violation—to the government.[24] However, the institution may not disclose any additional information without appropriate legal process from the government.

In 1982, Congress adopted the first anti-money laundering legislation, imposing an affirmative obligation on banks to report certain activity to the government.[25] This legislation has given the Treasury Department broad authority to impose recordkeeping and reporting regulations on banks. For example, banks are required to report to Treasury whenever they issue a check or money order in the amount of $3,000 or more.[26] More recently, Congress has also required financial institutions to adopt internal programs to search for, and report, possible money laundering.[27] These "due diligence" provisions were extensively amended by the *USA PATRIOT Act* in 2001, which expanded the categories of financial institutions that were covered by these reporting obligations.[28] Essentially, the money laundering legislation has led to the creation of a private data-mining capability, with private companies obligated to search for potential suspicious activity.

### Cable Viewing Records

As part of the Cable Act of 1984, Congress adopted a provision prohibiting cable companies from disclosing information about their customers to the government, expect pursuant to a court order.[29] The order could only be obtained upon "clear and convincing evidence" that the customer was suspected of engaging in a crime and if the order afforded the customer an opportunity to contest the government's claim.[30]

For many years, there was some confusion about whether the Cable Act's privacy provision should apply when the government was requesting information about a customer who was receiving Internet or telephone service from a cable provider. As mentioned above, federal surveillance law contains very different legal requirements for accessing such communication-related information. For example, the government is entitled to receive basic subscriber information under a subpoena, without having to provide any notice to the customer.

The *USA PATRIOT Act* resolved this statutory conflict by amending the Cable Act. The Act's privacy provision was narrowed to apply only to information about a customer's cable TV service (*e.g.*, records about what pay-per-view movies a subscriber orders). The *USA PATRIOT Act* amendments confirmed that when a cable company provides telephone or Internet service, the federal surveillance laws apply.

### Video Rental Records

In 1988, in reaction to the confirmation hearings for Judge Robert Bork (where opponents to Judge Bork's nomination revealed that he had rented pornographic videos), Congress passed the *Video Privacy Protection Act*.[31] The law expressly forbids video rental companies from disclosing any information about their customers except with the customer's consent or pursuant to a search warrant, court order, or grand jury subpoena.

### Educational Records

Congress has also specifically addressed government access to educational records. In 1974, Congress passed the *Federal Education Records and Privacy Act* of 1974 ("FERPA")[32], also known as the Buckley Amendment. This law generally required that any school or institution that receives federal funds for education may not release school records or any other personally identifiable information without the prior consent of the student's parents. In 1994, Congress amended the law to clarify that the government could obtain such records pursuant to a federal grand jury subpoena or administrative subpoena for "law enforcement purposes."[33]

In 2001, as part of the *USA PATRIOT Act*, Congress further revised the law to clarify that the Justice Department can seek a court order to collect any education records relevant to a terrorism investigation[34]. Such an order can only be sought with the approval of a senior Justice Department official (no lower than Assistant Attorney General) and can only be issued if a court finds that there are "specific and articulable facts" to believe that the records are relevant to a terrorism investigation. Like the surveillance laws mentioned above, the amendment also contains an immunity provision—protecting educational institutions from liability for complying with such an order. However, the amendment does not contain a reimbursement provision.

## Legal Problems Regarding Government Use of Pattern Recognition on Data in Private Hands

In counter-terrorism investigations, it is often helpful to run pattern recognition analysis on information like credit card charges or train tickets. For example, running similar analysis on the airline tickets purchased by the September 11th terrorists—and the forms of payment they used—would have shown a network of relationships between the terrorists, with several terrorists buying their tickets together or paying for the tickets of other conspirators.

However, data mining on masses of data about mostly innocent transactions does not fit the "search" model discussed in the previous section. Indeed, it is only after the government has already processed such data (seeing, for example, that a suspected terrorist is traveling with and paid for the tickets of several other individuals) that it typically has the "probable cause" or "criminal investigative relevance" necessary to obtain a search warrant or subpoena.

In addition, several federal laws adopted in the 1970s in response to scandals involving the governments monitoring of the anti-Vietnam War and civil rights movement have restricted the government's ability to mine such data prospectively.

### FBI Guidelines

For example, the *Guidelines* first adopted by Attorney General Edward Levi in 1976 restricted the ability of the Federal Bureau of Investigation to survey public records and commercial databases. The Guidelines prohibited FBI agents from using publicly-available sources of information—*e.g.*, libraries or the Internet—except as part of an "investigation." An investigation could only be

opened based upon allegations or information of criminal behavior. Thus, the FBI could not survey publicly-available information (like newspapers), let alone commercial databases, simply to generate leads.

