This product is part of the RAND Corporation monograph series. RAND monographs present major research findings that address the challenges facing the public and private sectors. All RAND monographs undergo rigorous peer review to ensure high standards for research quality and objectivity.

The Challenge of Domestic Intelligence in a Free Society

A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency

BRIAN A. JACKSON, EDITOR

Contributors: Agnes Gereben Schaefer, Darcy Noricks, Benjamin W. Goldsmith, Genevieve Lester, Jeremiah Goulka, Michael A. Wermuth, Martin C. Libicki, David R. Howell

Prepared for the Department of Homeland Security

HOMELAND SECURITY PROGRAM and
the INTELLIGENCE POLICY CENTER

This research was sponsored by the United States Department of Homeland Security and was conducted jointly under the auspices of the Homeland Security Program within RAND Infrastructure, Safety, and Environment and the Intelligence Policy Center of the National Security Research Division.

Library of Congress Cataloging-in-Publication Data

Jackson, Brian A.
The challenge of domestic intelligence in a free society : a multidisciplinary look at the creation of a U.S. domestic counterterrorism intelligence agency / Brian A. Jackson.
p. cm.
Includes bibliographical references.
ISBN 978-0-8330-4616-1 (pbk. : alk. paper)
1. Intelligence service—United States. 2. Terrorism—United States—Prevention. 3. Terrorism—Government policy—United States. I. Title.

JK468.I6J33 2009
363.325'1630973—dc22

2008046369

Cover photo courtesy of AP Photo/Mary Altaffer.

Published 2009 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Preface

With terrorism still prominent on the U.S. national agenda, whether the country's prevention efforts match the threat it faces continues to be central in policy debate. One element of this debate is questioning whether the United States, like some other countries, needs a dedicated domestic intelligence agency. To examine this question, Congress directed that the U.S. Department of Homeland Security Office of Intelligence and Analysis perform "an independent study on the feasibility of creating a counter terrorism intelligence agency" (U.S. Congress, 2006, p. 122). The results of this study are presented in three volumes:

- This volume contains a series of papers examining the U.S. context for domestic intelligence, current activities, and varied approaches for assessing options.
- An additional volume, published separately, *Considering the Creation of a Domestic Intelligence Agency in the United States: Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom* (Jackson, 2009), presents case studies of other nations' domestic intelligence organizations and activities.
- The overarching policy results of the assessment, including a discussion of the pros and cons of creating a new intelligence organization, are included in a companion volume to this work: *Reorganizing U.S. Domestic Intelligence: Assessing the Options* (Treverton, 2008).

This volume should be of interest to homeland security policymakers, state and local governments, law enforcement organizations, civil rights and civil liberties organizations, and private-sector organizations with interests in homeland security. This study is part of a larger body of RAND research related to homeland security, intelligence, and terrorism. Related RAND publications include the following:

- Peter Chalk and William Rosenau, *Confronting the "Enemy Within": Security Intelligence, the Police, and Counterterrorism in Four Democracies*, MG-100-RC, 2004
- K. Jack Riley, Gregory F. Treverton, Jeremy M. Wilson, and Lois M. Davis, *State and Local Intelligence in the War on Terrorism*, MG-394-RC, 2005
- Brian A. Jackson, Peter Chalk, Kim Cragin, Bruce Newsome, John V. Parachini, William Rosenau, Erin M. Simpson, Melanie Sisson, and Donald Temple, *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies*, MG-481-DHS, 2007.

The RAND Homeland Security Program

This research was conducted jointly under the auspices of the Homeland Security Program within RAND Infrastructure, Safety, and Environment and the Intelligence Policy Center of the National Security Research Division. The mission of RAND Infrastructure, Safety, and Environment is to improve the development, operation, use, and protection of society's essential physical assets and natural resources and to enhance the related social assets of safety and security of individuals in transit and in their workplaces and communities. Homeland Security Program research supports the Department of Homeland Security and other agencies charged with preventing and mitigating the effects of terrorist activity within U.S. borders. Projects address critical infrastructure protection, emergency management, terrorism risk management, border control, first responders and preparedness, domestic threat assessments, domestic intelligence, and workforce and training.

Information about the Homeland Security Program is available online (http://www.rand.org/ise/security/). Inquiries about homeland security research projects should be addressed to

Andrew Morral, Director
Homeland Security Program, ISE
RAND Corporation
1200 South Hayes Street
Arlington, VA 22202-5050
703-413-1100, x5119
Andrew_Morral@rand.org

The RAND Intelligence Policy Center

The Intelligence Policy Center is part of the RAND National Security Research Division (NSRD). NSRD conducts research and analysis for the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the defense agencies, the Department of the Navy, the Marine Corps, the U.S. Coast Guard, the U.S. Intelligence Community, allied foreign governments, and foundations.

For more information on RAND's Intelligence Policy Center, address queries to

John Parachini, Director
Intelligence Policy Center
RAND Corporation
1200 South Hayes Street
Arlington, VA 22202-5050
703-413-1100, x5579
John_Parachini@rand.org

More information about RAND is available at www.rand.org

Contents

Preface iii
Figures xi
Tables xiii
Acknowledgments xv
Abbreviations xvii

CHAPTER ONE
Introduction 1
Defining Domestic Intelligence 3
Arguments for Change in Current Domestic Intelligence Policies 6
About This Study 8

PART I
The U.S. Context for Domestic Counterterrorism Intelligence 11

CHAPTER TWO
The History of Domestic Intelligence in the United States: Lessons for Assessing the Creation of a New Counterterrorism Intelligence Agency 13
Agnes Gereben Schaefer
Domestic Intelligence Prior to World War I 14
World War I, the Palmer Raids, and the Stone Line 18
World War II and the Institutionalization of Domestic Intelligence Activities 22
Post–World War II Domestic Intelligence 30
Growing Concern About the FBI's Domestic Intelligence Activities 37

Terrorism and a Renewed Call for Expanded Domestic Intelligence Activities 42
Conclusions 44

CHAPTER THREE
Current Domestic Intelligence Efforts in the United States 49
Brian A. Jackson, Darcy Noricks, and Benjamin W. Goldsmith
Mapping the U.S. Domestic Intelligence Enterprise 50
Describing the Domestic Intelligence Enterprise 55
Discussion 69
Conclusions 77

CHAPTER FOUR
Societal Acceptability of Domestic Intelligence 79
Genevieve Lester
Public Threat Perception: Terrorism 82
The Balance of Civil Liberties and Security 89
Public Trust and Credibility 96
Public Perception and the Portrayal of Intelligence 100
Conclusions 103

CHAPTER FIVE
The Law and the Creation of a New Domestic Intelligence Agency in the United States 105
Jeremiah Goulka with Michael A. Wermuth
The Legality of Creating a New Federal Agency 108
Specific Legal Considerations 112
Conclusions 119

PART II
Exploring Different Approaches for Thinking About Creating a U.S. Domestic Counterterrorism Intelligence Agency 121

CHAPTER SIX
Weighing Organizational Models for a New Domestic Intelligence Agency 123
Genevieve Lester and Brian A. Jackson

Organizational Design and Domestic Intelligence 124
Adapting the Status Quo..... 126
Alternative Models for a Domestic Counterterrorism Intelligence Agency..... 132
Conclusions..... 147

CHAPTER SEVEN
Privacy and Civil Liberties Protections in a New Domestic Intelligence Agency..... 149
Martin C. Libicki and David R. Howell
The Privacy-Relevant Nature of Domestic Intelligence 150
Gauging Privacy..... 152
Elements of a Security/Privacy Trade-Off..... 157
Caveats 171
Conclusions..... 176

CHAPTER EIGHT
Exploring Measures of Effectiveness for Domestic Intelligence: Addressing Questions of Capability and Acceptability 179
Brian A. Jackson
The Need to Think About Intelligence Activities as a System for Linking Processes to Desired Outcomes..... 183
Exploring Potential Measures of Effectiveness for Domestic Intelligence Activities..... 186
Beyond Measures of Effectiveness: Exploring Measures of Acceptability and Factors That Shape the Legitimacy of Intelligence Activities..... 197
Conclusions..... 200

CHAPTER NINE
Exploring the Utility for Considering Cost-Effectiveness Analysis of Domestic Intelligence Policy Change..... 205
Brian A. Jackson
What Types of Benefits and Costs Are Associated with Domestic Counterterrorism Intelligence Activities? 206

How Can the Benefits of Domestic Counterterrorism Intelligence Activities Be Estimated? 213
How Can the Costs of Domestic Counterterrorism Intelligence Activities Be Estimated? 216
An Illustrative Break-Even Analysis of Changes in Domestic Counterterrorism Intelligence 226
Conclusions 235

CHAPTER TEN
Conclusion 239

Bibliography 241

Figures

3.1. The U.S. Domestic Intelligence Enterprise 52
6.1. Idealized Models for a New Domestic Intelligence Agency 133
8.1. Simplified Model of the Functions Making Up Intelligence and Counterterrorism Efforts 185
9.1. Critical Risk-Reduction Levels for Three Agency Models at Different Levels of Terrorism Risk (tangible costs only) ... 227
9.2. Drop in Critical Risk-Reduction Levels as Agency Costs Fall (from $5 billion to $0.5 billion annually) Due to Falling Transition Costs 229
9.3. Drop in Critical Risk-Reduction Levels as Agency Costs Fall (from $5 billion to $0.5 billion annually) for a Single Level of Terrorism Risk 230
9.4. Critical Risk-Reduction Levels for Three Agency Models at Different Levels of Terrorism Risk (tangible and low privacy cost) 231
9.5. Critical Risk-Reduction Levels for an Agency Costing $250 Million at Different Levels of Terrorism Risk (tangible and low, medium, and high privacy costs) 232
9.6. Critical Risk-Reduction Levels for Three Agency Models at Different Levels of Terrorism Risk (tangible and low estimate of total intangible costs) 233
9.7. Critical Risk-Reduction Levels for Three Agency Models at Different Levels of Terrorism Risk (tangible costs and privacy benefit) 234

Tables

8.1. Ideal Measures of Direct Counterterrorism Effect and Broader Efficiency and Effectiveness, by Intelligence Function 188
9.1. Summary of Illustrative Costs and Benefits of Intelligence-Policy Change 213

Acknowledgments

Like many RAND projects, this study relied on the efforts and contributions of a number of individuals inside RAND beyond those who are listed as authors of the chapters, as well as a variety of people outside of RAND who made critical contributions to the study.

First, we would like to acknowledge the contribution of our colleague and co–project leader for the study, Gregory Treverton. Greg's involvement significantly shaped the conduct of the project, and his experience and views were instrumental in shaping elements of the analyses included in this volume. In addition to the individual authors listed on the chapters, other RAND staff made important contributions to the conduct of the project, including, in alphabetical order, Mike Hix, Gordon T. Lee, Andrew R. Morral, John Parachini, K. Jack Riley, Lynn M. Scott, Douglas Shontz, Jerry M. Sollinger, and Katharine Watkins Webb. As part of the review of the various project documents and reports by experts both inside and outside RAND, Daniel Byman, James B. Bruce, Charles Nemfakos, Paul C. Light, and Paul R. Pillar all made important contributions to our thinking.

During our research, we reached out to experts and practitioners in the relevant fields and spoke to a wide range of individuals, only some of whom we can identify by name. A number of individuals inside and outside government at the federal, state, and local levels gave generously of their time and expertise in interviews with various project team members. However, because interviews were conducted on a not-for-attribution basis, we do not name those contributors in this monograph. The project also benefited from the involvement of a panel

of eminent experts in intelligence, law enforcement, and related areas who provided input at a key point in the study. The members of that expert panel, also listed alphabetically, were Marion Bowman, John Brennan, Joan Dempsey, Michael German, Richard Jerome, Richard Posner, Suzanne Spaulding, John P. Sullivan, and John Yoo.

Abbreviations

ACLU	American Civil Liberties Union
ADNET	Anti-Drug Network
ADVISE	Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement
APIS	Advance Passenger Information System
APL	American Protective League
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
AWW	America's Waterway Watch
BoI	Bureau of Investigation
CAPPS	computer-assisted passenger prescreening system
CBP	Customs and Border Protection
CI	counterintelligence
CIA	Central Intelligence Agency
CIFA	Counterintelligence Field Activity
COCOM	combatant command
COINTELPRO	counterintelligence program

COMINFIL	Communist Infiltration program
COMRAP	Comintern Apparatus program
CT	counterterrorism
CTD	Counterterrorism Division
DARPA	Defense Advanced Research Projects Agency
DCI	Director of Central Intelligence
DEA	Drug Enforcement Administration
DHS	U.S. Department of Homeland Security
DI	Directorate of Intelligence
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DNDO	Domestic Nuclear Detection Office
DNI	Director of National Intelligence
DoD	U.S. Department of Defense
DOJ	U.S. Department of Justice
EAD-NSB	executive assistant director for the National Security Branch
EMS	emergency medical services
EPIC	El Paso Intelligence Center
EU	European Union
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FIG	field intelligence group
FinCEN	Financial Crimes Enforcement Network

FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FTTTF	Foreign Terrorist Tracking Task Force
FY	fiscal year
GAO	U.S. General Accounting Office until 2004; U.S. Government Accountability Office thereafter
GID	General Intelligence Division
HCUA	U.S. House of Representatives Committee on Un-American Activities
HITDA	High Intensity Drug Trafficking Area
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HSA	Homeland Security Act
HSDN	Homeland Secure Data Network
HSIN	Homeland Security Information Network
HUMINT	human intelligence
I2F	Intelligence and Information Fusion
IAFIS	Integrated Automated Fingerprint Identification System
IC	intelligence community
ICE	Immigration and Customs Enforcement
IIC	Interdepartmental Intelligence Conference
IP	Internet protocol
IPv4	Internet protocol version 4

IRS	Internal Revenue Service
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISAC	information-sharing and analysis center
ISE	Information Sharing Environment
ISP	Internet service provider
JCN	Justice Consolidated Network
JIATF South	Joint Interagency Task Force South
JIATF West	Joint Interagency Task Force West
JITF-CT	Joint Intelligence Task Force for Combating Terrorism
JPEN	Joint Protection Enterprise Network
JRIC	Joint Regional Intelligence Center
JRIES	Joint Regional Information Exchange System
JTF North	Joint Task Force North
JTTF	joint terrorism task force
JUTNet	Justice Unified Telecommunications Network
LAPD	Los Angeles Police Department
LEO	Law Enforcement Online
MATRIX	Multistate Anti-Terrorism Information Exchange
MET	Mobile Enforcement Team
MID	Military Intelligence Division

MISI	Multi-Agency Information Sharing Initiative
NCIC	National Crime Information Center
NCTC	National Counterterrorism Center
N-DEx	Law Enforcement National Data Exchange
NDIC	National Drug Intelligence Center
NJTTF	National Joint Terrorism Task Force
NLETS	National Law Enforcement Telecommunication System
NOC	National Operations Center
NRC	National Response Center
NSA	National Security Agency
NSB	National Security Branch
NSS	National Security Service
OCDTEF	Organized Crime and Drug Enforcement Task Force
ODNI	Office of the Director of National Intelligence
OIA	Office of Intelligence and Analysis
OIPR	U.S. Department of Justice Office of Intelligence Policy and Review
ONDCP	Office of National Drug Control Policy
ONI	Office of Naval Intelligence
OSI	Office of Special Investigations
R&D	research and development
R-DEx	Regional Data Exchange

RISS	Regional Information Sharing Systems
SAR	suspicious-activity report
SRD	Systems Research and Development
SSN	social security number
TALON	Threat and Local Observation Notice system
TECS	Treasury Enforcement and Communications System
TEW	terrorism early warning group
TFI	Office of Terrorism and Financial Intelligence
TIA	Total Information Awareness; later Terrorism Information Awareness
TIDE	Terrorist Identities Datamart Environment
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Database
TWIC	Transportation Worker Identification Credential
US VISIT	United States Visitor and Immigrant Status Indicator Technology
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
USCG	U.S. Coast Guard
USCIS	U.S. Citizenship and Immigration Services
USJFCOM	U.S. Joint Forces Command

USNORTHCOM	U.S. Northern Command
USPACOM	U.S. Pacific Command
USSOCOM	U.S. Special Operations Command
USSOUTHCOM	U.S. Southern Command
USSS	U.S. Secret Service
VGTOF	Violent Gang and Terrorist Organization File
WMD	weapons of mass destruction

CHAPTER ONE

Introduction

In the current environment, the threat of terrorism is a major shaping force of many nations' international and domestic security policies. Nonstate groups with the intent and capability to take violent action are a reality in many countries given the existence of international movements, such as al Qaeda, that have the capacity to direct or inspire violence across the world, thereby creating another source of threat and risk. The threat of terrorist activity extends across a wide spectrum, from attacks causing little in the way of injury or damage to the potential for large-scale incidents. Although the probability of such high-consequence scenarios occurring is comparatively low, their ability to cause national-scale outcomes has meant that governments have focused their efforts on seeking to prevent them.

The core of government attempts to prevent violent and other criminal activity is intelligence and law enforcement, which, for many years, were viewed by Americans as separate activities. Put in place mainly to address the threat posed by agencies and agents of foreign governments, intelligence was viewed as an internationally focused activity that occurred largely outside U.S. borders. Intelligence agencies were charged with gathering information and learning about threats to the country, not prosecuting the perpetrators; these activities were designed to make it possible to take action to prevent attacks from happening. Law enforcement, in contrast, was done "at home" and, while certainly designed to help deter or prevent criminal activity, was largely a reactive enterprise. Law enforcement organizations, which generally did not act until after something had already happened, aimed to make

it possible to identify, apprehend, and punish those who broke the law. Differences between what Americans were comfortable with happening outside U.S. borders and which activities targeting Americans they thought should be prohibited to safeguard freedom from government intrusion meant that these two sets of activities were conducted under very different sets of rules, and barriers of various kinds—colloquially referred to as a "wall" to illustrate their perceived effect—were built between them.[1]

For many Americans, the attacks of September 11, 2001, called into question the fundamental assumptions that had underpinned U.S. intelligence and law enforcement activities. Actions by foreign individuals that were carried out largely within the United States resulted in a single attack that killed thousands of people. The boundary between intelligence agencies that had information and law enforcement organizations that could act domestically was viewed as part of the reason the attack was successful.

Perceived changes in the threat posed to the United States led to demand for more, and more effective, terrorism prevention and preparedness activities. According to some, these demands required a change in the way intelligence and law enforcement activities are carried out domestically and a significant alteration in the ground rules that regulate government monitoring and intervention activities within the United States. According to this view, to prevent future attacks, "intelligence must come home" and the government must be able to use data on persons and organizations located in the United States. At the same time, the United States has a history of distrusting centralized government power and, as a result, has often restrained government control over the lives and activities of individual citizens. The fact that responses to threats have consequences of their own—including the potential to significantly change the nature and character of the country—emphasizes the need to assess how intelligence activities can be sufficiently responsive while remaining acceptable to the population they are designed to protect.

---

[1] The history of domestic intelligence in the United States and the development of the separation of intelligence from law enforcement are discussed in greater detail in Chapter Two.

Defining Domestic Intelligence

What do we mean by the term *domestic intelligence*? The term *intelligence* sparks a range of associations, many of which stem from intelligence's connection with the secret activities of governments seeking to advance their interests in international affairs. In recent years, the term *intelligence* has been integrated into domestic law enforcement and public safety agencies as part of the phrase *intelligence-led policing*. Definitions of *intelligence-led policing* vary, but common elements include the use of information-gathering capabilities and the analysis and application of resulting information in crime prevention and response activities in addition to their more traditional use in the prosecution of past criminal acts (see, e.g., Weisburd and Braga, 2006; Milligan, Clemente, and Schader, 2006; Ratcliffe, 2002; Peterson, 2005). Use of the term *intelligence* has also spread beyond government organizations into private-sector organizations and elsewhere.[2] To some, the term is most closely associated with the collection of information; others see intelligence as a more general category that includes a much broader range of activities. Such variety in the use and understanding of these terms complicates policy debate, and the lack of standard definitions for intelligence activities focused on homeland security and domestic counterterrorism (CT) efforts has been cited as a significant impediment to designing and assessing policy in this area (Masse, 2003, 2006).