Attorney General Levi's guidelines were based on the view that investigating those who sympathize with violent groups is a violation of the sympathizer's First Amendment rights. Gathering even public data, like newspaper articles, on such groups, without specific allegations of criminal behavior, was considered too intimidating. Since 1976, the *Guidelines* have been amended three times: by Attorney General French Smith in 1983[35], Attorney General Richard Thornburgh in 1989[36], and, most recently, by Attorney General John Ashcroft in May of this year.[37] Although each of these amendments slightly loosened the restrictions imposed on the FBI, it was not until Attorney General Ashcroft issued his new *Guidelines* that the FBI received the authority to monitor the web, periodicals, and commercial databases (like Google or Experian) prospectively—not in the context of a specific criminal investigation.

### Privacy Act

The *Privacy Act* of 1974 also sought to regulate how the government can collect and maintain records about U.S. persons. Like the *Guidelines* adopted by the Justice Department, the Act contains special limits on the government's ability to gather information about "how any individual exercises rights guaranteed by the First Amendment."[38] The Act also restricts the reasons for which the government may collect information—such as "an authorized law enforcement activity"—and imposes requirements allowing parties to access the records held about them and contest the accuracy of those records.

The Act imposes similar restrictions on any "matching" programs conducted by the government or by the private sector on behalf of the government, unless the matching is conducted "subsequent to the initiation of a specific criminal or civil law enforcement investigation" or "for foreign counterintelligence purposes."[39]

These requirements are just restrictive enough to make it awkward for the government to take direct access of private databases for data-mining analysis. As a result, one of the emerging solutions being adopted by the government is to encourage or even require industry to keep the databases in private hands, run pattern recognition themselves, and report suspicious results to the government. As noted above, this approach has been used in the anti-money-laundering context. The Administration has discussed adopting similar approaches with respect to other records that might be of interest in counter-terrorism investigations.

## Legal Concerns of Private Parties When Government Seeks Access to Customer Data

In addition to the restrictions that the government faces in accessing information held by private parties, the parties themselves also have legal concerns about sharing the information with the government. The two principal concerns that private entities have when complying with government requests are: liability and reimbursement.

## Liability

### U.S. Law

Surprisingly, private entities face potential legal liability whenever they comply with a government request for data. Many of the federal statutes that restrict access to particular categories of information impose civil (and, frequently, criminal) liability on companies that fail to comply properly with the laws' requirements. For example, an Internet service provider that shares customer data with the government without proper legal authorization can be sued.[40] *The Right to Financial Privacy Act, the Federal Education Records and Privacy Act*, the *Cable Act* and the *Video Privacy Protection Act* all contain similar civil liability.[41] In addition to such specific, statutorily-based liability, private parties also face potential general liability for participation in any government action that is subsequently determined to violate an individual's constitutional rights.

Some federal statutes contain immunity provisions that protect private parties for any actions they take in complying with a court order or other legal process. For example, the *Federal Education Records and Privacy Act* provides that "an educational agency or institution that, in good faith, produces education records in accordance with an order issued under [FERPA] shall not be liable to any other person for that production."[42] Although common—similar protections exist for disclosure of communications and financial records—such immunity is not universal.

Furthermore, these protections are usually tied to compliance with the terms of a court order or subpoena. Both the *Electronic Communications Privacy Act* and the *Right to Financial Privacy* contain narrow exceptions where private entities are protected for voluntarily disclosing information to the government without such legal compulsion. However, these exceptions are extremely limited. Under RFPA, a bank may only disclose the name of the account holder and the suspected violation[43]; under ECPA, an Internet service provider or telephone company may only reveal customer records "if the provider reasonably believes that an emergency involving immediate danger of death or physical injury … justifies disclosure to the government."[44] As a result, private entities are reluctant to share information outside of compulsory contexts, where the government provides a subpoena or other legal process.

### Foreign Privacy Laws

These concerns are not limited to potential liability under U.S. laws. Indeed, in many ways, foreign laws present a greater obstacle to the sharing of information. Many of the companies from which the government might request information—such as financial institutions, airlines, telecommunications companies—are multi-national corporations that are subject to foreign privacy laws. For example, in 1995, the European Union adopted its Privacy Directive, which severely regulated how companies could collect and use the information that they collected from their customers[45]. Since then similar laws have spread to other countries, such as Canada and Australia, so that practically all databases outside the United States are subject to some data protection restrictions—enforceable through fines, jail terms and private lawsuits.