To guide the work reported in this volume, we define *domestic intelligence* as efforts by government organizations to gather, assess, and act on information about individuals or organizations in the United

[2] For example, an entire body of literature has grown around the concepts of business intelligence and competitive intelligence. The literature examines how data and information are collected, analyzed, and applied by the private sector to build or defend competitive advantage in the market.

States or U.S. persons elsewhere[3] that are *not related to the investigation of a known past criminal act or specific planned criminal activity*.[4]

It is often the case that an individual or organization that carries out a terrorist attack—or has specific plans to do so (e.g., the attacker has conspired to acquire weapons for a future attack)—has committed one or more specific crimes. In these cases, traditional law enforcement approaches for investigating and prosecuting these crimes apply. The major difference between intelligence approaches and those used during traditional law enforcement stems from the former's emphasis on preventing future events—i.e., on acting when the individuals or organizations planning an attack may not yet have committed any prosecutable criminal offenses. Intelligence activities can be *investigative* in nature and may resemble law enforcement activities. However, they do not have to satisfy the same legal requirements that constrain the initiation of a law enforcement investigation. An example of such an intelligence activity is investigating a tip about the suspected terrorist behavior of an unknown group to determine whether the tip is credible and, if it is, acting to prevent the attack. However, given substantial concern about the ability of even a single individual working alone to plan and execute acts of terrorist violence, investigative follow-up may not be enough to address the threat of terrorism. As a result, another type of intelligence effort can be more *explorative* in character,

---

[3] Federal law and executive order define a U.S. person as "a citizen of the United States, an alien lawfully admitted for permanent residence, an unincorporated association with a substantial number of members who are citizens of the U.S. or are aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the U.S." (NSA, undated). Although this definition would therefore allow information to be gathered on U.S. persons located abroad, our objective was to examine the creation of a domestic intelligence organization that would focus on—and whose activities would center around—individuals and organizations located *inside the United States*. Though such an agency might receive information about U.S. persons that was collected abroad by other intelligence agencies, it would not collect that information itself.

[4] As our discussion of intelligence-led policing suggests, traditional law enforcement does indeed involve the collection and use of information that is not linked to specific criminal activities. However, activities we consider *domestic intelligence* differ in the scope and breadth of effort involved. Domestic intelligence activities are not a new phenomenon; see, for example, discussion in Morgan (1980, p. 13).

seeking proactively to (1) identify individuals or groups that might be planning violent actions and (2) gather information that might indicate changes in the nature of the threat to the country more broadly (see, e.g., DeRosa, 2004). Such explorative activity inherently involves gathering a broader spectrum of data about a greater number of individuals and organizations who are unlikely to pose any threat of terrorist activity.

Our definition of *domestic intelligence* parallels those that appear in the academic literature that has examined U.S. policy in this area over the past several decades (see, e.g., Morgan, 1980). However, it is narrower than more-general definitions that seek to capture the full breadth of intelligence requirements associated with homeland security or homeland defense.[5] Our focus on the collection and use of information about individuals and organizations means that we have focused on the tactical threat-identification and threat-disruption parts of homeland security intelligence. Thus, we do not consider activities such as analyses designed to identify societal vulnerabilities or map the threat to those identified vulnerabilities to guide broader homeland security policies.[6] Others have noted that the boundary between intelligence and law enforcement activities has blurred over time, particularly in response to transnational threats such as drug trafficking and terrorism. This blurring of the boundary between the two complicates an examination focused largely on the CT mission.[7]

---

[5] For a more general review of homeland security intelligence, see Masse (2006).

[6] The 2002 *National Strategy for Homeland Security* (Office of Homeland Security, 2002, pp. 15–19) includes a four-part breakdown of homeland security intelligence and information-analysis roles and responsibilities: (1) tactical threat analysis, (2) strategic analysis of the enemy, (3) vulnerability assessment, and (4) threat-vulnerability integration, or "mapping." Though this taxonomy was not included in the 2007 version of the national strategy, we found it useful for defining the scope of the domestic intelligence activities considered during this study. Similar broad definitions are suggested in Markle Foundation Task Force (2002) and Gilmore Commission (2002, p. iv).

[7] See, for example, discussion in Best (2001). This blurring—and the difficulty of crafting clear boundaries between activities focused on national security threats and those focused on aiding "in the capture of prospective or practicing criminals"—was cited as a particular difficulty in a review of Department of Homeland Security intelligence activities in June 2007 (DHS OIG, 2007, p. 3).

Arguments for Change in Current Domestic Intelligence Policies

Because of the prominence of the terrorist threat, particularly in the years since the 9/11 attacks, how the United States has responded to the threat of terrorism, the effectiveness of the steps that have been taken, and the appropriateness of such steps given deeply held values of personal freedom and liberty have been prominent questions in public and policy discussions. Nationally chartered commissions, nongovernmental organizations, scholars, commentators across the political spectrum, and the public have weighed in on various issues related to CT and intelligence.[8] Most of these discussions have addressed terrorism and intelligence writ large, covering issues relevant to *all* national intelligence efforts, domestic and foreign, rather than domestic intelligence alone. Others have been specific to domestic intelligence activities. The following issues that are relevant and central to the consideration of a new domestic intelligence agency have been raised:[9]

1. **The difficulty of identifying a small number of threatening individuals in the general population of a large and diverse nation.** Terrorism will always be a threat posed to the many by the few, which means that intelligence activities must detect weak signals of threat behaviors against a strong background of legitimate activity. There are concerns that U.S. domestic intelligence efforts, as currently constituted, may not be sufficient to detect all threats to the country.
2. **The need for sufficient adaptability to respond to dynamic threats.** Many terrorist organizations have demonstrated that they can rapidly alter their behavior and adapt their tactics in the face of CT pressure. To keep pace with an agile threat,

[8] The findings and arguments of many of these actors are reviewed in Chapter Three, which assesses current domestic counterterrorism intelligence efforts.

[9] Of these issues, the first two—the difficulty of identifying a small number of threatening individuals against a large background of other people and the need for adaptability—are problems relevant to all intelligence efforts. The remaining issues are specific to domestic intelligence activities.

intelligence organizations must be able to adapt as well. Large, bureaucratic organizations frequently face challenges in doing so, and the ability to change rapidly may conflict with other objectives—including societal goals of intelligence oversight.

3. **Problems in interagency cooperation.** In contrast to foreign intelligence, which mainly involves federal organizations, domestic intelligence is an inherently interagency and multilevel enterprise. The United States has thousands of independent law enforcement organizations, and government and nongovernmental entities not normally associated with security missions (e.g., the fire service and private-sector firms) may have information that could indicate threatening activity. The involvement of many organizations in intelligence activities has always posed a risk of breakdowns in information sharing, turf battles, and bureaucratic duplication and inefficiency.
4. **Differences in the ways in which law enforcement and intelligence organizations operate.** Preventing terrorism domestically inherently straddles functions that have historically been divided between law enforcement and intelligence agencies. In the United States, law enforcement organizations—most notably, the Federal Bureau of Investigation (FBI)—have central roles in domestic intelligence activities related to the prevention of terrorism. These different types of organizations have distinct cultures and have generally focused their efforts quite differently, leading to questions about whether the two can be mixed effectively and whether doing so undermines the nation's ability to detect and prevent terrorism. Separating intelligence efforts from law enforcement activities has been an argument for changing domestic intelligence organizations and activities.
5. **Concern about the effect of intelligence activities on personal privacy and civil liberties.** Intelligence activities that require government intrusion into individuals' private lives raise significant and real concerns about the effect of those activities on individuals and on the character of the nation, entities that such activities are intended to protect. Since 9/11, some people have raised questions about the type of information the U.S.

government has gathered on individuals and organizations in the United States and about how that information has been collected and used. Throughout the history of U.S. domestic intelligence, questions about how long the government should store intelligence data about individuals—and about how responsive the government is to direction to destroy those data—have come up repeatedly.

All of these factors have been cited as rationales for changing the way in which domestic intelligence and CT activities are carried out.

About This Study

In spite of significant changes to U.S. domestic intelligence activities in recent years, questions remain about whether the United States has the right organizational and technical tools in place to protect the nation. One element of this debate is the question of whether the United States needs a dedicated domestic intelligence agency. The argument that such an agency is necessary has been raised during policy debates and considered by a number of national commissions that address U.S. domestic security and the threat of terrorism.[10] Such a policy change is, of course, only one of many possible changes that could be made in U.S. CT policy, but it is one that recurs in policy discussions[11] and could be a reaction to a future terrorist attack on the United States.

To examine this potential policy change, Congress directed that the U.S. Department of Homeland Security Office of Intelligence and Analysis perform "an independent study on the feasibility of creating a counter terrorism intelligence agency" (U.S. Congress, 2006, p. 122). If such an agency were built, the major rationale for doing so would be the desire to improve security and the belief that a new agency would

[10] What different individuals and organizations meant by considering the need for a domestic intelligence agency differed. The range of options and their implications will be discussed in subsequent chapters.

[11] For example, discussion during October 2007 congressional hearings as reported in Johnson (2007).

be more *capable* of protecting the country from terrorism than are current domestic intelligence efforts. However, given significant concerns about the effect of security and intelligence policies on the American people, privacy, and the character of the country, any new organization would also have to be *acceptable* to the public. RAND was not asked to make a definitive recommendation about whether to create such an agency but was charged with examining relevant options and issues in order to frame policy choices.

In considering the potential creation of a new domestic intelligence agency, we approached the issue from a variety of directions, seeking insights that would help us understand the pros and cons of creating such an organization and describe different approaches for doing so. This research effort resulted in a set of topical papers and analyses that address different parts of this policy issue and examine it from different perspectives. The overall study examined both issues associated with and approaches to understanding the U.S. domestic context for domestic intelligence and ways of examining the decision to create a new domestic intelligence agency. In addition, we examined the histories of several nations that already have such an agency in an effort to learn from their experiences.

This volume presents the set of papers focused on the U.S. domestic context and approaches for understanding the decision to create a new domestic intelligence agency, organized into two sections:

- *Part I: The U.S. Context for Domestic Counterterrorism Intelligence:* Policy discussion about creating a new domestic intelligence agency and how such an organization might be designed must understand and consider the current environment for domestic intelligence in the United States. Domestic intelligence efforts have a long, complex, and controversial history in this country that shapes public views. The nature and effectiveness of current intelligence activities shape the potential benefits of making major organizational changes and constrain the options for doing so. Chapters Two through Five examine various elements of the domestic context for intelligence efforts including U.S. history surrounding these matters, current domestic intelligence efforts,

factors shaping the societal acceptability of intelligence activities, and the institutional legal issues in creating a new federal agency.

- *Part II: Exploring Different Approaches for Thinking About Creating a U.S. Domestic Counterterrorism Intelligence Agency:* The complexity of the different factors shaping consideration of domestic intelligence, ranging from different views on the scope of the threats these efforts address to divergent levels of trust in the government agencies managing them, make considering new—potentially expanded—intelligence efforts difficult. The second part of this volume (Chapters Six through Nine) contains four conceptual contributions, each focused on different ways of thinking through potential changes in domestic intelligence activities and how to assess them. They include examinations of different organizational models of such an agency, approaches to considering privacy and civil liberties protections in an operational context, a discussion of potential metrics for assessing domestic intelligence activities, and an exploration of how quantitative approaches, such as cost-benefit or cost-effectiveness analysis, might inform thinking about domestic intelligence policy change.

This volume is one of three RAND publications that resulted from this research effort. The other two are a cross-cutting policy document examining the pros and cons of creating a new intelligence organization (Treverton, 2008) and a companion volume containing the remainder of the foundational research papers for the study examining other countries' domestic intelligence efforts (Jackson, 2009).

PART I

The U.S. Context for Domestic Counterterrorism Intelligence

In considering creating a new domestic counterterrorism intelligence agency, the current domestic environment must be central in policy deliberation. The chapters in this part of the book explore that domestic environment from four directions:

- While the current focus is the risk of terrorism, domestic intelligence efforts have been a part of the United States since the founding of the nation. The ways in which those efforts have been carried out—and the controversies they have created—shape how any new agency would be received. The first chapter examines that history.
- Though having a new domestic agency would be a major shift in intelligence policy, government organizations at all levels are already undertaking such activities in the fight against terrorism. Chapter Three examines the current state of the U.S. domestic intelligence enterprise and maps the connections among ongoing efforts and organizations at all levels, inside and outside government.
- Whether a new federal domestic intelligence agency could be successfully created would also depend on whether the American people viewed doing so to be acceptable. Public views of intelligence activities have varied over time, with threat perceptions shaping the scope and nature of intelligence efforts that are viewed as acceptable. The third chapter in this part of the book examines the information available for understanding public acceptability of intelligence activities and the factors that shape it.

- Most legal debate regarding domestic intelligence focuses on privacy and civil liberties issues stemming from surveillance. However, the institutional legal and constitutional questions arising in the context of the possible creation of a new federal agency are rarely addressed. These questions do not inherently consider how to conduct domestic intelligence activities. The final chapter discusses the specific legal issues connected with the creation of a new domestic intelligence agency.

CHAPTER TWO

The History of Domestic Intelligence in the United States: Lessons for Assessing the Creation of a New Counterterrorism Intelligence Agency

Agnes Gereben Schaefer

The history of domestic intelligence in the United States dates back to the founding of the country and, when examined closely, reveals cyclical episodes in which concerns about spies and "enemies within" have spurred increased domestic intelligence activity. This overview of the historical development of domestic intelligence in the United States reveals two common themes that have arisen during those cyclical episodes that are particularly relevant to considering the creation of a new domestic intelligence agency:

- the struggle to organize political institutions around intelligence and counterterrorism (CT) and determine their appropriate scope and responsibilities
- the attempt to balance civil liberties and national security, particularly during wartime.

From the concern about French spies during John Adams's presidency to concerns about al Qaeda during the George W. Bush administration, these two themes have been raised time and again, and remarkably similar arguments have been made regarding how to protect the nation against potential threats.

Domestic Intelligence Prior to World War I

Internal surveillance during the first century and a half of U.S. history was sporadic, with the federal government responding ad hoc to crises of the moment. Once the crises waned, intelligence and surveillance efforts ceased, and the governmental mechanisms that supported domestic intelligence were dismantled (Morgan, 1980). For instance, the Adams administration was concerned that French agents were spreading Jacobinism[1] in the United States, that the Jeffersonian opposition would align itself with France, and that this would lead to the same sort of social upheaval that occurred in France during the French Revolution.

In response to concerns that social upheaval would occur in the United States, the Federalist-led Congress passed four laws in 1798 that became known as the Alien and Sedition Acts. These laws were passed in the name of national security and increased the government's authority to crack down on dissent. The first of the four laws, the Naturalization Act, made the process of naturalization more difficult by extending the residence requirement for U.S. citizenship from five years to 14 years (U.S. Congress, 1798). The Alien Act granted the President of the United States the authority to deport any alien whom he deemed "dangerous to the peace and safety of the United States." The Alien Enemies Act allowed that, in wartime,

> all citizens, denizens, or subjects of the hostile nation or government, being males of the age of fourteen years and upwards, who shall be in the United States and not naturalized, shall be liable to be apprehended, restrained, secured and removed, as enemy aliens.

The Sedition Act was the most far-reaching of the four laws and legislated that any person who was found guilty in a court of law of writing, printing, uttering, or publishing "any false, scandalous or malicious writing or writing against the United States" would be punished by a fine not exceeding $2,000 and imprisoned for no more than two years.

---

[1] Violent revolutionary beliefs associated with elements of the French Revolution.

The Federalists blatantly used the Sedition Act against their political opposition. For instance, the Sedition Act was used to shut down several opposition newspapers or arrest their editors.

The public overwhelmingly viewed the Alien and Sedition Laws as an assault on First Amendment freedoms. In response to the Alien and Sedition laws, Jefferson and Madison anonymously drafted the Kentucky and Virginia Resolutions, which declared the Alien and Sedition Acts void and accused Congress of overstepping its authority. The public's discontent with the Alien and Sedition laws was mighty and probably played a large part in the election of Thomas Jefferson in 1800. Ultimately, the Alien and Sedition Acts were repealed or allowed to expire, and they became viewed as examples of unacceptable governmental interference in the political process and served to constrain future leaders when responding to dissent (Morgan, 1980, p. 19). During subsequent episodes of wartime, Congress enacted laws that restricted civil liberties (using the same national security arguments that underlay the Alien and Sedition Acts), but never to the extent that the Alien and Sedition laws of 1798 did.

Intelligence During the Civil War and Spanish-American War

During the Civil War, most security intelligence functions were performed by the military. In response to the threat from saboteurs, President Abraham Lincoln suspended the writ of habeas corpus in 1861, and the Habeas Corpus Act of 1863 allowed the government to round up suspected spies and saboteurs (see Morgan, 1980, p. 20). When the military discontinued its surveillance program after the Civil War, Allan Pinkerton, who had worked for the War Department under President Lincoln, founded a private detective agency. The Pinkerton Agency and other private detective forces later served the government and private companies (Finnegan, 1998, p. 11; Church Committee Report, 1976, p. 378), until 1892, when Congress prohibited government agencies from hiring people currently employed in the private sector (Theoharis, 2004, p. 16).

It was not until the 1880s that intelligence became institutionalized within the military. Up until this point, intelligence was primarily carried out during war, and therefore, intelligence capabilities were

thin and expertise was difficult to maintain. In 1882, the U.S. Navy established the Office of Naval Intelligence (ONI) with the purpose of observing and reporting on advances in maritime technology overseas (Batvinis, 2007, p. 33). The United States' victory over the Spanish Navy during the Spanish-American War confirmed the value of ONI, and in 1899, it became formally institutionalized in the Navy bureaucracy. Within a few years of the war however, ONI experienced a sharp decline as interest in war-planning intelligence subsided (Batvinis, 2007, p. 33).

With the establishment of the Division of Military Information in 1885 as part of the Military Reservations Division, Miscellaneous Branch, of the Adjutant General's Office, the U.S. Army was given a permanent intelligence organization. Before this, without any organizational support, each U.S. commander served as his own intelligence officer, and the intelligence function was limited to reconnaissance in time of war or during domestic military campaigns (Finnegan, 1998, p. 8).

During the Spanish-American War, the U.S. Secret Service—which was established in the U.S. Department of the Treasury to investigate counterfeiting in 1865—served as the main civilian intelligence agency. The Secret Service had "organized an emergency auxiliary force to track down Spanish spies, placed hundreds of civilians under surveillance, and asked the Army to arrest a number of alleged spies."[2]

Establishment of the U.S. Department of Justice

The Justice Department was established in 1870 primarily to address corruption in Congress. Its investigative authority stemmed from an appropriations statute first enacted in 1871, allowing the attorney general to use funds for "the detection and prosecution of crimes against the United States" (Church Committee Report, 1976, p. 379). Secret Service agents were regularly assigned to the Justice Department as investigators until 1908, when Congress prohibited this practice (some believe to prevent them from investigating corruption in Congress). In

[2] Church Committee Report (1976, p. 378). It was not until after the assassination of President William McKinley that the Secret Service was authorized to protect the President.

response, in 1908, the attorney general issued an order authorizing the creation of the Bureau of Investigation (BoI). Until this point, federal crime-detection activity increased in response to passing crises, such as the rise of the Ku Klux Klan in the 1870s and concern about Spanish spies during the 1890s. With the creation of the BoI, a permanent force of agents was placed under the attorney general's direct control (Jeffreys-Jones, 2007, p. 39). Importantly, there was no formal congressional authorization for the bureau, but Congress regularly approved its appropriations (Church Committee Report, 1976, p. 379).