The EU Privacy Directive, and related, implementing laws promulgated by the European Union's member countries,[46] for example, impose strict privacy practices on entities that are responsible for the processing of data. Depending on the circumstances, these restrictions can include, among other things, the obligation to use personal data for specified purposes only, the obligation to guarantee the security of the data against accidental or unauthorized access or manipulation, the obligation to notify a specific independent supervisory agency before carrying out all or certain types of data processing operations, and the obligation to notify data subjects of uses made of personally identifiable data. There are exceptions to the Directive and these privacy laws that can come into play in connection with the assertion by an EU member country of the need to process data for law enforcement, national security and other specified purposes. However, it is uncertain whether these exceptions apply to requests by the U.S. government. In the absence of an express exception, a company could face substantial liability for disclosing, without consent, a customer's personal data to the U.S. government for purposes not contemplated when the data was supplied. Indeed, the EU consistently threatens private companies with sanctions for cooperation with the U.S. government.

Substantial civil and criminal penalties apply to violations of the EU privacy laws. Any data subject who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to the Directive may be entitled to receive compensation. Further, in addition to private lawsuits, EU member states have laid down sanctions to be imposed in case of infringement of the provisions adopted pursuant to the Directive. In Spain, for example, the maximum fine is approximately $500,000; in Germany, it is approximately $300,000. Some statutes even impose prison sentences on offenders.

### Reimbursement

Another significant concern for private industry is reimbursement. The costs of collecting and providing information to the government can be substantial. In industries—like communications and finance—where the government makes frequent demands for information, companies must often establish separate departments, solely devoted to processing and responding to government requests. The large telephone companies and Internet service providers, for example, have entire staffs of clerks, attorneys, and former law enforcement agents (often as large as 30-50 employees) just to handle government subpoenas and court orders.

Provisions for reimbursing private companies for the costs of complying with such requests are fairly spotty. In those contexts where Congress has adopted specific statutes—such as the laws governing government surveillance of communications and government access to financial records—it has often adopted reimbursement provisions, entitling the private party to compensation for its costs in assisting the government. For example, the Electronic Communications Privacy Act provides that the government must compensate a telephone company or Internet service provider for its expenses, with a court determining what is a reasonable amount if the company and the government are unable to reach agreement.[47] Similarly, the Right to Financial Privacy Act confirms that the government must pay a financial institution a reimbursement fee, based on rates established by the Federal Reserve.[48]

Reimbursement is less clear, however, where Congress has not adopted definitive compensation provisions. For example, when responding to government subpoenas, the courts have developed a fairly amorphous common law rule. If the cost incurred by a private party is not "unreasonable," then the party is usually required to bear that cost without compensation as a "cost of citizenship." If, however, the cost is fairly significant (for example, the government has asked for several years worth of records for a particular customer), courts have suggested that the party should move to quash or modify the order. Then, a court can either restrict the government's request or require the government to compensate the party for the extraordinary costs.

## Endnotes

[1] *Katz v. United States*, 389 U.S. 347 (1967).

[2] Omnibus Crime Control and Safe Streets Act, Pub. L. 90-351 (1968) (codified, as amended, at 18 U.S.C. §§ 2510 et seq.).

[3] *Privacy Act*, Pub. L. 93-579, 88 Stat. 1897 (1974) (codified, as amended, at 5 U.S.C. § 552a).

[4] Department of Justice, *Guidelines on Domestic Security Investigations* (March 1976).

[5] *See, e.g.*, 18 U.S.C. § 2703(d) (authorizing an order that permits the government to obtain information from telephony companies and Internet service providers); 20 U.S.C. § 1232g(j)(2)(B) (authorizing an order that permits the government to obtain records from educational institutions).

[6] *United States v. Miller*, 425 U.S. 435 (1976). As discussed below, the *Miller* case involved bank records that were collected by the Bureau of Alcohol, Tobacco and Firearms pursuant to a grand jury subpoena. The Supreme Court ruled that the defendant had no Fourth Amendment "expectation of privacy" in the records because the records were "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." *Id.* at 442.

[7] Forty-five states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands also have adopted surveillance laws that apply to state and local law enforcement agencies within their jurisdiction. Generally, these state laws follow the federal rules, although, in a few cases, states have adopted more restrictive requirements.

[8] Electronic Communications Privacy Act, Pub. L. 99-508 (1986) (codified, as amended, at 18 U.S.C. §§ 2510 *et seq.*, 2701 *et seq.* & 3121 et seq.).

[9] Foreign Intelligence Surveillance Act, Pub. L. 95-511 (1978) (codified, as amended, at 50 U.S.C. §§ 1801 *et seq.*, 1841 *et seq.* & 1861 et seq.).