During this same period, the country was also dealing with the threat of terrorism from individuals and anarchist groups. Attacks that occurred included bomb and firearm attacks, including the assassination of President McKinley by Leon Czolgosz in 1901. Even before the assassination, domestic intelligence activities in response to the anarchist threat included

> according to a memorandum by George Cortelyou, the president's personal secretary, "pretty thorough records of the criminal and anarchist classes, the secret service having in some instances alphabetical lists of all the anarchists in a city". [S]ince Czolgosz's name had not appeared on any of these lists prior to his deadly deed, one may question their value. (Jensen, 2001, p. 20)

After the assassination, law enforcement responses to the perceived threat included arrests of significant numbers of individuals on suspicion of involvement in the attack (see Jensen, 2001).

The BoI was created during an era in which the role of the federal government increased and the states'-rights tradition was slowly supplanted with the perspective that federal, state, and local governments should share responsibility, particularly in the area of law enforcement. Due to the emergence of nationwide transportation, increased immigration, and new communication technology, the role of the federal government needed to change and expand beyond its traditional roles of promoting foreign commerce and defending against foreign invasion (Theoharis, 2004, p. 1). With the passage of the Mann Act (which banned the interstate transportation of women for "immoral purposes") and other federal statutes, the criminal investigative responsibilities of

the Justice Department and the BoI expanded. Even as late as 1915, however, the bureau was not involved in domestic intelligence activities because it was the Justice Department's position that the BoI had no authority to engage in such activities. During this time, the Secret Service was the primary agency that investigated potential spies.

In 1916, the attorney general objected to the Secret Service investigating activities that did not actually violate federal law, but President Woodrow Wilson and his secretary of state continued to be interested in these types of investigations. In response, the attorney general went to Congress and requested an amendment to the Justice Department's appropriations statute, which would allow the Justice Department to take over responsibility for the investigations that the Secret Service was conducting. The statute was revised to allow

> the Attorney General to appoint officials not only to detect federal crimes, but also to conduct such other investigations regarding official matters under the control of the Department of Justice or the Department of State. . . . This amendment was intended to be an indirect form of authorization for investigations by the Bureau of Investigations, although a State Department request was seen as prerequisite for such inquiries. (Church Committee Report, 1976, p. 379)

As the United States entered World War I, preparation for the war and domestic security investigations rested mostly with the Secret Service and the Justice Department's BoI because the military lacked the resources to conduct intelligence operations (Church Committee Report, 1976, pp. 379–380).

World War I, the Palmer Raids, and the Stone Line

In response to the country's entry into WWI, the passage of the Immigration (1917), Espionage (1917), Sedition (1918), and Anarchist (1918) Acts provided the Justice Department (and the BoI) with legal authority to conduct domestic intelligence activities. Reminiscent of the Alien and Sedition Acts of 1798, the Espionage Act of 1917 made it "ille-

gal to oppose the draft and other wartime policies," and the Sedition Act of 1918 made it "illegal to criticize the government, especially in its prosecution of the war" (Jeffreys-Jones, 2007, p. 70). The Immigration Act of 1917 enlarged the classes of aliens excludable from the United States, and the Anarchist Act of 1918 expanded the provisions for excluding subversive aliens. All of these pieces of legislation allowed the BoI to increase its scope in the name of national security. Thus, as in the early history of the country, the domestic intelligence apparatus was strengthened in response to perceived external threats.

The initial threat was the activity of German agents, including sabotage and espionage. In response to this threat, the BoI and military intelligence worked directly with the American Protective League (APL), a nongovernment group. The APL,

> composed of well-meaning private individuals, was formed as a citizen auxiliary to "assist" the Bureau of Investigation. In addition to the authorized auxiliary, ad hoc groups took it upon themselves to "investigate" what they felt were un-American activities. (Church Committee Report, 1976, p. 381)

> [During World War I] the threat to the nation's security and the war effort was perceived by both government and private intelligence agencies as extending far beyond activities of enemy agents. Criticism of the war, opposition to the draft, expression of pro-German or pacifist sympathies, and militant labor organizing efforts were all considered dangerous and targeted for investigation. (Church Committee Report, 1976, p. 382)

Post–World War I Intelligence

The end of the war in 1918 did not bring an end to domestic intelligence activities. The BoI shifted its attention away from critics of the war to the activities of radical and anarchist groups (Church Committee Report, 1976, p. 382). In the spring of 1919, the country experienced a string of terrorist bombings. In response, Attorney General A. Mitchell Palmer established a General Intelligence Division (GID)

within the Justice Department to investigate political militants. Palmer assigned J. Edgar Hoover to head the newly established GID due in part to Hoover's experience during the war as head of the department's program for compiling information on enemy aliens. Less than two weeks after the GID was established, the director of the BoI ordered an expansion of bureau examination "of anarchist and similar classes, Bolshevism, and kindred agitations advocating change in the present form of government by force or violence, the promotion of sedition and revolution, bomb throwing, and similar activities" (Church Committee Report, 1976, p. 383).

In 1919, the mood in the country was that the country indeed needed to "act decisively against the radical threat." For example, the secretary of state wrote a private memo to the attorney general in which he stated, "It is no time to temporize or compromise; no time to be timid or undecided; no time to remain passive. We are [face] to face with an inveterate enemy of the present social order" (Church Committee Report, 1976, p. 383). These words would echo in eerily similar ways in the speeches made by officials in subsequent times of war.

In November 1919, the GID directed agents from the BoI and the Immigration Bureau to carry out simultaneous raids against radicals in 11 cities. On January 2, 1920, BoI and Immigration Bureau agents in 33 cities rounded up some 10,000 people believed to be members of the Communist and Communist Labor Parties. These raids, known as the Palmer Raids, were seen as major abuses of due process, and the Senate Judiciary Committee investigated them in 1921. Ultimately, the committee was divided in its findings, but the Justice Department and the BoI were put on the defensive.

In addition to the Justice Department's and Immigration Bureau's operations after the war, military intelligence continued its wartime surveillance activities into the postwar era. After 1919, the Military Intelligence Division (MID) "resumed investigations aimed at strikes, labor unrest, radicals, and the foreign language press" (Church Committee Report, 1976, p. 387). The APL disbanded, but its former members still "served as volunteer agents for military intelligence as well as for the Bureau of Investigation" (Church Committee Report, 1976, p. 387). Following the Palmer Raids, the GID and military intelli-

gence shared more information, with military intelligence agreeing to "provide Hoover with information from foreign sources, since the State Department had refused to do so and Hoover was prohibited from having agents or informants outside the United States" (Church Committee Report, 1976, p. 387).

Corruption and Reform

Ironically, with Prohibition came an era of lawlessness in the 1920s and a new set of challenges for law enforcement. Local and state authorities could not curb the tide of criminal activities (due to either corruption or a lack of resources); therefore, the emergence of a federal role in law enforcement seemed necessary. However, during the early 1920s, the Justice Department and the BoI became entangled in the corruption that characterized Warren Harding's administration. Most significantly, when Congress asked that the Justice Department investigate members of the Harding administration, the director of the BoI, William J. Burns, instead used BoI agents to investigate the members of Congress who asked for the investigation. These investigations included physical surveillance and illegal entries into Senate offices to open mail and search files. This incident served only to further tarnish the image of the Justice Department and the BoI after the Palmer Raids.[3]

In an effort to restore the Justice Department and BoI reputations, Calvin Coolidge appointed Harlan Fiske Stone, an outspoken critic of the Palmer Raids, to be attorney general in 1923. Stone was particularly concerned that the BoI had become "a secret political police force." In fact, he believed that "the organization was lawless, maintaining many activities [that] were without any authority in federal statutes, and engaging in many practices [that] were brutal and tyrannical in the extreme" (Church Committee Report, 1976, p. 388). In 1924, Stone offered J. Edgar Hoover the position of director of the BoI. Hoover accepted on the conditions that the BoI be removed from politics, that appointment and promotion be made solely on merit, and that the BoI be responsible only to the attorney general (Morgan, 1980, p. 30). Stone agreed to these conditions. In addition to appoint-

[3] During this time, the GID was made part of the BoI.

ing Hoover as director of the BoI, Stone established the Stone Line—a policy that restricted the BoI to investigating particular violations of federal laws and specifically prevented it from gathering intelligence. Now an investigation could be undertaken only if it was alleged that there was a specific violation of a federal statute. In response to the reforms enacted by Stone, the American Civil Liberties Union (ACLU) declared that the Justice Department's "red-hunting days were over," and over the next decade, the BoI disengaged from domestic intelligence (Church Committee Report, 1976, p. 389).

At the same time, exchanges of potentially consequential information among the BoI, MID, and ONI ended. The MID was severely weakened when, in 1920, the Army's countersubversion squad was disbanded, and in 1921, the Negative Intelligence Branch of the MID was eliminated. As a result of the elimination of its Negative Intelligence Branch, the MID could now supply reports to BoI field offices "only upon a specific request" of MID headquarters in Washington. "With that decision, any chances of developing a functional counterintelligence information-sharing system capable of protecting U.S. interests from foreign intelligence aggression [were] delayed for another fifteen years" (Batvinis, 2007, p. 44).

World War II and the Institutionalization of Domestic Intelligence Activities

Echoing previous episodes in history, the rise of Nazi Germany, Imperial Japan, and Stalinist Russia resulted in increased concern about internal security. In 1934, President Franklin D. Roosevelt ordered the BoI to conduct an investigation of "the activity of the Nazi movement in this country" (Church Committee Report, 1976, p. 393). In January 1936, the secretary of war advised the attorney general that there was "definite indication" of foreign espionage in the United States, and he urged the Justice Department to establish

> a counterespionage service among civilians to prevent foreign espionage in the United States and to collect information so that

> in case of an emergency any persons intending to cripple our war effort by means of espionage or sabotage may be taken into custody. (Church Committee Report, 1976, p. 393)

In his State of the Union address in January 1934, Roosevelt reinforced the need for an increased federal role in law enforcement by identifying crime as a serious threat to "our security" and one that required "the strong arm of the federal Government" (Theoharis, 2004, p. 42). In 1935, the BoI's name was officially changed to the Federal Bureau of Investigation (FBI), identifying it as a national law enforcement agency.

With growing concern about Nazi propaganda in the United States, Roosevelt began to consider options for investigating the sources of this propaganda. "Aware of the strict limitations on intelligence investigations, [Roosevelt] recognized that only immigration laws applied in this situation, making the Immigration Services (an agency of the Department of Labor) the lead agency for any potential investigation," and the Secret Service and FBI would also be involved. The FBI would serve as the "clearinghouse" for all information that was collected (Batvinis, 2007, p. 46).

In August 1936, President Roosevelt met with Hoover to discuss the state of domestic intelligence. Hoover informed Roosevelt that the FBI was not collecting domestic intelligence and that it did not have the authority to do so unless it involved a violation of U.S. law. However, Hoover also informed Roosevelt that, under the Appropriations Act of 1916, the FBI was authorized to undertake investigations at the request of the secretary of state. The secretary of state requested such investigations in order to improve the nation's intelligence, and over the next two years, FBI domestic intelligence activities increased.

Thus, President Roosevelt used his executive authority to determine that the FBI would be the primary civilian agency responsible for carrying out domestic intelligence. However, Roosevelt chose to handle this confidentially, so his orders were kept secret and Congress was deliberately excluded from the domestic intelligence policymaking process until after war broke out in Europe in 1939. It was the international character of communism and fascism that justified both the

President's desire for domestic intelligence and the secretary of state's request to have the FBI conduct investigations.

FBI field offices were immediately ordered

> to obtain from all possible sources information concerning subversive activities being conducted in the United States by Communists, Fascists, representatives or advocates of other organizations or groups advocating the overthrow or replacement of the Government of the United States by illegal methods. (Church Committee Report, 1976, p. 396)

This order represented a new mind-set in which an *investigation* was "conducted when there [was] a specific violation of a Criminal Statute involved, always presuppose[d] an overt act and [was] proceeded upon with the very definite intention of developing facts and information that will enable prosecution under legislation." *Intelligence* activities, on the other hand, involved monitoring activities that did not include an overt act or violation of a specific statute but could have become a violation of law in the event of a declaration of war or national emergency (Theoharis, 2004, p. 46).

The Creation of the Interdepartmental Intelligence Conference

After a series of espionage incidents in the late 1930s, Roosevelt ordered his attorney general to chair a committee of representatives from the FBI, MID, and ONI to study the extent to which there were issues with coordination among them. Significantly, "the only truth [Hoover] wanted to convey to the President was that internal security and counterespionage must be a civilian governmental responsibility concentrated in a single agency. The military must focus its attention on warfighting without distractions" (Batvinis, 2007, pp. 53–54). Hoover's plan concentrated all counterespionage investigations in the FBI and included the FBI takeover of the Federal Communications Commission, Immigration and Naturalization Services (then under the Department of Labor), and the Customs Services (then under the Department of the Treasury) (Batvinis, 2007, p. 54). In addition, Hoover also recommended that counterintelligence (CI) policy be taken away from the State Department and given to the FBI, ONI, and MID.

In November 1938, Roosevelt met with Hoover in secret and approved most elements of his plan. In June 1939, Roosevelt created the Interdepartmental Intelligence Conference (IIC), comprised of the FBI, ONI, and MID, which was a "huge blow to the prestige and historical authority of the [State Department]" (Batvinis, 2007, p. 67). The State Department could continue to collect information, but it needed to inform the IIC of its actions. The establishment of the IIC was a pivotal event in the history of CI in the United States. "For the first time in U.S. history, a new structure composed of specialized agencies with core competencies in such matters would focus on, direct, and coordinate all espionage, counterespionage, and sabotage investigations involving the federal government" (Batvinis, 2007, p. 68).

In response to the German invasion of Poland and the nonaggression pact between Germany and the Soviet Union in August 1939, Roosevelt declared a national emergency and issued a public statement that "the FBI [would] take charge of investigative work in matters relating to espionage, sabotage, and violations of neutrality regulations" (Church Committee Report, 1976, p. 404). Two days after issuing the statement, President Roosevelt declared a national emergency "in connection with and to the extent necessary for the proper observance, safeguarding, and enforcing of the neutrality of the United States and the strengthening of our national defense within the limits of peacetime authorizations" (Church Committee Report, 1976, p. 405). In conjunction with the declaration of national emergency, Roosevelt also directed the attorney general to increase the number of FBI personnel by 150 agents. In a press conference, Roosevelt said that the expansion of the government's investigative personnel was "to protect against 'some of the things that happened' before World War I":

> There was sabotage; there was a great deal of propaganda by both belligerents, and a good many definite plans laid in this country by foreign governments to try to sway American public opinion. . . . It is to guard against that, and against the spread by any foreign nation of propaganda in this country which would tend to be subversive of our form of government. (Church Committee Report, 1976, p. 405)

Congress accepted Roosevelt's actions as necessary in order to mitigate the repercussions of the tensions in Europe. In September 1939, Hoover argued before the House Appropriations Committee that the establishment of a GID "was made necessary by the President's proclamation directing that all complaints of violations of the national defense statutes and proclamations be report[ed] to the FBI" (Church Committee Report, 1976, p. 407). The new GID became the division responsible for supervising complaints of espionage, sabotage, and internal security matters.

The FBI's independence became further solidified when President Roosevelt signed a secret directive on June 26, 1939, that ordered that only the FBI, MID, and ONI "control and handle" investigations relating to "all espionage, counterespionage, and related matters," thereby circumventing the State Department (Theoharis, 2004, p. 48). To prevent potential conflict among the three agencies, delimitation agreements gave the FBI "exclusive responsibility to 'handle all cases involving allegations of espionage, sabotage, and related matters as pertained to persons in the United States" (Theoharis, 2004, p. 49; see also Batvinis, 2007, pp. 98–99). Thus, domestic intelligence functions became institutionalized within the FBI.

One of the main characteristics of the FBI domestic intelligence program authorized by President Roosevelt was its broad investigative scope:

> President Roosevelt never formally authorized the FBI or military intelligence to conduct domestic intelligence investigations of "subversive activities", except for his oral instruction in 1936 and 1938. His written directives were limited to investigations of espionage, sabotage, and violations of the neutrality regulations. Nevertheless, the President clearly knew of and approved informally the broad investigations of "subversive activities" carried out by the FBI. (Church Committee Report, 1976, p. 405)

The assumption that people or organizations in the United States posed a threat was not questioned, and Congress allowed the FBI wide latitude under Roosevelt's proclamation. "With no clear legislative or executive standards to keep it within the intended bounds, the FBI

(and military intelligence in its sphere) had almost complete discretion to decide how far domestic intelligence investigations would extend" (Church Committee Report, 1976, p. 411).

The Custodial Detention Index

In 1939, the FBI began developing a list of individuals "on whom information [was] available indicating strongly that [their] presence at liberty in this country in time of war or national emergency would constitute a menace to the public peace and safety of the United States Government" (Church Committee Report, 1976, p. 413). This program was described as a "custodial detention index," and its purpose was to "enable the government to make individual decisions as to the dangerousness of enemy aliens and citizens who might be arrested in the event of war" (Church Committee Report, 1976, p. 417). The groups targeted were the Socialist Workers Party, the Proletarian Party, Lovestoneites, "or any of the other Communist organizations, or . . . their numerous 'front organizations,' as well as persons reported as 'pronouncedly pro-Japanese" (Church Committee Report, 1976, p. 419).

The FBI's activities during this period mirrored concern in society about subversion and protecting national security, and some developments could have threatened the expansion of FBI powers. For instance, in 1938, the U.S. House of Representatives Committee on Un-American Activities (HCUA) was established, and in 1940, Rep. Martin Dies called for the creation of a Home Defense Council, which could have been a threat to the FBI's jurisdiction had it been implemented (Jeffreys-Jones, 2007, p. 104). In October 1941, the attorney general endorsed Hoover's request "that the FBI should be given the job of doing security checks on all federal employee[s]," a move apparently calculated to forestall any attempt by the HCUA to push for legislation that might move the function to somewhere in the executive branch other than the FBI (Jeffreys-Jones, 2007, p. 104).

The Red Scare

In the early 1940s, there was consensus that the country faced a threat from international communism, and the primary targets of FBI surveillance at this time were communists as well as members of the German

American Bund, Italian fascist organizations, and domestic far-right and extremist groups, such as the Ku Klux Klan and the Knights of the White Camelia. In response to these threats, the early 1940s ushered in the expansion of the FBI's intelligence activities and responsibilities. For instance, in May 1940, President Roosevelt moved the Immigration Bureau to the Department of Justice, making the attorney general responsible for all immigration matters, including the power to compile lists of aliens who could be detained or deported in times of war. In 1940, President Roosevelt authorized the FBI to conduct electronic surveillance of "persons suspected of subversive activities against the Government of the United States, including suspected spies" (Church Committee Report, 1976, pp. 422–423). In addition, in June 1940, President Roosevelt assigned foreign intelligence responsibilities in the Western Hemisphere to a Special Intelligence Service of the FBI (Church Committee Report, 1976, p. 424). This allowed the FBI to focus on intelligence activities in Latin America, a region that was suspected of being a target of Nazi infiltration that could spread to the United States. By 1945, "the FBI had emerged as the unacknowledged intelligence arm of the White House" (Theoharis, 2004, p. 64).

In addition to the expansion of FBI intelligence activities, several laws were passed to address these threats. For instance, in the early 1940s, Congress passed two statutes that addressed "subversive activities." The Smith Act of 1940 "made it a federal crime to urge military insubordination or advocate the violent overthrow of the government," and the Voorhis Act of 1941 "required the registration of all subversive organizations having foreign links and advocating the violent overthrow of the government" (Church Committee Report, 1976, p. 410).

In February 1941, the jurisdictions of the FBI, ONI, and MID were clarified. The FBI could conduct counterespionage investigations in all matters within the United States and U.S territories except for the Panama Canal Zone. The MID could initiate investigations at all continental military installations and the Panama Canal Zone, Panama, and the Philippine Islands. The ONI was responsible for all naval installations as well as Guam, American Samoa, Palmyra Atoll, Midway, and Johnson Island. "For the first time in the nation's history, a more structural rationality was applied to the investigation of

foreign intelligence attacks against U.S. interests both at home and [in] U.S. possessions" (Batvinis, 2007, p. 96). Most importantly, the Stone Line was eliminated, and the FBI was now authorized to move into CI activities that it had not been able to conduct since the Stone Line had been established.

FBI CI activities expanded greatly after 1941, but the success of those efforts is questionable. In 1943, the FBI began a national security investigation dubbed COMRAP (Comintern Apparatus) that targeted Soviet recruitment in the United States. FBI reports summarizing the results of the investigation indicated that FBI agents established only that "American Communists were Communists, not Soviet spies" (Theoharis, 2004, p. 63).

In 1943, the attorney general decided that the Custodial Detention Index was no longer useful and that it was based on faulty assumptions. The FBI director did not comply with the attorney general's order to abolish the list, however, and instead, the FBI changed the name from the Custodial Detention Index to the Security Index. Neither the attorney general nor the Justice Department was informed of the decision to maintain the list, and the FBI's orders to the field said,

> the fact that the Security Index and the Security Index Cards are prepared and maintained should be considered strictly confidential, and should at no time be mentioned or alluded to in investigative reports, or discussed with agencies or individuals outside the bureau other than duly qualified representatives from ONI and MID. (Church Committee Report, 1976, p. 421)

It was not until May 1945 that the War Department's MID acquired an organization to

> establish intelligence priorities and requirements, missions that finally allowed it to put into practice all components of the modern intelligence cycle: determining requirements, collecting the appropriate information, processing the acquired data into finished intelligence, and disseminating the results, a circular process that often generates a new set of requirements, initiating the cycle again. (Finnegan, 1998, p. 6)

During World War II, military and political leaders recognized that intelligence was crucial to military success. In response, the Army was forced to create a large intelligence structure, and the MID instituted formal training for intelligence personnel in a variety of disciplines (Finnegan, 1998, p. 6).

Post–World War II Domestic Intelligence

In 1946, Hoover informed Attorney General Ramsey Clark of the existence of the Security Index, and the Security Index program was officially reinstated. In 1947, President Harry Truman signed an executive order establishing the Employees Loyalty Program (EO 9835). The Security Index was viewed as a valuable tool to help identify people working in the executive branch of the U.S. government who were disloyal to the U.S. government or involved in subversive activities. During this time, the Armed Forces Security Agency also instituted a surveillance program called Project SHAMROCK, through which it intercepted international telegraphic messages transmitted through the United States (Theoharis, 1984, p. 67).

In 1946, the HCUA became a standing, permanent committee and investigated suspected communists in influential positions in the United States. In 1948, the committee brought charges of espionage against Alger Hiss of the State Department. Hiss was taken to trial and found guilty of perjury, reinforcing the general sentiment that "there were Communists among us."[4] During this period, the FBI worked closely with the HCUA. "[HCUA] members had established a[n] 'informal' relationship with the FBI, one that dated at least to May 1947—but on the strict condition that FBI officials' covert assistance not be known" (Theoharis, 2004, p. 77). In addition, the FBI worked closely with Senator Joseph McCarthy until Hoover severed its relationship with McCarthy in 1953. However, some view the FBI's contri-

[4] Releases of foreign intelligence information many years later, including the VENONA decryptions of Soviet communications, confirmed this, emphasizing the intersection between domestic and foreign intelligence activities in CI efforts in particular (discussed in Moynihan, 1998).

bution to McCarthyism as having significantly damaged the organization's reputation: According to Jeffreys-Jones (2007, p. 154), it "helped to drive millions of Americans into cringe mode. Its infractions of civil liberties, its reluctance to fight organized crime, and its obstruction of national security coordination—all these went unchecked at the height of the McCarthy era."

The 1947 National Security Act

Until 1947, foreign intelligence was conducted by the State Department and the military. The 1947 National Security Act (Pub. L. No. 235) created the Central Intelligence Agency (CIA), prohibiting it from performing "law enforcement or internal security functions," and a limitation of the authority of the Director of Central Intelligence (DCI) to inspect FBI intelligence (Church Committee Report, 1976, p. 458). While the director of the CIA would serve as DCI in charge of the entire intelligence effort, the CIA would be allowed to "operate only in the foreign sphere. The FBI had to give up foreign work, surrendering its Latin American assets in the process" (Jeffreys-Jones, 2007, p. 137). In the future, the FBI would work only on the domestic front. Ironically, while the establishment of the CIA was, in part, an effort to centralize authority, its result was to divide intelligence into two spheres: domestic and foreign.

The National Security Act also allowed the National Security Council to grant authority in 1949 to the FBI and military intelligence for counterespionage operations and the investigation of "subversive activities" (Church Committee Report, 1976, p. 458). This greatly increased the FBI's independence, and the line of authority for FBI and military domestic intelligence now bypassed the attorney general, instead flowing from the National Security Council to the IIC, composed of the FBI director and the heads of the military intelligence agencies.

The Continuation of the Security Index

In the 1950s, Congress provided tacit support to the FBI's domestic intelligence activities by passing several key pieces of legislation. The Emergency Detention Act of 1950 outlined specific standards for appre-

hending individuals in the event of an "internal security emergency." The basic criterion was whether there was "reasonable ground to believe that such person probably will engage in, or probably will conspire with others to engage in, acts of espionage and sabotage" (Church Committee Report, 1976, p. 442). Neither the FBI nor the Justice Department made changes in either the Security Index criteria or their detention plans to make them conform to the law. In fact, the attorney general "advised Hoover to disregard the law and proceed with the program as previously outlined" (Church Committee Report, 1976, p. 442). The Justice Department also advised the FBI that

> it did not have adequate personnel to review the placement of names on the Security Index and that in an emergency, all persons now or hereafter included by the [FBI] on the Security Index should be considered subjects for immediate apprehension, thus resolving any possible doubtful cases in favor of the Government in the interests of the national security. (Church Committee Report, 1976, p. 442)

By May 1951, the Security Index had grown to 15,390 names, 14,000 of whom were labeled as communists (Church Committee Report, 1976, p. 443). By the end of 1954, the number had increased to 26,174, of whom 11,033 were designated for priority apprehension (Church Committee Report, 1976, p. 446).

In 1954, Congress passed the Communist Control Act, which provided that the Communist Party was "not entitled to any of the rights, privileges and immunities attendant upon legal bodies created under the jurisdiction of the laws of the United States" (see Church Committee Report, 1976, pp. 427–428). In 1955, the FBI decided to voluntarily revise the Security Index criteria because all cases were not being reviewed by Justice Department attorneys, and the FBI wanted to "minimize the inevitable criticism of the dual role" it had in both investigating and making judgments on "the soundness of these cases" (Church Committee Report, 1976, p. 446). The FBI created a new Subversives Control Section to supervise the Security Index, and as a result of the revisions to the Security Index standards, the Security Index was reduced to 12,870 names by mid-1958 (Church Committee

Report, 1976, p. 446). However, the Security Index cards on individuals taken off the index after 1955 were retained in field offices. These cards would be destroyed only if the subject agreed to become an FBI source or informant or "otherwise indicate[d] complete defection from subversive groups." Consequently, the canceled cards served as a supplementary detention list, despite the tighter standards for the Security Index (Church Committee Report, 1976, p. 446). In 1956, the canceled cards were the bases for a Communist Index.[5] There is no indication "that the Justice Department was ever advised of the existence of the Communist Index" (Church Committee Report, 1976, p. 447). In mid-1959, the Communist Index was reviewed and reduced from 17,783 names to 12,784 names, and by mid-1959, the Security Index included 11,982 names (Church Committee Report, 1976, p. 447). Throughout the 1950s, the supervision of the collection of information for the Security Index was a major responsibility of the FBI's Intelligence Division.

The Broadening of Domestic Surveillance Activities

The public's concern about the communist threat in the 1940s and 1950s reinforced the FBI's focus on infiltrating communist organizations. During this time, the FBI's power and independence grew. For instance, the FBI's first counterintelligence program (COINTELPRO) began during this time. These programs were secret and employed questionable tactics (see Churchill and Vander Wall, 2002). These programs first focused on investigating communist organizations and individuals and later expanded to hate groups and nationalists.

At the same time as these programs were instituted at the FBI, other agencies were also broadening their domestic surveillance activities. For instance, beginning in the late 1950s, the CIA began one of the largest domestic surveillance programs in the history of the United States: Operation CHAOS. CHAOS was the centerpiece of a major CIA effort begun in 1967 in response to White House pressure for intelligence about foreign influence on American dissent. The CHAOS mission was to gather and evaluate all available information about foreign

[5] The Communist Index was renamed the Reserve Index in 1960.

links to racial, antiwar, and other protest activity in the United States. A second major element of Operation CHAOS was to pursue specific inquiries from the FBI about the activity of particular Americans traveling abroad. In the process, the CHAOS project amassed thousands of files on Americans, indexed hundreds of thousands of Americans into its computer records, and disseminated thousands of reports about Americans to the FBI and other government offices. Some of the information concerned the domestic activity of those Americans (Church Committee Report, 1976, pp. 681–682). In 1967, the radical magazine *Ramparts* exposed that the CIA was secretly funding the National Student Association, the largest student group in the United States. At the same time, the National Security Agency (NSA) instituted a major surveillance effort, Operation MINARET, which, beginning in 1967, intercepted international communications of targeted dissidents and activists (Theoharis, 1984, p. 67).

The FBI's broadest program for collecting intelligence was known as COMINFIL (Communist Infiltration) and was begun in 1956. Despite the decline of the Communist Party in the 1950s and 1960s, the FBI and the Justice Department argued that COMINFIL investigations should continue because they believed that the Communist Party would try to "repair its losses" (Church Committee Report, 1976, p. 451). By 1960, the FBI had opened about 432,000 headquarters files on individuals and groups in the "subversive intelligence field," and between 1960 and 1963, an additional 9,000 files were opened (Church Committee Report, 1976, p. 451).

In the 1960s, the United States faced a new set of internal security issues, including civil rights demonstrations, the emergence of radical hate groups, and urban unrest. These were essentially law enforcement issues that required improved police-community relations and careful planning to ensure peaceful demonstrations. However, the FBI continued to view them within a domestic intelligence framework that emphasized communist "influence" (Church Committee Report, 1976, p. 470). For instance, in 1965, the FBI expanded its investigations to include the Ku Klux Klan as well as "black nationalist groups" (Church Committee Report, 1976, p. 475). In addition, through its COMINFIL program, the FBI intensified its investigations of individ-

uals and organizations involved in the civil rights movement as well as the antiwar movement and student groups. The FBI continued to cast a wider and wider net in its domestic surveillance activities.

COINTELPRO Efforts

In 1961, Hoover decided to institute a COINTELPRO–Socialist Workers Party. This program targeted members of the Socialist Workers Party who were in positions that could influence American society. This program was more focused than the COMINFIL program.

In 1964, the FBI instituted COINTELPRO–White Hate in response to the Justice Department's concerns about the spread of Ku Klux Klan activity and violence in the South. The program targeted racist organizations, such as the American Nazi Party, the White Knights of Mississippi, and the National States' Rights Party, and helped weaken the Klan's power, as evidenced by its decline in membership from 14,000 in 1964 to 4,300 in 1971 (Jeffreys-Jones, 2007, p. 172). In 1971, the criteria for investigating individuals were widened still further to include not only persons with "a potential for violence," but also anyone else who, in judgment of the special agents in charge, should be subject to investigation due to extremist activities. By 1971, the FBI program for investigating the Klan and hate groups delegated virtually unlimited discretion to the field and specifically required FBI agents to report on lawful political speeches (Church Committee Report, 1976, p. 474).

The FBI had been monitoring African American leaders in the early 1960s, most notably Dr. Martin Luther King Jr., but FBI intelligence programs that dealt with "black extremists" and civil disorders were greatly affected by the events of 1964. During the first urban ghetto riots in the summer of 1964, President Lyndon Johnson instructed the FBI to investigate their origins and extent (Church Committee Report, 1976, p. 475). In its report, the FBI noted the growth of black militancy, claimed that "a number of violent agitators had arisen," and, without mentioning his name, described the activities of Malcolm X as an example of a leader urging African Americans "to abandon the doctrine of non-violence" (Church Committee Report, 1976, p. 475). The report also highlighted the role of "a Marxist-Leninist group following

the more violent Chinese Communist line and other individuals 'with histories of communist affiliation' in alleged attempts to instigate riot activities" (Church Committee Report, 1976, p. 475), indicating that the FBI was continuing to operate within its traditional framework that emphasized the communist threat. In June 1964, the FBI established a special desk in the Domestic Intelligence Division to supervise an "intensification of the investigation of communist influence in racial matters" (Church Committee Report, 1976, p. 479). In 1965, the FBI's General Racial Matters program was expanded to include intelligence on demonstrations, racial violence, and riots. In 1967, COINTELPRO–Black Nationalist Hate was initiated to "expose, disrupt, misdirect, or otherwise neutralize the activities of black nationalists, hate-type organizations and groupings, their leadership, spokesmen, membership, and supporters, and to counter their propensity for violence and civil disorder" (Theoharis, 2004, pp. 121–122).

In 1967, Hoover instructed "that an index be compiled of racial agitators and individuals who have demonstrated a propensity for fomenting racial discord." The standards for this index, known as the Rabble Rouser Index,[6] were soon expanded to cover persons "with a propensity for fomenting" any disorder affecting the "internal security," not just those related to radical politics (Church Committee Report, 1976, p. 511). This expansion of the index was an attempt to develop a nationwide list of "agitators of all types that had a bearing on national security" (Church Committee Report, 1976, p. 511).

In 1968, the FBI instituted COINTELPRO–New Left in response to the growth of radical groups on college campuses and student opposition to the Vietnam War. The FBI tried to disrupt these types of groups and prevent them from disseminating their messages.

At the same time as these COINTELPRO efforts were moving ahead, an FBI intelligence program targeting Cuba's President Fidel Castro and his sympathizers began in November 1960, when field officers were instructed to consider "recommending for the Security Index those individuals who are not on the Security Index but who . . . would be deemed dangerous or potentially dangerous to the internal security

[6] In 1968, the Rabble Rouser Index was renamed the Agitator Index.

of the U.S. in the event of an emergency involving Cuba and the U.S." (Church Committee Report, 1976, p. 467). In response to the Cuban missile crisis in 1962, the FBI intensified its program for placing pro-Cubans on the Security Index and established a special Cuban section of the index (Church Committee Report, 1976, p. 467).

Growing Concern About the FBI's Domestic Intelligence Activities

The 1970s marked a turning point in the history of domestic intelligence in the United States. In 1970, President Richard Nixon appointed a secret interagency task force, directed by White House aide Tom Charles Huston, to review and evaluate intelligence-collection methods, outline how the activities of the intelligence agencies could be better coordinated, and recommend any needed changes. The task force recommended that the President authorize a series of "clearly illegal" investigative techniques, including "the increased use of wiretaps and bugs, authorizing the interception of telegraph and other communications transmitted internationally, and lowering the minimum age of informers to eighteen" (Theoharis, 2004, p. 129). This so-called Huston Plan was later recalled, but the FBI lowered the minimum age of informers in order to aid with surveillance of college students.

In February 1971, the U.S. Senate Committee on the Judiciary Subcommittee on Constitutional Rights began a series of hearings on federal data banks and the Bill of Rights, which marked a pivotal point in domestic intelligence policy. This subcommittee reflected "the growing concern among Americans for the protection of the privacy of the individual against 'the information power' of government" (Church Committee Report, 1976, p. 548). The ranking minority member of the subcommittee, Senator Roman Hruska (R-NE), endorsed the need for a "penetrating and searching" inquiry (Church Committee Report, 1976, p. 548).

In 1971, the FBI also faced the first serious congressional action that might curtail its domestic intelligence operations when Congress repealed the 1950 Emergency Detention Act. The repeal of this act also

technically repealed the Security Index. However, the attorney general advised that the repeal

> [d]oes not alter or limit the FBI's authority and responsibility to record, file and index information secured pursuant to its statutory and Presidential authority. An FBI administrative index compiled and maintained to assist the Bureau in making readily retrievable and available the results of its investigations into subversive activities and related matters is not prohibited by repeal of the Emergency Detention Act. (Church Committee Report, 1976, p. 545)

The Security Index was immediately reconstituted as the Administrative Index with revised standards.

The Church Committee

In December 1974, just on the heels of the Watergate scandal, *The New York Times* accused the CIA of domestic spying (Colby, 1976), and a firestorm of public outrage erupted. Congress became increasingly concerned about domestic intelligence activities. The article focused on Operation CHAOS, which illegally monitored the activities of thousands of antiwar and civil rights activists (Theoharis, 2004, p. 137). Attempting to address growing public distrust of the intelligence agencies, President Gerald Ford appointed a special commission in 1975, its members selected by Vice President Nelson Rockefeller, to investigate only CIA domestic abuses (Theoharis, 2004, p. 138).

In response to the climate of reform that developed in the wake of Watergate, both the Senate and House established special committees to investigate the domestic and foreign activities of the intelligence agencies. The Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (known as the Church Committee after its chair, Frank Church) conducted a thorough investigation of the activities of the intelligence agencies and issued 14 reports. The reports revealed widespread abuses of power, not just in the CIA, but also in the FBI and military intelligence agencies. For instance, they documented

> [t]he FBI's extensive use of illegal investigative techniques and the questionable authority under which many FBI programs operated. They discovered that the presidents and their attorneys general in some cases had no knowledge of the scope and purpose of highly questionable FBI activities and in others sought to avoid meeting their oversight responsibilities. They also discovered that FBI investigations were not confined to criminals or suspected spies but also targeted individuals and organizations engaged in legitimate political activities. (Theoharis, 2004, p. 139)

These reports included 96 suggested reforms to domestic intelligence. Some of these reforms were implemented, and others were not. The Church Committee reports marked the end of the FBI's rapidly growing strength and reach in domestic intelligence. In fact, public-opinion polls taken in 1975 found that only 37 percent of respondents held a "highly favorable" rating of the FBI, a drop from an 85-percent rating in 1966 and a 71-percent rating in 1970 (Theoharis, 2004, p. 139).

Adding to this perception, in February 1976, the U.S. General Accounting Office (GAO) released a report on the efficiency and effectiveness of the FBI. The report charged that "86 percent of 300 'soft cases' that it had reviewed (cases based on 'soft' evidence, such as the way a person looked), no connection at all was made with extremist groups, yet the data collected were not only retained but passed on to third parties" (Jeffreys-Jones, 2007, p. 188). By middle of the 1970s, the FBI "was a demoralized agency that had lost the confidence of the American people" (Jeffreys-Jones, 2007, p. 190).

The Wall

The era of FBI reform continued into the late 1970s. President Jimmy Carter had campaigned on the need to reform the FBI and, in 1978, signed an executive order that prevented the FBI from engaging in the prevention of "subversion" (EO 12036; Jeffreys-Jones, 2007, p. 203). That same year, Congress passed the Foreign Intelligence Surveillance Act (FISA), which established a special court that would review government requests for electronic surveillance of U.S. citizens and resident aliens. FISA provided special procedures for conducting electronic surveillance for foreign intelligence purposes and provided a frame-

work for the surveillance of U.S. citizens and others whom the court determined to be potential agents of a foreign power. After 9/11, FISA would later be at the center of a controversy surrounding warrantless wiretapping by the NSA.