[10] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, Pub. L. 107-56 (2001) (codified in various sections of Titles 18 and 50 of the U.S.C.).

[11] 18 U.S.C. § 2703(c)(2).

[12] 18 U.S.C. § 2710. It is worth noting that many of the authorities adopted by Congress for counterintelligence and counter-terrorism investigations are specifically restricted to the FBI. *See also* 50 U.S.C. §§ 1861 *et seq.* (authorizing the Director of the FBI to obtain an order from the FISA court to access business records and other tangible items in foreign intelligence and terrorism investigations).

[13] Telephone companies and cable providers, however, are subject to separate federal laws that regulate their ability to distribute such information for commercial purposes. See 47 U.S.C. §§ 222 & 551.

[14] *See* 18 U.S.C. § 3123 (authorizing pen register/trap and trace orders in criminal investigations); 50 U.S.C. § 1842 (authorizing such orders in national security investigations).

[15] 18 U.S.C. § 2703(c)(1).

[16] 18 U.S.C. § 2703(d).

[17] 18 U.S.C. § 2703(a)-(b).

[18] 18 U.S.C. § 2518; 50 U.S.C. § 1805. FISA also permits the President of the United States to authorize surveillance without an order from the FISA court if the President finds, based on a certification from the Attorney General, that: i) there is no substantial likelihood that the surveillance will acquire communications to which a U.S. person is a party, and ii) either the communications are used exclusively by foreign powers or (for non-voice communications) are acquired from property or premises under the open and exclusive control of a foreign power. *See* 50 U.S.C. § 1802.

[19] 425 U.S. at 443.

[20] Right to Financial Privacy Act, Pub. L. 95-630, 92 Stat. 3697 (1978) (codified, as amended, at 12 U.S.C. §§ 3401 *et seq*).

[21] *See, generally*, 12 U.S.C. §§ 3405-3407.

[22] 12 U.S.C. § 3409(b).

[23] 12 U.S.C. § 3414.

[24] 12 U.S.C. § 3403(c).

[25] Bank Secrecy Act, Pub. L. 97-258, 96 Stat. 997 (1982) (codified, as amended, at 31 U.S.C. §§ 5311 et seq.).

[26] 31 U.S.C. § 5325.

[27] 31 U.S.C. § 5313(h).

[28] *See, e.g.*, Department of the Treasury, *Anti-Money Laundering Programs for Mutual Funds*, Interim Final Rule, 67 Fed. Reg. 21,117 (April 29, 2002) (codified at 31 C.F.R. pt. 103).

[29] Cable Communications Policy Act, Pub. L. 98-549, 98 Stat. 2794 (1984) (codified, as amended, at 47 U.S.C. § 551).

[30] 47 U.S.C. § 551(h).

[31] Video Privacy Protection Act, Pub. L. 100-618, 102 Stat. 3195 (1988) (codified at 18 U.S.C. § 2710).

[32] Family Educational Rights and Privacy Act, Pub. L. 93-380, 88 Stat. 571 (1974) (codified, as amended, at 20 U.S.C. § 1232g).

[33] 20 U.S.C. § 1232g(b)(1)(J). The provision also confirmed that the issuing agency or court could instruct the educational institution not to disclose the existence or the contents of the subpoena.

[34] 20 U.S.C. § 1232g(j).

[35] Department of Justice, *Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations* (March 1983).

[36] Department of Justice, *Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations* (March 1989).

[37] Department of Justice, *Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations* (May 2002).

[38] *See, e.g.*, 5 U.S.C. § 552a(e)(7).

[39] 5 U.S.C. § 552a(a)(8)(B)(iii) & (vi).

[40] *See, e.g.*, *McVeigh v. Cohen*, 983 F.Supp. 215 (D.D.C. 1998) (Where a Virginia-based Internet service provider paid an undisclosed sum in 1998 to settle a claim by a homosexual Navy sailor that the provider had improperly disclosed information about him to a Navy investigator).

[41] *See* 12 U.S.C. § 3417; 20 U.S.C. § 1232g(f); 47 U.S.C. § 551(f); 18 U.S.C. § 2710(c).

[42] 20 U.S.C. § 1232g(j)(3).

[43] 12 U.S.C. § 3403(c).

[44] 18 U.S.C. § 2702(c).

[45] European Union Council Directive 95/46/EC, 1995 O.J. (L 281) 31.

[46] *See, e.g.*, Spanish Organic Law 15/1999 on the Protection of Personal Data (B.O.E. 1999, 23570).

[47] 18 U.S.C. § 2706.

[48] 12 U.S.C. § 3415.