In 1980, a pivotal court case (*United States v. Truong Dinh Hung*, 629 F. 2d 908, 4th Cir., 1980) found that the government did not need to obtain a warrant when "the object of the search or the surveillance is a foreign power, its agents or collaborators" and "the surveillance is conducted 'primarily' for foreign intelligence purposes" (DOJ OIG, 2006a, p. 23). However, "the government's primary purpose in conducting an intelligence investigation could be called into question when prosecutors had to assemble a prosecution or had led or taken a central role in a prosecution" (DOJ OIG, 2006a, p. 23). As a result, "the wall" was built between intelligence investigations and criminal investigations: "The wall began as a separation of intelligence investigators from contact with criminal prosecutors, and evolved to include a separation of FBI investigators working on intelligence investigations from investigators working on criminal investigations" (DOJ OIG, 2006a, p. 21). While things could be "passed over the wall" under certain circumstances, this ruling greatly limited the ability to share information across intelligence and criminal investigations.

Successes and Setbacks in the 1980s and 1990s

In the 1980s and 1990s, the FBI targeted organized crime and was able to successfully prosecute many organized-crime bosses. In 1984, the FBI exposed a heroin ring that distributed its goods nationwide in pizza parlors (Jeffreys-Jones, 2007, p. 211). Several high-ranking crime bosses were convicted, including a former Sicilian mafia leader. In 1987, Philadelphia mafia boss Philip Leonetti was arrested, and with help from his testimony, in 1992, John Gotti was convicted. Following an FBI–Drug Enforcement Administration (DEA) inquiry and a U.S. invasion of Panama, General Manual Noriega was put on trial in 1988 in the United States for drug and money-laundering offenses (Jeffreys-Jones, 2007, p. 212).

In 1986, the FBI's powers were increased when Congress authorized it to investigate terrorist attacks against Americans outside

the United States: "The strengths that the FBI brought to CT were nowhere more brilliantly on display than in the case of Pan American Flight 103, which blew up over Lockerbie, Scotland in 1988, killing 270 people" (9/11 Commission Report, 2004, p. 175). The FBI, CIA, and British intelligence agencies worked together on a long investigation into the Pan Am bombing. They built a case against the Libyan government, and eventually, Libya acknowledged responsibility. The investigation into the Flight 103 bombing was the first of a series of overseas terrorism investigations in which the FBI would be involved. The complexity and length of the case allowed the FBI to demonstrate that it could successfully collaborate with other domestic and foreign intelligence agencies on major terrorism investigations.

In addition to these successes, the FBI also experienced some setbacks in the 1990s and early 21st century. In particular, three events raised questions among some in the public as to whether some of the FBI's tactics were overly aggressive:

- the 1992 shooting of a right-wing survivalist's wife, who was carrying her baby at the time, at Ruby Ridge
- the catastrophic 1993 fire that broke out during a siege at the Branch Davidian headquarters in Waco, Texas
- the investigation into the 1996 Atlanta Centennial Olympic Park bombing that resulted in a large defamation-of-character lawsuit because Richard Jewell was publicly named as a suspect in the bombing and later cleared without charges.

Damage to the FBI's reputation also resulted from the discovery of spies within the organization itself: When FBI surveillance caught Robert Hanssen and arrested him for espionage in 2001, Hanssen's response was, "What took you so long?" (Jeffreys-Jones, 2007, p. 226). In addition, the 1994 prosecution of CIA officer Aldrich Ames renewed concerns about the role of prosecutors in intelligence investigations. The U.S. Department of Justice Office of Intelligence Policy and Review (OIPR) worried that Ames might escape conviction because the judge might rule that the FISA warrants had been misused due to numerous prior consultations between FBI agents and prosecutors. As a result,

the OIPR became the gatekeeper for the flow of FISA information to criminal prosecutors (9/11 Commission Report, 2004, p. 78).

In response to the incidents at Ruby Ridge and Waco, Timothy McVeigh carried out the second-worst peacetime terrorist attack on U.S. soil, second only to the 9/11 attacks. McVeigh was a former militia member who believed that the federal government was abusing its powers, and in 1995, he used fuel oil and fertilizers to blow up the Alfred P. Murrah Federal Building in Oklahoma City, killing 168 people. The FBI led the successful investigation into the bombing; McVeigh was convicted in 1997 and executed in 2001.

Terrorism and a Renewed Call for Expanded Domestic Intelligence Activities

Though the collapse of the Soviet Union in 1991 "undercut the anxieties that had lent unquestionable support to foreign intelligence/counterintelligence," a new threat to internal security came to the fore in the 1990s: terrorism (Theoharis, 2004, p. 149). In 1993, a bomb exploded underneath the World Trade Center, killing six people. This internal threat affected both domestic law enforcement activities and shaped a broader environment for domestic intelligence. As the 9/11 Commission Report would highlight a decade later, "the FBI and Justice Department did excellent work investigating the [1993 World Trade Center] bombing" (9/11 Commission Report, 2004, p. 72). Within a week of the 1993 bombing, the FBI had arrested the person who rented the truck that carried the bomb, and later, several conspirators were convicted. A consequence of this successful investigation was that "it created an impression that the law-enforcement system was well equipped to cope with terrorism" (9/11 Commission Report, 2004, p. 72).

With its new power to exercise federal jurisdiction overseas when a U.S. national is murdered, assaulted, or taken hostage by a terrorist or when certain U.S. interests are attacked, the FBI's investigative expertise was increasingly called on overseas as well. For instance, the FBI assisted in the long investigation into the 1996 attack on the Khobar

Towers in Saudi Arabia that killed 19 Americans. After an intense investigation, 19 people were indicted in 2001. However, it has not been decided whether Iran or al Qaeda was ultimately responsible. In 2000, a small boat approached the USS *Cole* while the *Cole* was harbored in Aden, Yemen. It detonated a bomb that put a large gash in the side of the *Cole* and killed 17 U.S. sailors. The FBI played a major role in the long investigation and ultimately determined that al Qaeda was responsible for the bombing.

The events of September 11, 2001, marked the next major turning point in the history of domestic intelligence and have driven the current debate on whether to form a separate domestic intelligence agency. As in the past, questions have been raised about the effect of domestic security activities on the nation: For example, in the words of Jeffreys-Jones (2007, p. 233), one of the "the immediate response[s] to 9/11 by the Administration and Congress—strengthening the FBI's powers—was imposed at a cost to civil liberties. To defend liberty, the argument ran, America had to curtail it." As in the past, the premise for the expansion of federal surveillance powers was that the FBI was denied the powers that could have allowed it to prevent the 9/11 attacks (Theoharis, 2004, p. 158). In October 2001, President George W. Bush signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act. The PATRIOT Act reversed some of the reforms of the 1970s, including the removal or reduction of some of the safeguards in the 1978 FISA law. In addition to traditional wiretapping, Internet activity, email, and voice mail could now be monitored with reduced court oversight (Jeffreys-Jones, 2007, p. 233). In July 2008, President Bush signed the FISA Amendments Act of 2008 into law. The act makes further amendments to FISA by granting immunity to telecommunication companies that cooperate with federal law enforcement agencies by providing personal records of suspected individuals, and it allows the government to conduct warrantless surveillance for up to a week instead of the previously allowed 48 hours.

Like many previous episodes that triggered the expansion or contraction of domestic intelligence, the 9/11 attacks were the catalyst for major intelligence reform. Attorney General John Ashcroft reorganized

FBI operations, and new surveillance guidelines were issued. Most importantly, though, Ashcroft and FBI Director Robert Mueller III explicitly stated that they would create a new culture in the FBI that would shift from law enforcement to terrorism prevention (Theoharis, 2004, p. 159).

Conclusions

Looking back at the history of the country, the questions that are being asked now—including the question of whether the country needs a new domestic intelligence agency—have precedents in situations and crises that have come before. The view that many things changed after 9/11 has been central in a variety of policy discussions that have been carried out in the years since the attacks. However, the issues confronting the country today are similar to those confronted by previous presidents, Congresses, and courts: How should the intelligence community (IC) be organized to minimize overlap in some areas and gaps in others? How can sharing information across the IC and law enforcement be fostered? How does the country balance civil liberties with security? And how can the activities of organizations that rely on secrecy to preserve the effectiveness of their operations be meaningfully overseen and regulated?

Many of the broad themes outlined in Chapter One have repeatedly resurfaced throughout the history of domestic intelligence in the United States.

Difficulty in Identifying a Small Number of Threatening Individuals in the General Population of a Large and Diverse Nation

While the types of individuals deemed threatening to the United States have changed throughout its history (e.g., foreign spies, saboteurs, anarchists, communists, terrorists), the nation has always been concerned about maintaining its ability to identify those individuals who pose threats. Because these threatening individuals have represented a small fraction of the population, the country has continually struggled with how to balance national security with the civil liberties of

those who are not threats. This tension has become particularly evident during times of war. Whether it was during the Revolutionary War, the Civil War, the Spanish-American War, World War I, World War II, the Cold War, or the war on terror, the country's heightened focus on security often led to actions that attempted to find all possible threats but, in doing so, jeopardized civil liberties.

The Alien and Sedition Acts were some of the earliest and most far-reaching attempts to crack down on political opposition and dissidents. The public's vehement opposition to the Alien and Sedition Acts was an early signal to the country's leaders that the American public took its civil liberties protection seriously. Throughout the history of the United States, the public would continue to be a watchdog and has opposed government actions that could infringe on those civil liberties.

With the development of the Custodial Detention Index in 1939, the U.S. government began to cast a much wider net in order to identify potential threats to the United States. This movement continued with the establishment of the HCUA in 1940 and the 1947 National Security Act, which expanded the FBI's domestic surveillance activities.

During the 1950s, 1960s, and early 1970s, the U.S. government cast its widest net ever in an attempt to find communists. This net began with the establishment of the Security Index, and continued with the CI, COMINFIL, COINTELPRO, CHAOS, and MINARET programs. The wide net cast by the FBI, CIA, and NSA caught up thousands of innocent Americans. It was not until the Church Committee report was released in the 1970s that such wide-reaching surveillance efforts were deemed as overreaching their bounds.

Concern About the Effect of Intelligence Activities on Personal Privacy and Civil Liberties

On a related note, concern has increasingly grown about the effect of intelligence activities on personal privacy and civil liberties. This concern became particularly acute when the government began actively keeping lists of people who were potential threats (e.g., the Custodial Detention Index and the Security Index) and began to actively infiltrate organizations in order to identify potential threats (e.g., the CIA's

Operation CHAOS amassed information on antiwar protesters during the 1960s).

While the American public was shocked to learn through the Church Committee report of the extensive domestic surveillance efforts during the 1960s, the public has been equally shocked to learn of some of the domestic surveillance efforts that have taken place since 9/11. These domestic surveillance efforts included the warrantless wiretapping of international phone calls of individuals who were deemed threats, the establishment of a no-fly list, and the Defense Advanced Research Projects Agency's (DARPA's) establishment of the Total Information Awareness (TIA) program, which was later renamed Terrorism Information Awareness in response to the public outcry over the initial program name—and then subsequently dissolved.

The concern about the intrusion of intelligence activities on personal privacy has become particularly intense as technology and surveillance capabilities have become more sophisticated. In particular, civil liberties advocates have become increasingly concerned about the vulnerability of privacy as personal information is increasingly stored on computer systems, and surveillance techniques (e.g., more-sophisticated wiretapping and eavesdropping devices) allow for increased information gathering. As technology continues to advance, these concerns will only become more prevalent and complicated.

Interagency Cooperation Problems and Differences in Organizational Cultures

Since its inception, the United States has struggled with the organizational structure of its domestic surveillance activities. Initially, the military, the Secret Service, and the State Department were responsible for surveillance responsibilities. However, before World War I, the military's surveillance capabilities had decreased, and domestic security investigations rested primarily with the State Department, with a smaller role played by the Secret Service and the newly formed BoI within the Justice Department.

In an attempt to organize the nation's disparate intelligence activities, in November 1938, President Roosevelt created the IIC, comprised of the FBI, ONI, and MID. The exclusion of the State Department was

seen as an affront to its historical prestige and authority. As time went on, the FBI was given more independence and authority, and it became the de facto primary civilian domestic intelligence agency.

As time has passed, the cast of agencies involved in domestic intelligence activities has grown, and therefore, coordination among these agencies has grown increasingly complicated. The events of 9/11 highlighted interagency-coordination problems, and once again, calls for reorganization arose. The establishment of the Department of Homeland Security promises to further complicate both the delineation of responsibilities and coordination across agencies.

The coordination of domestic intelligence activities is particularly complex because such activities overlap with the responsibilities of so many agencies. The military and CIA have gradually been restricted to foreign intelligence activities, while the FBI has taken on the primary role in domestic intelligence activities. However, there must be coordination and information exchange among these agencies because threats have become increasingly transnational in nature.

In addition to these historical interagency-coordination problems, the events of 9/11 also led to increasing calls to separate law enforcement and intelligence activities. Since the late 1950s, the FBI increasingly took on surveillance activities until the Church Committee reforms in the 1970s put additional oversight and accountability mechanisms in place. With the events of 9/11, the FBI has once again been asked to take on increased surveillance responsibilities, and some have questioned whether law enforcement and intelligence activities can be conflated in a single organization because of the risk that such activities will come into conflict with one another.

Thus, domestic surveillance efforts in the United States have historically been extremely complex because they require coordination across various government agencies, coordination across international and domestic activities, and melding of various organizational cultures. The nation has always struggled with the delineation of responsibilities across agencies and how to streamline the domestic intelligence enterprise. The calls for reorganization since the 9/11 attacks are merely the latest episode in a cyclical reevaluation of the organizational structure of the country's domestic surveillance activities.

CHAPTER THREE

Current Domestic Intelligence Efforts in the United States

Brian A. Jackson, Darcy Noricks, and Benjamin W. Goldsmith

In considering the creation of a new domestic counterterrorism (CT) intelligence agency, the United States is not starting with a blank slate. Both before and since September 11, 2001, a variety of organizations have had roles touching on CT, meaning that there are already many individual organizations with responsibilities that could be considered domestic intelligence.[1] Furthermore, a variety of other security and related missions involve domestic intelligence activities. Efforts to control illegal drug smuggling into the country have long had associated intelligence efforts; law enforcement activities focused on controlling money-laundering involve significant financial intelligence infrastructures; and the transition to what has come to be known as intelligence-led policing has meant that even "traditional" law enforcement activities have intelligence elements. Since 9/11, some of these investigative and intelligence activities previously focused on other issues have also been applied to CT.

Current U.S. domestic intelligence efforts therefore cannot be assessed by looking at one organization or even just the efforts made at one level of government. Even the subset of intelligence efforts focused on preventing terrorism is a set of activities that emerged from the

[1] Our broad framing of the U.S. domestic intelligence enterprise resembles the framing of the "homeland security intelligence community" described in Masse (2006, pp. 21–23). The *DHS Intelligence Enterprise Strategic Plan* (DHS, 2006a) uses the somewhat more general description of the Homeland Security Stakeholder Community, of which the Homeland Security Intelligence Community is the subset that possess intelligence elements.

actions of multiple actors, rather than being specifically designed for this particular mission. Because all the elements of this system play important roles in today's effort to address the terrorist threat domestically, the potential benefits of founding a new agency cannot be considered in isolation, but instead must be compared with the organizations and their intelligence activities that are currently in place—to which we refer as the *national domestic intelligence enterprise*.

One part of RAND's research effort therefore focused on identifying those activities that were currently ongoing to understand both the variety of current activities and how they could shape the context in which a new domestic intelligence agency might be created.

Mapping the U.S. Domestic Intelligence Enterprise

To inventory and map current domestic intelligence efforts, an open-source review was undertaken to identify all relevant activities that involve collecting, analyzing, and sharing information about individuals and organizations in the United States. While the focus of the overall RAND study was on domestic CT intelligence, it was our view that mapping the full range of domestic intelligence efforts is important for understanding the institutional context for any new potential intelligence agency; as a result, the team did not limit its search to activities focused only on the CT policy area.

Beyond a desire to understand ongoing domestic intelligence activities as comprehensively as possible, there were broader reasons for being inclusive in our search: Past successes in intelligence activities in counternarcotics in particular (e.g., in multiagency coordination and joint activities among intelligence, defense, and civilian agencies) have provided important templates for some current efforts to design CT intelligence. More importantly, given the focus on the CT mission across the government, some of these ongoing efforts have added CT to their mission portfolios, strengthening the trend toward proliferation of domestic CT intelligence activities.

Sources of information for this review included interviews with intelligence and law enforcement agencies involved in domestic intel-

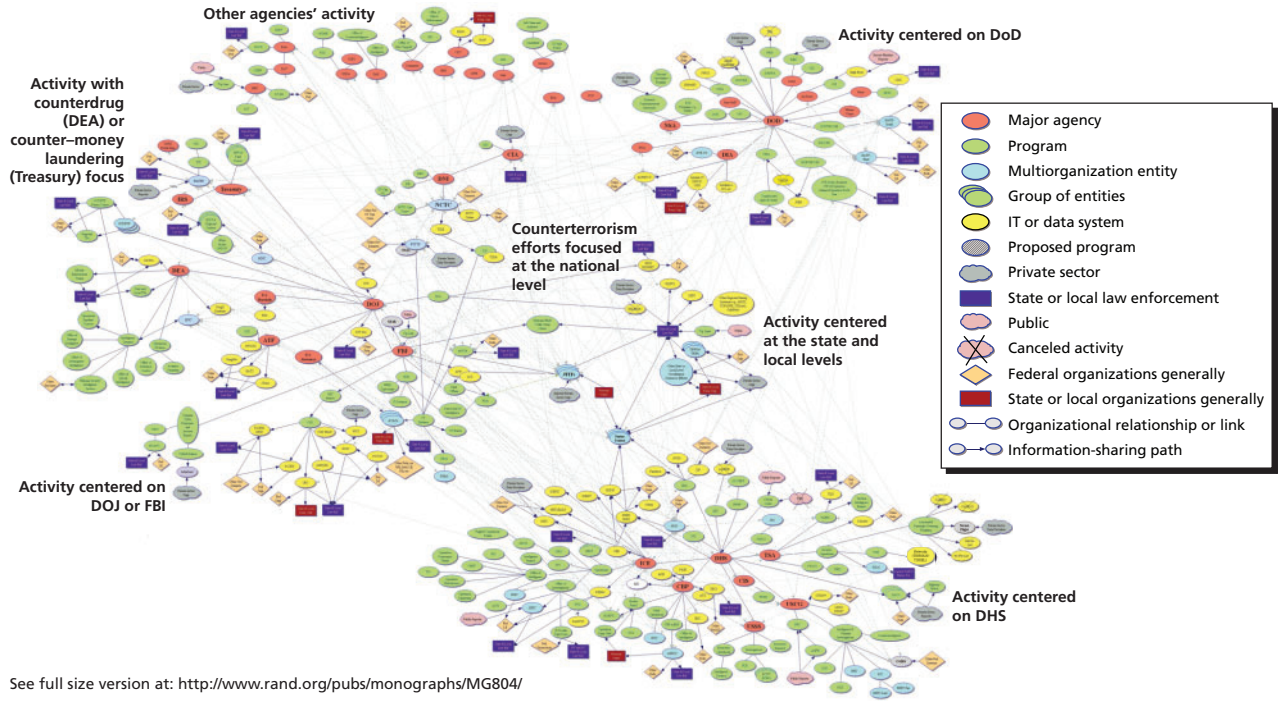
ligence; published, programmatic descriptions of these organizations; analyses of government activities by internal executive branch offices (e.g., inspectors general), legislative branch organizations (e.g., the U.S. Government Accountability Office, Congressional Budget Office), nongovernmental organizations, and press reporting. The goal of the effort was to catalog, as comprehensively as possible, programs, initiatives, and activities and the cooperative or information-sharing linkages that existed among them to map the topography of the current domestic intelligence enterprise. From the varied sources, the following information was extracted and cataloged:

- the identity of entities, whether organizations, programs, multiagency task forces or groups, information systems, or classes of actors (e.g., state and local law enforcement and even the general public) involved in activities that could reasonably be described as domestic intelligence based on the definition adopted in our study (see Chapter One)
- descriptive information on the missions, goals, and activities of those entities
- data on other organizations or groups connected to each entity through the sharing of information, connectivity through joint information systems, collaboration or joint membership, or authority relationships.

All the data that could be gathered on current domestic intelligence and intelligence-related activities are summarized in a single map included in miniature in Figure 3.1.[2] The goal in crafting a map of domestic intelligence was to provide a visual representation of current domestic intelligence activities, both to help understand initiatives that are now in place and to assess the institutional context that a new domestic intelligence agency would face. Details on interpreting the figure are in Text Box 3.1.

[2] The size of the U.S. domestic intelligence enterprise makes the resulting map of it ill-suited for presentation in a book format. Readers are encouraged to view the larger version of this figure available at http://www.rand.org/pubs/monographs/MG804/.

Figure 3.1
The U.S. Domestic Intelligence Enterprise



See full size version at: http://www.rand.org/pubs/monographs/MG804/

NOTE: DEA = Drug Enforcement Administration. Treasury = U.S. Department of the Treasury. DOJ = U.S. Department of Justice. FBI = Federal Bureau of Investigation. DHS = U.S. Department of Homeland Security. DoD = U.S. Department of Defense. IC = intelligence community.

RAND *MG804-3.1*

Text Box 3.1
Reading the Map (Figure 3.1)

Indicator	Description
Color-coded entities on the map: The colors of the map elements convey information about the nature of the entity.	
Light-red oval	Major agency (DHS, DOJ, FBI) or its component
Green oval or circle	Component office or program-level organization or activity within a larger organization
Blue oval or circle	Unit, office, center, or task force specifically created to be a multiagency, highly linked node within the domestic intelligence network (e.g., fusion center, Joint Terrorism Task Force [JTTF], National Counterterrorism Center [NCTC])
Yellow oval or circle	Database or information system, generally included only when accessible to multiple organizations—i.e., an agency's internal information system is not included even if it might be used for domestic intelligence–related activities.
The map also includes a set of more-generic entities that show connections among broad categories of organizations or to identify entities categorically if specific data on them could not be found in the open literature.	
Purple rectangle	State or local law enforcement
Dark-red rectangle	State or local response organization or National Guard—i.e., an entity other than law enforcement that may have CT, counterdrug, or counter–money-laundering responsibilities or missions
Beige diamond	Other federal organization or system
Gray irregular shape	Private-sector organization
Pink irregular shape	The public

Text Box 3.1—Continued

Linkages: On the map, two types of linkages are pictured: (1) organizational relationships (lines with no arrows) and (2) information-sharing relationships (arrows show the general direction of information flow, whether unidirectional or bidirectional). Because of the number of links among organizations active in this area, some links are shown as light-gray dotted lines, particularly those tying many individual organizations and activities to multiagency organizations or nodes in the network. These links are not intended to be different from the others shown but were lightened to make the overall figure easier to interpret.

In constructing the map, we also struck a compromise between the desire to show all links among all organizations and increasing the map's overall complexity. As a result, in some cases, systems or organizations are shown linked to generic identifiers (e.g., federal law enforcement organization or state or local law enforcement). We also use these generic identifiers in multiple places on the map (e.g., boxes representing state and local law enforcement organizations appear at many sites on the map) because this repetition produced a simpler and more user-friendly result than drawing a large number of long linking lines to one spot in the diagram.

Crossed-out or gray entities: Entities that are crossed out indicate programs or initiatives that have been canceled. They are included to provide some context for terminated domestic intelligence programs. Entities shown with gray, hatched backgrounds are planned programs that are not yet operational, based on the knowledge available to the research team.

Stacks of entities: A stack of three objects designates a situation in which multiple versions of the same organization exist across the country that, although guided by similar rationales and guidelines, may differ in the organizations that participate, the way they are structured, and the activities they undertake. Prominent examples of such heterogeneous elements within the domestic intelligence enterprise include fusion centers, JTTFs, terrorism early warning groups (TEWs), information-sharing and analysis centers (ISACs), and antiterrorism advisory councils, as well as a number of regional task force structures for counterdrug and counter–money-laundering missions.

In examining the results of this effort, the reader should bear in mind both the purpose that guided the analysis and the nature of the information sources on which it was based. First, since this review drew only on open-source data, the assessment was limited to those programs and initiatives whose activities have been publicly disclosed. The picture we assembled is also a mosaic of descriptive, relational, and programmatic information from a wide range of sources that almost certainly differed in their inclusiveness and comprehensiveness. Though we made multiple efforts to assess the completeness and currency of sources, such an effort can never fully guarantee consistency. This work also represents a snapshot in time. The dynamic nature of CT and intelligence efforts during this period makes any effort at comprehensive mapping perilous. While our study was ongoing, some programs changed significantly or were discontinued. In spite of these caveats and limitations, for the purposes for which it was created—describing the current domestic intelligence enterprise from core efforts to more peripheral, but still relevant, activities—we believe that the result still has significant value for understanding the nature of domestic intelligence today and the potential effects of major changes in intelligence policies.

Describing the Domestic Intelligence Enterprise

Even at the highest levels of government, federal responsibilities for domestic CT are split among several agencies. Overall, the FBI has primary responsibility for interdicting terrorist activity within the United States; DHS has primary responsibility for protecting and deterring against terrorist attacks; and the NCTC has primary responsibility for coordinating information-sharing and integrating foreign intelligence into the system. Moving outward from these core agencies—through multiagency entities aimed at improving coordination or information systems to move intelligence data throughout the country—reveals an increasingly complex system (as shown in Figure 3.1).

Today, the domestic intelligence enterprise has grown to encompass a wide array of federal agencies in addition to state and local

entities. This complexity has grown not just out of efforts to combat terrorism, but also from activities aimed at such problems as money-laundering and transnational crime. Given the connections and relationships among entities within the intelligence enterprise, boundaries are difficult to draw between different parts of the system. To provide a structure for discussion, we have broadly divided the enterprise into six categories, driven by the focus of the activities or the agencies that are central to their functioning:

- *nationally focused CT intelligence efforts* centered on the Director of National Intelligence (DNI) and the NCTC, as well as the FBI-managed Foreign Terrorist Tracking Task Force (FTTTF)
- *DHS-centered activities*, which include agencies responsible for and efforts related to border, transportation, and infrastructure security, among others
- *DOJ-centered activities*, which include FBI activities. This set of activities also includes a variety of information-collection and information-sharing activities aimed at other law enforcement missions
- *DoD-centered efforts*, including the activities of its associated agencies, military activities within the United States, and contributions to border security by military commands and task forces
- *counternarcotics and anti–money-laundering activities* centered in the DEA and the Department of the Treasury
- *state-, local-, and private sector–focused activities*, including federally sponsored programs (such as fusion centers and the JTTFs that span the gap between federal, state, and local) and activities conducted by local law enforcement organizations and private industry
- *activities conducted by other federal agencies* that do not necessarily focus on CT, criminal justice, or national security but that relate to the collection, sharing, and use of information on U.S. persons or domestic activities.

The following sections discuss examples of organizations and activities in each of these areas to sketch both the breadth and variety of domestic intelligence efforts in the United States.

Nationally Focused Counterterrorism Intelligence Efforts

The cluster of activities we have labeled *nationally focused* consists of intelligence activities that, in large part, bridge the divide between foreign and domestic intelligence. This cluster includes many of the activities of the IC, coordinated by the Office of the DNI (ODNI); the DNI reports directly to the President, acts as the principal adviser to the National Security Council and the Homeland Security Council (for intelligence matters related to national security), and oversees and directs the implementation of the National Intelligence Program) (ODNI, undated[a]). In this capacity, the DNI is responsible for coordinating the activities of the full range of IC organizations for both domestic and international terrorism (along with any other threats to U.S. interests) (ODNI, undated[b]).

The NCTC was established by Executive Order 13354, and the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. No. 108-458) placed it under the ODNI. The NCTC is the primary U.S. government organization for analyzing and integrating all intelligence pertaining to terrorism and CT—except for purely domestic terrorism, for which the FBI is the lead federal agency (Whitelaw, 2006). The NCTC serves as both the focal point for combining intelligence acquired through its partner CT organizations[3] and a national focal point for the production of integrated and interagency-coordinated analytic assessments of terrorism issues, warnings, alerts, and advisories.[4] It also manages the Terrorist Identities Datamart Environment (TIDE), which consolidates all information on terrorists and their

---

[3] NCTC partners include DOJ, Central Intelligence Agency (CIA), Department of State, DoD, DHS, and other entities, such as the Department of Energy, Nuclear Regulatory Commission, U.S. Capitol Police, the Department of Health and Human Services, Department of Agriculture, and Treasury.

[4] In our interviews, one member of a federal intelligence organization drew a distinction between the NCTC, which views its primary customer as "up"—the President and executive branch decisionmakers—and other elements of domestic intelligence activities that are

identities into a single database. In addition to the NCTC, the DNI manages the Information Sharing Environment (ISE), which aims to develop a coordinated set of procedures and policies for sharing CT information within the government.

Another post-9/11 effort to improve sharing and use of domestic terrorism intelligence is the FBI-managed FTTTF, which emphasizes mining of disparate "all-source" data streams in order to "provide information that helps keep foreign terrorists and their supporters out of the United States or leads to their exclusion, removal, surveillance, or prosecution" (DOJ OIG, 2005a; see also Shelby, 2002). Information sources reportedly include some 30 governmental data systems, including the FBI's criminal database, border security and immigration data sets, and customs data; 11 commercial sources; and four international data sets (GAO, 2005, p. 14). The FTTTF is an example of a broadly multiagency effort at the federal level for domestic intelligence and CT: As of November 2004, the FTTTF was staffed by the FBI, the DOJ Office of Legal Counsel, DoD, DHS, Immigration and Customs Enforcement (ICE), the Office of Personnel Management, and the CIA (Tanner, 2003).

Department of Homeland Security–Centered Activities

DHS contains a wide array of programs and agencies involved in intelligence activities in the United States or at the U.S. border. The Office of Intelligence and Analysis is the central organizational element of DHS for intelligence management and is a member of the intelligence community (USIC, undated). DHS contains U.S. Citizenship and Immigration Services (USCIS), Customs and Border Protection (CBP), ICE, Transportation Security Administration (TSA), U.S. Coast Guard (USCG), and the U.S. Secret Service (USSS), whose organizational missions involve intelligence activities, as well several other offices and efforts relevant to intelligence.

In its operational activities, DHS is a user of domestic intelligence information. The Office of Operations Coordination is responsible for

---

oriented "down" from the federal level to state and local law enforcement and homeland security organizations.

bringing together information regarding terrorist threats in the United States and coordinating among various agencies responsible for domestic security. It operates the National Operations Center (NOC), which "collects and fuses information from more than 35 Federal, State, territorial, tribal, local, and private-sector agencies" (DHS, 2008c). Some DHS domestic intelligence–related activities focus on specific threats or respond to single classes of incidents. For example, the Domestic Nuclear Detection Office (DNDO) focuses on nuclear and radiological threats to the United States. Its Operations Directorate runs the Joint Analysis Center, which houses staff from the FBI, Nuclear Regulatory Commission, the Department of Energy, and DoD and experts from parts of DHS, as well as a hotline to deal with radiological issues (Oxford, 2007).

DHS has put in place a number of IT systems for sharing information among agencies. The Homeland Security Information Network (HSIN) was a Web-based information portal for sensitive but unclassified information.[5] The Homeland Secure Data Network (HSDN) is similar to HSIN but transmits classified information. Other DHS information systems provide data on individuals that are used directly for security purposes. For example, among its most visible duties, the TSA maintains the No-Fly List and Selectee List, two databases that restrict access to commercial air travel. Individuals who meet certain criteria are placed on the Selectee List, which flags them for additional security screening. Individuals on the No-Fly List are barred from commercial air travel in United States ("Documents Show Errors," 2006).

As part of both its research and development (R&D) activities and its initiatives to pursue its organizational missions, DHS has been involved in developing information systems and analytical tools for intelligence missions. These have included the Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement (ADVISE) system, an expert-software program designed to produce "watch and warning" indicators by analyzing large amounts of data; ADVISE ran into difficulties and was halted due to privacy concerns (DHS OIG,

[5] DHS is reportedly reexamining or replacing the HSIN system (Hsu and O'Harrow, 2008).

2007b; Clayton, 2007). Still ongoing, however, is the Intelligence and Information Fusion (I2F) program (see DHS OIG, 2006).

DHS also manages programs and entities that seek to explicitly bridge organizational boundaries for domestic information-gathering and information-sharing purposes. For example, the information-sharing and analysis centers (ISACs) are a collection of public-private partnerships established to protect critical physical and electronic infrastructure from terrorist attacks. They encourage communication and the spread of best practices within an industrial sector, promote communication between sectors, and aid coordination and communication with the federal government (ISAC Council, 2004). A number of other DHS-managed programs have sought to reach out to the public and private sectors to gather domestic intelligence information. For example, the USCG-run America's Waterway Watch (AWW) asks people to be alert for suspicious activity and unusual events or individuals they may encounter in or around ports, docks, marinas, riversides, or beaches (USCG, 2005). Agencies within DHS also use tip lines and hotlines to collect information. Examples include the USCG-led National Response Center (NRC), which accepts reports of various incidents, including suspected terrorist activity (NRC, undated).

Department of Justice–Centered Activities

In addition to its domestic CT and counterintelligence (CI) activities, DOJ oversees an array of federal law enforcement activities. Other DOJ activities include investigating narcotics trafficking and organized crime and prosecuting federal crimes. Agencies that we have placed in this category include the FBI, DEA, U.S. Attorneys Offices, United States Marshals Service, and the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF). In pursuit of their organizational missions in both law enforcement and CT, these organizations collect, analyze, and share data on individuals and domestic activities.

The FBI is the focal point for a significant part of the federal government's CT efforts. In addition to its role in criminal investigations, it has become the central agency at the federal level for domestic intelligence and CT efforts since 9/11. These efforts are managed by the National Security Branch (NSB), which oversees FBI efforts to gather,

analyze, and act on threats to national security. Among other activities, the NSB Counterterrorism Division (CTD) runs the previously mentioned FTTTF and the National Joint Terrorism Task Force (NJTTF). The NJTTF is a multiagency task force that provides administrative, logistical, policy, financial, and training support and guidance to the JTTFs (discussed with state and local activities). The NJTTF both coordinates intelligence-gathering for the JTTFs and consolidates the information received from them into reports that are shared vertically with the other JTTFs in the field and horizontally with all of the participating NJTTF agencies. The NJTTF includes representatives from more than three-dozen other government agencies that collect and process terrorist intelligence.[6] A number of other information-fusion and database activities are carried out within the CTD, including management of the Terrorist Screening Center (TSC), which consolidates terrorist watch lists into a single directory and provides information on these lists to other agencies through the Terrorist Screening Database (TSDB).

The NSB Directorate of Intelligence (DI) and its components manage intelligence collection within the United States. In this role, it has elements in all operations divisions of the FBI and manages the Field Intelligence Groups (FIGs) in each FBI field office. In contrast to the more operationally oriented JTTFs, the FIGs perform more-traditional intelligence functions: identifying intelligence gaps, obtain-

[6] DOJ OIG (2005b). Agencies participating in the NJTTF include Air Force Office of Special Investigations; Army Criminal Investigative Command; Army Intelligence and Security Command; ATF; CBP; DEA; Defense Criminal Investigative Service; Defense HUMINT (human intelligence) Services; Defense Intelligence Agency; Defense Threat Reduction Agency; DHS; DoD; DOJ; Environmental Protection Agency; FBI; Federal Air Marshal Service; Federal Bureau of Prisons; Federal Protective Service; ICE; Internal Revenue Service; Metropolitan Police Department in Washington, D.C.; National Railroad Police; Naval Criminal Investigative Service; New York City Police Department; Nuclear Regulatory Commission; Office of Personnel Management; Treasury Inspector General for Tax Administration; TSA; U.S. Capitol Police; U.S. Department of Agriculture; U.S. Department of Energy; U.S. Department of Health and Human Services; U.S. Department of the Interior; U.S. Department of State; U.S. Department of Transportation; U.S. Department of the Treasury; U.S. Food and Drug Administration; U.S. Joint Forces Command (USJFCOM); U.S. Marshals Service; U.S. Northern Command (USNORTHCOM); U.S. Postal Inspection Service; U.S. Special Operations Command (USSOCOM); USCG; and USSS.

ing and analyzing raw intelligence, and generating intelligence products and disseminating them to their communities of interest (Spiller, 2006). Like many agencies within the domestic intelligence enterprise, the FBI has mechanisms in place to reach out to the public and private sectors for information, including an online tip line (FBI, undated[a]) for submitting terrorism tips (Lum, 2005).

The organizations in this cluster of the domestic intelligence enterprise also maintain and operate a broad array of information systems for storing and sharing intelligence and other information. Many of these systems were built for law enforcement rather than CT purposes but have found broader application in the current threat environment. Examples include the following:

- Justice Consolidated Network (JCN) for federal agencies to share information on fingerprints, arrest records, and other data gathered during investigations
- Justice Unified Telecommunications Network (JUTNet), a sensitive but unclassified network that transmits similar information between federal, state, and local agencies and provides videoconferencing and other telecommunication capabilities
- Regional Information Sharing Systems (RISS), which provide information-sharing, analytical support, and training to federal, state, and local law enforcement
- National Crime Information Center (NCIC), a database of crime reports, warrants, criminal records, and other information collected from and available to almost all law enforcement agencies around the country
- Violent Gang and Terrorist Organization File (VGTOF), which tracks individuals with known connections to gangs or terrorist groups
- Integrated Automated Fingerprint Identification System (IAFIS), a database of national fingerprint information obtained from criminal arrests and civil background checks
- Law Enforcement Online (LEO), one of the largest information-sharing networks, which can exchange sensitive but unclassified

information among all levels of law enforcement using a Web-based architecture
- Law Enforcement National Data Exchange (N-DEx), a data-mining project that collects criminal justice information and searches these records for new linkages. The Regional Data Exchange/Multi-Agency Information Sharing Initiative (R-DEx/MISI) is a similar program designed to share investigative information and search for linkages on a smaller scale.

Department of Defense–Centered Activities

DoD is involved in significant intelligence-collection efforts abroad. While many of these are forbidden from operating within the United States, DoD does conduct domestic information collection in support of its force-protection and criminal-investigation efforts. The Counterintelligence Field Activity (CIFA) was tasked with developing and managing CI operations for DoD. After 9/11, this role expanded to include not just defense against foreign governments, but also CT and possibly other activities as part of DoD force-protection efforts. From 2003 until 2007, CIFA operated the Threat and Local Observation Notice (TALON) system, a database of potential threats.[7]

The National Security Agency (NSA) conducts electronic and signal intelligence against targets outside of the United States and is one of the largest intelligence agencies in the United States. Its activities have included monitoring traffic between foreign citizens passing through the United States and communication between foreign citizens and U.S. citizens; the scope of this monitoring has increased considerably as technological changes have increased the volume of communication overall and transiting the United States.[8] Other intelligence

[7] This database came under significant scrutiny when it was revealed that it included information on military protesters and demonstrators and was ultimately canceled because of the controversy ("Pentagon to Close Disputed Database," 2007). In April 2008, Under Secretary of Defense for Intelligence James R. Clapper recommended closing down the CIFA program entirely (Warrick, 2008) by consolidating it into a new Defense Counterintelligence and HUMINT Center (see CIFA, 2008).

[8] The NSA's post-9/11 monitoring activity, including the extent to which it monitored communications involving U.S. persons without oversight of the Foreign Intelligence Surveil-

agencies within DoD also carry out activities that link to and share information with domestic entities, including efforts like the Defense Intelligence Agency's (DIA's) Joint Intelligence Task Force for Combating Terrorism (JITF-CT) and the Defense Information Systems Agency (DISA) Anti-Drug Network (ADNET), which shares information from a variety of agencies involved in combating drugs and drug-related crime and reportedly includes data-mining capabilities.

Each element of the armed services—the Army, Air Force, Navy, and Marines—has intelligence capabilities of its own, oriented toward providing information during wartime, but that also inform peacetime activities. Some of these activities relate to domestic missions, including law enforcement and CT force protection. Each branch has a criminal investigative service. Some of these, notably the Air Force's Office of Special Investigations (OSI) Eagle Eyes program, include activities for threat reporting and information collection from service members domestically.

The DoD combatant commands (COCOMs) command all military forces within a geographic area of responsibility. As part of this responsibility, they often provide specialized intelligence collection on a region of the world and manage joint task forces operating in that area. At least three of the commands have areas of responsibility that include the United States. USNORTHCOM was created after 9/11 to oversee operations in the air, land, and sea approaches to the United States and activities within the continental United States and Alaska. Given this area of responsibility, it is heavily focused on CT and civil-defense activities. It runs the Joint Protection Enterprise Network (JPEN), which shares information across DoD and the COCOMs on threats to U.S. forces and installations. It also manages Joint Task Force North (JTF North), which assists federal law enforcement with identifying and stopping transnational threats to the United States, such as terrorism and all forms of smuggling. One element of this mission is Operation Alliance, which focuses on narcotrafficking. U.S. Southern Command (USSOUTHCOM) focuses on planning for Central and South America. As a result, a significant portion of its activities is focused on

---

lance Court (FISC), has been an area of substantial controversy.

counterdrug operations. It operates the Joint Interagency Task Force South (JIATF South), which brings personnel from a variety of DoD and law enforcement entities together to prevent illegal trafficking within the Caribbean. U.S. Pacific Command (USPACOM) is responsible for activities in the Pacific and East Asia, including Hawaii. It manages the Joint Interagency Task Force West (JIATF West), which targets transnational threats and smuggling in the Pacific.

Counternarcotics and Anti–Money-Laundering Activities

Because of the transnational nature of narcotics trafficking and money-laundering activities, domestic intelligence activities—and intelligence activities focused on events at U.S. borders—have been in place to help address these problems for some time.

Counternarcotics Activities. Drug-related activities in the United States span a number of agencies. In addition to the DoD activities focused on drug trafficking discussed previously, a range of programs involving intelligence collection, analysis, and sharing are in place at a number of levels. The central actor in counternarcotics and, therefore, domestic intelligence activities in this area is the DEA. The agency's Intelligence Division manages a number of offices and programs that interface both with other agencies in the intelligence community (e.g., the division's National Security Intelligence Section) and operations to support state and local law enforcement activities (such as Operation Pipeline, which provides training, communication, and analytic support to local law enforcement targeting private motor vehicles involved in drug trafficking, and Operation Convoy, its commercial-vehicle counterpart). The Intelligence Division manages information-fusion centers. For example, the El Paso Intelligence Center (EPIC) is the major hub for collecting, analyzing, and disseminating drug-related intelligence for all levels of law enforcement and government. It covers drug, alien, and weapon smuggling, as well as terrorism-related smuggling. To support state and local operations, the DEA has organized Mobile Enforcement Teams (METs) to assist state and local law enforcement facing particularly difficult drug-enforcement challenges. When requested by state and local law enforcement, the DEA will send

a team to assist in investigation, intelligence collection and analysis, arrests, and prosecution.

Outside DEA Intelligence, there are a number of explicitly interagency organizations focused on collecting and sharing counterdrug intelligence. The High Intensity Drug Trafficking Areas (HITDAs) are regions designated by the White House Office of National Drug Control Policy (ONDCP) as focus areas for addressing drug-trafficking control. Each of the 31 HITDAs has a HIDTA Regional Intelligence Center, which coordinates among federal, state, and local agencies to improve counterdrug work. In this role, it manages a database of ongoing investigations and manages drug intelligence-sharing within that region's law enforcement community. Several other intelligence programs are run directly by DOJ. The National Drug Intelligence Center (NDIC) manages drug-related intelligence from all national security and law enforcement organizations and supports ONDCP and the HIDTA program. It serves as a hub for drug-related intelligence and includes representatives from all federal law enforcement agencies, DHS, the State Department, and DoD. DOJ also manages the Organized Crime and Drug Enforcement Task Force (OCDETF) program, which coordinates activities by a variety of federal agencies focusing on major drug-smuggling and money-laundering operations. There is an OCDETF in each of the 93 U.S. Attorneys Offices, which are each, in turn, a member of one of the nine OCDETF regions.

Financial Crime–Focused Activities. The central organizational actor for combating most financial crime is the Department of the Treasury, although many agencies across the U.S. domestic intelligence enterprise also have roles to play (e.g., the USSS, which we have located in the homeland security portion of our map). Treasury operates the Office of Terrorism and Financial Intelligence (TFI), which aims to coordinate department activities focused on terrorism, weapons of mass destruction (WMD) proliferation, and other national security issues. In this role, it coordinates assets involved in intelligence collection and enforcement. The Office of Intelligence and Analysis (OIA) falls within TFI, specifically focusing on collecting, analyzing, and sharing intelligence and CI information relating to Treasury.

Treasury operates two major information systems, which serve as the backbone for many federal information-sharing systems and are among the most important networks in sharing domestic law enforcement and intelligence information. The Treasury Enforcement and Communications System (TECS) is a text-based database compiling records from a wide array of federal agencies and systems, such as NCIC, the National Law Enforcement Telecommunication System (NLETS), and border-control agencies. The Financial Crimes Enforcement Network (FinCEN) collects and shares information on financial crime, terrorist financing, and other crimes involving the financial system. It shares information and analysis with a range of law enforcement and government agencies and collects data from the private sector.

State-, Local-, and Private Sector–Centered Activities

Efforts at the state and local levels are the most decentralized and diverse elements of the current institutional system for domestic intelligence. Local police departments' capabilities vary over a wide range, from rural sheriffs' offices staffed by only a few individuals to major police departments in such cities as New York and Los Angeles with dedicated intelligence and CT capabilities (Riley et al., 2005). Other activities at the state and local levels involve agencies outside law enforcement, as well as multiagency entities—some organized and supported from the federal level—for coordination and information-sharing. These include fusion centers and JTTFs.

A *fusion center* receives resources, expertise, and information from multiple agencies to maximize those agencies' "ability to detect, prevent, investigate, and respond to criminal and terrorist activity" (DOJ and DHS, 2006). DHS supports the fusion center program (Masse, O'Neil, and Rollins, 2007). A recent U.S. Government Accountability Office (GAO) report identified fusion centers in at least the planning stages in nearly every state in the nation.[9] Some states have more than one. The state of California, for example, has four.[10] Although there is

[9] Wyoming will partner with Colorado in its fusion efforts (GAO, 2007c, p. 16).

[10] The Los Angeles Joint Regional Intelligence Center (JRIC) includes personnel from the Los Angeles Police Department, the Los Angeles County Sheriff's Department, and the FBI.

great variation in terms of staff size and partnerships, almost all fusion centers are led by state or local law enforcement entities and have federal personnel assigned to them. In general, fusion centers are mechanisms for information-sharing between state and local and federal entities (DHS, FBI, DEA, ATF), as well as collaborative operational efforts "to detect, prevent, investigate, and respond to criminal and terrorist activity" (GAO, 2007c, p. i). Some fusion centers also include personnel from public health, social services, public safety, and public works organizations.

State and federal representatives provide a broad spectrum of information to fusion centers, including the locations and capabilities of area hospitals, details from calls to the state's 911 emergency system, and names from federal terrorist watch lists. The combination of these data is designed to provide a clearer picture of threats facing each state. In addition, it helps inform police investigations, contingency planning, and emergency response (Masse, O'Neil, and Rollins, 2007; see also DOJ and DHS, 2006; NCTC, 2006). In coordination with locally based federal officials, the fusion centers gather, process, analyze, and interpret locally generated information that is not threat- or incident-related and disseminate it at the national level via the FBI, DHS, DoD, or other appropriate agency channels. Because most fusion centers are fairly young, the state fusion centers to date seem to have played a greater role in disseminating data among local police departments and down the chain from federal players to local police departments than in serving as a focal point for accumulating information.

The other prominent federally directed domestic CT activities at the state and local levels are the JTTFs. The FBI-led JTTFs have "primary operational responsibility for terrorism investigations that are not related to ongoing prosecutions" (OHS, 2002b, pp. 25–28). Although the majority of fusion centers are still in the setup phase, the JTTFs have been in existence for much longer—and many are colocated with the nascent fusion centers. The first JTTF was established in New York City in 1980. There were 36 JTTFs in operation

---

It includes seven counties, from north of San Diego to San Luis Obispo. In April 2006, the Los Angeles TEW was folded into the Los Angeles JRIC.

at the end of 2001 (Carey, 2001), and today, there is at least one in each of the FBI's 56 field offices and another 50 or so spread out among other major cities (FBI, 2004a).[11] JTTFs are operational entities that undertake surveillance, source development, and investigative activities but also focus on information-sharing with local law enforcement. JTTF personnel on the FBI side are often located in the FBI's field and regional offices, and their primary focus is addressing terrorism threats and preventing terrorist incidents. The JTTFs share classified and unclassified information with their federal, state, and local partners and hold meetings for their members and agency liaisons (DOJ OIG, 2005a). The regional JTTFs are coordinated at the national level by a centralized JTTF at FBI headquarters in the Strategic Information and Operations Center (discussed previously).

Other Federal Agencies

A number of other federal organizations play smaller institutional domestic intelligence roles. They may participate in activities that others spearhead, or they may collect and share information in specialized topical areas (e.g., the Department of Energy's intelligence role in specialized areas or information systems for collecting and sharing public health alerts and epidemiological information maintained by the Department of Health and Human Services). Some of these agencies have explicit intelligence roles, missions, and capabilities. However, many federal agencies have few intelligence or intelligence-related capabilities and participate in domestic intelligence activities mainly through information-sharing and joint task forces.

Discussion

To understand the pros and cons of establishing a new domestic CT intelligence organization, a picture of the existing system's structure

[11] According to an FBI white paper (2006b), there were 101 JTTFs across the country and the national-level JTTF was comprised of personnel from 38 federal agencies as of September 2006.

and function is critical. The goal of the mapping effort whose results are summarized in Figure 3.1 was to characterize that existing system. What did we learn from the effort? It is now an oft-cited aphorism that "it takes a network to fight a network" (Arquilla and Ronfeldt, 2001), emphasizing the difficulty that structured bureaucratic organizations sometimes have in taking on flexible, loosely coupled, and mutable terrorist organizations. Whether or not that aphorism is true, it is clear based on our review that current domestic intelligence activities constitute—if nothing else—a very complex network of organizations and information-sharing relationships.

Looking across the map, several descriptive points are particularly relevant when considering the advantages and disadvantages of the current U.S. domestic intelligence enterprise:

- There is a wide variety of connections among levels of government for information-sharing. For example, in our map, state and local law enforcement appears more than 20 times, linked to various information systems, across organizational centers, or to task forces created for different CT, law enforcement, counterdrug, and counter–money-laundering purposes.[12]
- Similar activities are proliferating at different places in the domestic intelligence system. In addition to data collected from the literature, interviewees and expert-panel participants cited this proliferation as a result of confusion and ambiguity in individual agencies' roles within the domestic intelligence enterprise and uncertainty about who is responsible for what parts of the effort. The fact that so many independent organizational actors are involved inherently makes both understanding current domestic intelligence capabilities and oversight of those activities challenging.
- There are a number of routes for both the members of the public and private-sector organizations to input (and receive) information from the domestic intelligence enterprise. There is a pro-

[12] An alternative way of representing this arrangement would be to include only a single entry for state and local law enforcement with many links to other parts of the network. We include multiple entries to produce a map that is easier to read and understand.

liferation of tip lines in many organizations, including multiple elements of DHS (the USCG NRC; AWW and its state counterpart, River Watch; Highway Watch®, CBP), DOJ (including the FBI and ATF), and at the state and local levels. Private-sector interaction and information-sharing mechanisms include submissions of data into such organizations as FinCEN, ISACs, JTTFs, fusion centers, and TEWs. The role of private-sector data providers in data-mining programs at many places in government is also notable.

- A wide variety of information systems are in place for a range of purposes. Some federal systems provide conduits for data or intelligence to other federal agencies or to state and local governments; others have been created and are maintained from the bottom up for horizontal sharing at the state and local levels.[13] Because of the tendency to link multiple information systems into single organizational entities (e.g., fusion centers or JTTFs), there may, in fact, be more connectivity throughout the network than is represented here. In addition, some data systems are hosted on other information systems as well, meaning that there may be more links through which information can flow.

However, though it was possible to identify many relevant organizations and map the reported links between them, it is more difficult to make the jump from this structural picture to what the programs and links *mean* for the effectiveness of current intelligence efforts. For example, while the links among domestic intelligence–related activities are extensively documented, how those links work in reality is not always clear. At one extreme, a link may simply represent joint access to an information system, while at the other, it may involve actual joint activities mixing individuals from multiple organizations. In addition, the scope of the activities included in this mapping differs significantly from one organization to another. At one end of the spectrum, such

[13] For example, "In the absence of a clear, consistent system for homeland security intelligence requirements management, state, local, tribal, and private sector entities have developed their own informal and formal structures and networks to share information and intelligence" (LLIS, 2005, p. 2).

agencies as the FBI are devoting a large fraction of their total organizational effort to activities focused on domestic intelligence and CT. At the other end, agencies like DoD, while involved in some parts of domestic intelligence, are devoting only a small slice of their total organizational effort to them. Exact figures for personnel and resources for many of these agencies and activities are also classified and therefore not available in open sources.

In exploring the concept of creating a new domestic CT intelligence organization, the current complexity of domestic intelligence activities—and the uncertainty in the current enterprise's functioning and effectiveness—is an important factor in policy deliberation.[14,15] It also significantly complicates the very concept of managing the U.S. domestic intelligence enterprise.[16] The following sections consider some of the current system's broader conceptual advantages and disadvantages that would contribute to the costs and benefits of making significant changes to that system.

General System Advantages

Networked, So Relatively Agile and Responsive to the Needs of Individual Agencies. The current system is a highly interconnected network composed of numerous independent elements. Each element is responsible for a certain limited domain and has significant resources it

---

[14] Some expert contributors to this study were critical of the structure of the current domestic intelligence enterprise—even dismissing it as having "no structure" and critical of the confusion it creates for the CT domestic intelligence mission. One expert described domestic intelligence as "a pickup ballgame without a real structure, leadership, management, or output."

[15] Our results for domestic activities echo public reporting of internal government consideration of overall U.S. CT efforts:

> The counterterrorism infrastructure that resulted [from the post-9/11 expansion] has become so immense and unwieldy that many looking at it from the outside, and even some on the inside, have trouble understanding how it works or how much safer it has made the country. . . . Institutions historically charged with protecting the nation have produced a new generation of bureaucratic offspring—[DoD's CIFA and JITF-CT, Treasury's OIA], and the FBI's National Security Service (NSS), to name a few—many with seemingly overlapping missions. (DeYoung, 2006)

[16] Comments of participant in the project expert panel.

can bring to bear on that area. As a result, the current network is good at collecting information and acting within these domains. For example, in the past several decades, the USCG has focused on intercepting drugs smuggled into the country by air and sea. Its focus has allowed it to maintain tight control over airspace around the southern U.S. border.[17] Sea shipping has proved to be a more intractable problem, but the USCG's focus has made it better at interdiction than any other agency in the government. This functional expertise applies directly to analyzing and preventing smuggling in support of terrorism—expertise that might otherwise be dispersed or nonexistent. The benefits of this sort of functional focus are replicated many times in the current network.

Highly Diverse in Organizational and Analytical Culture, So Greater Potential Creativity. In conjunction with freedom of action, each agency's focus brings something different to CT analysis. Every organization approaches the terrorism threat differently, so the resulting analysis in the system overall will be more creative and represent a more comprehensive description of potential threats. TSA might approach security for port workers through regulation and credentialing, the USCG may consider how individuals could gain access to these areas from the water, and the FBI may consider how such credentialed workers could be bribed or otherwise compromised. If different organizations can recruit analysts from different backgrounds and disciplines, this can increase the quality of the results as well.[18]

Potentially Able to Expand and Contract Smoothly. Because each element of the domestic intelligence network is a part of a larger agency with a broader mission, there will *potentially* be less resistance if a task is moved to another agency or an operation is shut down than in a dedicated organization whose entire existence is focused on that single mission. In practice, the extent to which this is true is debatable and would likely differ considerably from case to case and based on the bureaucratic behavior of the specific organizations involved. For exam-

---

[17] The USCG shares lead-agency responsibilities for air interdiction with CBP and is the lead agency for maritime interdiction for the U.S. drug-interdiction mission (USCG, 2008a).

[18] This was one advantage that was identified in examinations of other nations' experiences in managing and staffing domestic intelligence efforts (see Jackson, 2008).

ple, in the DoD context, each major command maintains its intelligence apparatus in spite of the fact that DIA was created to centralize those functions for DoD—even though the military commands have many functions other than intelligence.[19]

Similarly, new structures can be created and plugged into the existing system as new threats are recognized. The creation of the NCTC and TSC demonstrates that even a major node can be added to the network.[20] Where a large agency would have an entrenched bureaucratic interest in maintaining programs or preventing new ones from arising elsewhere in the government, the current system has a high churn in low-level operations as programs and responsibilities are created, reallocated, and eliminated.

General System Challenges

Limited Strategic Direction, Coordination, and Lack of a Uniform Legal Framework for the Overall Enterprise. In the current system, the only individual with overarching strategic direction over the totality of domestic intelligence is the President. This causes problems in creating and sustaining a unified direction and approach to threats. For example, in 2007, GAO cited problems in planning interagency strategy and coordination in developing HSIN (a major DHS information-sharing network) and in responding to in-air security threats (Powner, 2007; Berrick, 2007a). Even if an agency is selected to lead strategy on an issue, the amorphous nature of the network can dilute that responsibility and the ability to act on it, undermining progress. For example, in the past few years, responsibility for developing a CT information-sharing framework has resided at the White House, the Office of Management and Budget, DHS, and the ODNI (GAO, 2007a, p. 88). Problems of this sort have been a recurring theme in interagency homeland security and CT efforts in the past several years.

---

[19] We would like to acknowledge Paul Pillar for bringing this example to our attention.

[20] The creation of the NCTC as additive to current arrangements—and the fact that other organizations have not ceded CT to the new entity—is a counterexample to the potential advantage cited in the previous paragraph. In spite of the opportunity for organizations with multiple missions to give up parts of their CT responsibility, this did not occur in practice.

The lack of overarching coordination and direction can also create uncertainty about legal boundaries. Since 9/11, some domestic intelligence operations have come under fire for going beyond what they are legally allowed, undermining public trust in and cooperation with domestic intelligence–collection agencies. A 2005 incident in which an Army intelligence alert led Akron police to monitor a nonviolent protest demonstrates the challenges. Based on information gathered from the military's TALON reporting system, the DHS Joint Regional Information Exchange System (JRIES), and the Web, Army intelligence decided that protesters could be coordinated and pose a threat to military personnel. Ultimately, in a May 2005 report to USNORTHCOM, the Army itself rejected this assertion (see Block and Solomon, 2006). This incident raised concerns about military activities within the United States because the Army alert and resulting police surveillance were based on the perception of a threat not seen by any civilian agencies. The Army asserts that it legally received information by searching the Web or government databases, but the line between receiving (which is legal for the military) and gathering (which is not) is unclear (Block and Solomon, 2006). Such lack of coordination and delineation of boundaries can also lead to questionable activities and to flawed analysis as agencies cross over into subjects they are ill suited to analyze.

False Positives and Information-Quality Concerns. Reflecting the desire of current intelligence entities to function effectively as a network, many efforts have sought to improve the volume of information moving through the system. There has been less attention to the quality of what is being shared. Efforts focused on identifying a few threatening actors against a background of many innocent ones will invariably generate false positives—individuals or organizations incorrectly flagged as potential threats. Some data are available publicly on such false positives in some intelligence programs. For example, NSA monitoring of communications to U.S. citizens led that agency to pass thousands of tips to the FBI each month. Yet, law enforcement and CT officials stated that these tips were vague, diverted attention from more-useful work, and produced very few new leads (Bergman et al., 2006). False positives can be a significant problem when automated

techniques, such as data mining, are used to seek out new leads as well. For example, the vast majority of annual hits from the TSDB are false alarms, in one case leading to the incorrect detention of the same person 21 times in a single year (Nakashima, 2007b).

In addition to concerns about systems producing false positives, there are concerns about current efforts simply collecting so much data that are of such low quality that they do not provide much CT benefit. This issue of information quality has been raised about suspicious-activity reports (SARs). In the financial arena, in which transmitting SARs has been an established part of efforts to counter criminal activity, there were concerns even before 9/11 that the "volume of these reports was interfering with effective law enforcement" (Schulhofer, 2002, p. 52). Suspicious-activity reporting through law enforcement and other channels into federal government organizations has been reported to be of even less practical utility.[21] An NCTC official was quoted in the press, observing, "In many instances the threshold for reporting is low, which makes it extremely difficult to evaluate some of this information" (Pincus, 2006).

Although problems with false positives and information quality can certainly occur within a single intelligence organization, the diversity inherent in a complex domestic intelligence enterprise could produce additional complications. In a networked system with dispersed authority and responsibility, both these data concerns pose related but distinct problems. In the case of false positives, the concern is that, if the central focus is on information-sharing among those organizations, these spurious hits will travel to many separate intelligence organizations, both increasing the chances that the false identification will result in costs imposed on the individual and creating burdens and potentially wasted effort for multiple organizations. In the case of data-quality concerns, a dispersed and diverse system of autonomous organizations makes it hard to create standards and common practices to maintain a high quality of information flowing into the system from across the country.

[21] Author discussions with federal officials.

Competing Bureaucratic Interests and Imperatives. The diversity that gives the domestic intelligence network its agility also creates limitations on the flow of information. Currently, information is collected and managed in a diverse array of organizations. With almost all of them, domestic intelligence collection and CT make up just one mission among many, so their information-sharing systems, institutional rules, and organizational norms are not specifically designed for CT. This creates friction in a variety of ways. Different databases may not record the same information in the same format, making sharing and analysis difficult. For example, as of 2006, the FBI and DHS systems for recording fingerprints were incompatible because of differences in the way they were designed. FBI fingerprinting requirements made for a slow, but highly accurate, process, while DHS requirements allowed for rapid processing of many people. Both systems are important to identifying potential terrorists, yet other priorities drove each agency's requirements. This was a recognized problem going back to the 1990s, but there was no agreement until mid-2005, and the two systems are not expected to be fully compatible until 2009 (DOJ OIG, 2006c).

Finally, in spite of a focus on interagency cooperation in the current domestic intelligence and CT effort, bureaucratic competition within the same mission area can also create suspicion of outsiders and makes intelligence professionals less willing to share analytic products, much less raw information. Though some intelligence professionals we interviewed cited progress in this area, views were not unanimous, and some assured us that interagency conflicts over responsibility and stature were still a factor hindering cooperation among organizations.

Conclusions

When we consider the creation of a new domestic intelligence agency, current domestic intelligence activities represent the institutional context that such an organization would inhabit, disrupt, or replace in part or in total. Based on our structural-mapping exercise, the complexity of the current system is clear. In creating a new agency, simplifying that complexity could be one goal, moving activities that are

currently spread among multiple organizations into a single organizational home. Doing so could address some challenges with the current system by making it possible to impose more-centralized direction and standards of operation. However, though the complexity that currently exists seems to suggest a structural benefit from creating a new agency, the lack of comprehensive information on the functioning of that system is reason for caution. In our review of current efforts, we sought out data on how well those efforts were performing. Though anecdotal evidence of some problems is available (e.g., the issues cited under "General System Challenges"), how those problems are affecting the nation's ability to prevent terrorist attacks is not entirely clear. Though questions have been raised since 9/11 about the functioning of domestic intelligence efforts, the reality remains that there have been no major successful attacks since then. Whether the reason for that fortunate reality is the effectiveness of current efforts or simply luck is not clear. As a result, to the extent that current relationships and processes are providing effective capabilities to collect, analyze, share, and act on intelligence data, the founding of a new organization might disrupt capabilities that are already in place and—at least in the near term—disrupt success in preventing terrorist activity.

CHAPTER FOUR

Societal Acceptability of Domestic Intelligence

Genevieve Lester

This chapter explores the societal acceptability of a domestic counterterrorism (CT) intelligence agency. While it is quite clear that the government is *capable* of creating a new agency to gather and analyze domestic intelligence, the question addressed in this chapter is how acceptable such an agency might be to the American public. Not only does American democracy have governing institutions and legal structures different from those of other countries discussed in international case studies of domestic intelligence institutions (Jackson, 2008), but Americans have expectations about such issues as civil liberties, privacy, and individualism that may differ from those in other democracies discussed here.[1]

The societal context of a U.S. domestic intelligence CT agency is complex: On one level, issues of security and defense cross national boundaries; democratic governments aim to protect their populations and the rule of law controls the lengths to which governments may go to do this. On a second level, American values, ethics, and idiosyncratic form of democracy add very specific cultural layers to the roles of domestic intelligence and homeland security. Finally, on a third level, the United States is still in post-9/11 flux in terms of understanding and calibrating the requirements for security efforts. U.S. institutions are still adjusting to the societal shock of the terrorist attacks, although the initial horror has dissipated in the years since 2001. This continu-

[1] For space considerations, this discussion is limited to the U.S. societal context. I rely on my colleagues' work in other chapters to draw out specific comparisons with the other democracies discussed in the companion volume (Jackson, 2008).

ing recalibration is reflected in the public's and policymakers' changing attitudes toward the threat of terrorism.

This chapter focuses on the second and third conceptual levels—other chapters having addressed the first. It discusses the potential societal acceptability of a domestic CT intelligence agency in terms of American cultural and public requirements and examines these characteristics within the context of the dynamic, post-9/11 security environment. Discussion of a domestic intelligence agency has appeared cyclically in the public domain—generally upon the revelation of intelligence-reform failures or after the publication of intelligence-reform recommendations. Debate, usually taking place among academics and policy elites, has, however, rarely engaged the public actively or deeply.

In order, then, to capture a sense of the acceptability of a new agency in the absence of specific empirical data, and to discover where public attention *does* focus, this chapter takes several analytical cuts at the problem. It investigates the broader domestic intelligence issues that could influence public opinion, in tandem with issues of governance (such as the credibility of government institutions and policy), and finally, issues of public threat perception. This chapter seeks to explore the cycles and trends of public opinion and understand how these trends might shape the societal context in which a domestic CT intelligence agency would function.

The challenges encountered by the current efforts to redefine the role and structure of domestic intelligence in American society are not only a function of the ramifications of the threat—real and perceived—of terrorism. They are also linked to the current political context and the relationship of trust—or lack thereof—between the public and policymakers. These issues are analogous to the problems uncovered by the Church Committee (discussed in greater detail in Chapter Two) 30 years ago. A comparison of reactions and reform measures then and now demonstrates that political scandals—such as the revelations about the counterintelligence program (COINTELPRO) and other Federal Bureau of Investigation (FBI) and Central Intelligence Agency (CIA) abuses—cause introspection and a focus on reestablishing pro-

priety, whereas intelligence "failures," such as Pearl Harbor and the attacks on 9/11, engender a focus on efficacy (Gill, 2002, p. 298).

The Church Committee, responding to the public outrage in reaction to political scandal and to protect the civil rights of U.S. citizens, recommended that the foundations of a "wall" between law enforcement and intelligence be put in place. What was once perceived as a safeguard for the American people, however, has been much criticized in the post-9/11 era. This wall, blamed for information-sharing failures, has been vigorously dismantled in wave after wave of post-9/11 intelligence-reform initiatives.

The current security environment—with reform efforts focusing predominantly on the *efficacy* of intelligence and security—may require a new type of wall, no wall at all, or perhaps an entirely different structure, any of which can engage the emerging threat while balancing the responsibilities of protecting civil liberties, maintaining the openness and transparency expected in a democracy, and fostering the appropriate oversight required by law. Regardless of whether a new structure is created—or what type of structure this turns out to be—the political context, the credibility and transparency of policymakers and institutions, and the cycle of public threat perception will all play substantive roles in its creation. Understanding the dynamics of these issues is imperative for policymakers, who have enormous decisionmaking power, particularly in times of national emergency.

This chapter begins by investigating trends in public perception of the terrorist threat as well as the public's view of the efficacy of government measures in handling this threat. This section introduces the question of a public sense of the *need* for a new agency, laying the groundwork for an assessment of the acceptability of an agency devoted solely to countering this threat. The second section focuses on the issue of the perceived trade-off between civil liberties and security, delving into what the public feels is an appropriate balance. The third considers public perception of specific CT law enforcement measures, such as surveillance and other potentially invasive information-gathering techniques, and queries the public view of the potential trade-off between the use of the techniques and the individual's expectation of personal privacy. This section also looks into the controversial area of demo-

graphic targeting as a tool in CT operations. Finally, the fourth section addresses the crucial triangular relationship among public trust, credibility, and effectiveness in terms of the role of a potential domestic CT intelligence agency.

Public Threat Perception: Terrorism

At the time of this research, there had only been one concrete polling question that had focused specifically on a domestic intelligence agency. A FOXNews/Opinion Dynamics poll (2004a) asked respondents, "Do you think the creation of a domestic intelligence agency in the United States, similar to Great Britain's MI-5, would be more likely to help in the fight against terrorism or hurt the privacy and civil liberties of Americans?" The responses to this question were oriented toward "helping the fight" (39 percent) but were analytically inconclusive: Twenty-eight percent thought that it would hurt liberties, 9 percent said that it would neither help the fight nor hurt liberties or said that it would do both, and 24 percent were not sure (FOXNews/Opinion Dynamics, 2004a). Thus, to understand the acceptability of a domestic CT intelligence agency, we have investigated a broader range of information on public threat perception and other issues related to the objective of this study.

Public perception of threat informs the public's policy preferences. Understanding these preferences helps policymakers make acceptable decisions about issues that are emotional and sensitive, such as security and privacy. Put differently,

> Ordinary citizens depend on the critical roles played by policy experts and advocates, but if the views of the general public are not discredited and ignored, they can provide important guidelines about the boundaries within which acceptable and sustainable public policies can be shaped. (Herron and Jenkins-Smith, 2006, p. 178)

This section explores the dynamics of public threat perceptions and shows how the rhythm of public response to threat could affect sup-

port for intelligence and law enforcement operations and ultimately a domestic CT intelligence agency.

Terrorism as a public phenomenon and as a dynamic threat challenging the United States highlights issues of threat perception and the post-9/11 conception of homeland security—a concept and phrase that were introduced into common usage in reaction to that experience. In the current security environment, the rise of terrorism as a threat has pressed particularly on the societal component of national security: Not only does terrorism bring conflict to the domestic level (and to U.S. shores)—blending the domestic and foreign spheres—but it is particularly focused on destabilizing society on a social and psychological level (Lewis, 2005, p. 18).

In the words of terrorism expert Martha Crenshaw, "The political effectiveness of terrorism is importantly determined by the psychological effects of violence on audiences" (Crenshaw, 1986, quoted in Huddy, Feldman, Taber, and Lahav, 2005, p. 593). Further, as stated to the point of aphorism by RAND's Brian Jenkins, "Terrorists want a lot of people watching, not a lot of people dead" (recently adjusted to include the more extreme, "many terrorists want a lot of people watching *and* a lot of people dead"). Both of these statements point to the symbolic, psychological, and *public* aspects of the terrorist threat (Jenkins, 2006, pp. 8–9). Finally, to quote Jenkins once again, "Terrorism is aimed at the people watching; terrorism is theater" (Jenkins, 2006, p. 11).

In these circumstances, fundamental issues of the public perception of terrorism, the feelings of the individual citizen regarding personal risk and vulnerability, and his or her notion of the threat level of the nation at large become exceedingly important. Threat perceptions influence public behavior, economic activity, and individual responses to emergency and disaster (Burns, 2007). They also influence public support for CT measures and policy (Huddy, Feldman, Taber, and Lahav, 2005, p. 593; Jenkins-Smith and Herron, 2005, p. 603). Individuals tend to rely on their perceptions of both the general terrorism threat and the threat of specific terrorist acts when they make choices about which policies to support (Joslyn and Haider-Markel, 2007). Threat perception can thus be an indicator of the public's willingness to accept measures intended to protect them but for which they may have

to sacrifice—both in the concrete (such as invasive searches at airports) and in the ethereal and ambiguous (such as the rumor of technological surveillance that cannot be assessed adequately by the layperson) (see Bamford, 2006).

Public threat perception on a behavioral level is quite complex, influenced by a range of variables, and affected by cognitive biases and individuals' use of mental heuristics. Many factors affect how the public perceives terrorism risk and threat. These break down by age, race, gender, education level, income level, region, and proximity to past attack sites.[2] Public threat perception manifests itself in a range of ways, some public and some private. In the public arena, fear of a terrorist attack may change travel and consumer behavior, while, on a personal level, individuals may suffer from sleeplessness, anxiety, and depression. Further, emotion and affect influence how the public gauges the probability of a terrorist attack (Sunstein, 2003, p. 121). Fear, in contrast to anxiety, elicits a different perceived probability of potential attack. In this context, fear tends to elicit aggressive reactions, whereas anxiety causes risk-averse behaviors. Anxiety can, however, also have a positive effect: It can cause the public to experiment with new and innovative policy options as complacency and the status quo are challenged. An attack of striking magnitude can cause familiar heuristics and behavioral patterns to be questioned, leaving room for change (Jenkins-Smith and Herron, 2005, p. 603). This outcome could have obvious ramifications for public support of new policies regarding security issues as well as for institutional change.

Further, general feelings of heightened threat tend to influence public support for direct government action and for strong symbolic gestures (Huddy, Feldman, Taber, and Lahav, 2005, p. 594). There are strong links between a sense of national identity, in this context, and policy preferences (Schildkraut, 2002, p. 513). Again, strong feelings of threat can influence the public's support for strident—even poten-

---

[2] Among many studies focusing on aspects of these attributes, see Fischhoff et al. (2003). See also Huddy, Feldman, Capelos, and Provost (2002, esp. p. 498), for breakdowns based on age, race, gender, and occupation. See Huddy, Feldman, Taber, and Lahav (2005); Davis and Silver (2004a).

tially invasive—security measures. As one study demonstrated, "perceived threat increased support for homeland security policies designed to minimize future risk, even when such policies violate support for civil liberties" (Huddy, Feldman, Taber, and Lahav, 2005, p. 596). Heightened threat perception has, according to this study, "consistently increased support for domestic antiterrorism policies," including government-issued identification cards and domestic surveillance (Huddy, Feldman, Taber, and Lahav, 2005, p. 603). Heightened threat perception immediately after the attacks on 9/11 was linked more to concern that the government would not in fact enact strong CT measures than that these measures would infringe unnecessarily on civil liberties (Huddy, Feldman, Taber, and Lahav, 2005, p. 603).

The typical cycle for heightened terrorism-threat perception is quite intuitive—immediately after an event, there is a spike in public response and anxiety, and fear rises. This trend gradually diminishes as time passes after the attack and the availability of the image fades. Public perception is nuanced and mercurial. The connection, thus, between threat perception and support of national security policies is fragile and worthy of careful study. As Herron and Jenkins-Smith (2006) point out, by 2003, the public's perceived threat levels had dropped even below those in the pre-9/11 survey period. These perceptions cycle, and survey questions and timing can affect data on them. Further, media coverage of events and threat warnings from the administration can affect public threat perception. Polling data suggest that the U.S. Department of Homeland Security's (DHS's) color-coded terrorism advisory system did cause spikes in public concern about terrorism when adjusted upward to orange (high) (Davis and Silver, 2004b, p. 16).[3]

Perceptions of threat can also spike in response to nonterrorism events, such as during the beginning stages of the war in Iraq (Davis and Silver, 2004b, p. 10). The spikes tend to revert quickly—within

[3] By 2005, it was pointed out that the DHS advisory system, subject to much criticism and even public mocking, had been given a lower-key role in threat communication and was no longer highlighted in the media as a guide for public response—although, as of this writing, it continues to exist (Mintz, 2005; Fessler, 2007). The main criticisms of the system were vagueness, unclear expectations of how the public should respond to a given alert level, and an increasing view that the alerts were a political tool.

a week, according to the data on the orange alerts (Davis and Silver, 2004b, p. 17). This cycle is, of course, affected by many of the demographic characteristics listed already: gender, age, race, income, and education level. Interestingly, however, there appears to be resilience in the American public: While it has often been mentioned that 9/11 changed American society forever, inferences drawn from polling trends seem to indicate that the American public adjusts to and absorbs changes in threat reasonably effectively and efficiently. This is demonstrated by the return to baseline or even below-baseline perceptions of personal threat as the time since attack elapses (see Lewis, 2005, and Herron and Jenkins-Smith, 2006, among others, for a discussion of this trend).

The public's perception of the threat of terrorism combined with individuals' sense of the effectiveness of the current CT structure can provide an understanding of the acceptability of a domestic CT intelligence agency. In terms of immediate security solutions, the public looks to the government for protective measures directly after an event. People expect the security services to protect them capably, so, polling data indicate, they will tend to accept, for a while, whatever measures public officials deem appropriate. Terrorists challenge this trust and acceptance by trying to demonstrate that the government cannot fulfill its responsibility to protect the public (Kuzma, 2007, p. 93).

According to Herron and Jenkins-Smith's extensive study of public attitudes toward security issues, public expectations of government action in response to terrorism have tended to follow—once again—a cyclical and intuitive trend (Herron and Jenkins-Smith, 2006, pp. 65–93). Surveys conducted between 1995 and 2001 showed significant increases in the mean assessment of the requirement that the government act to prevent terrorism (see Herron and Jenkins-Smith, 2006). By 2003, public expectation that the government act had receded but remained above pre-9/11 levels (Herron and Jenkins-Smith, 2006, pp. 74–75). The crucial linked concept is whether the public feels that the government *can* do something to stop terrorism. In 2001, respondents believed more strongly on average than they did before or have since that the government could do something to stop terrorists. By 2003, however, respondents' mean assessments had

reverted to their pre-9/11 levels. This is similar to the trends found in mean confidence in the government's ability to prevent terrorism and the public's willingness to accept intrusive measures, both of which increased right after 9/11, then declined to pre-9/11 levels by 2003 (Herron and Jenkins-Smith, 2006, p. 75).

Only 32 percent of the respondents felt that all large-scale attacks against the United States in the subsequent five years could be prevented. In terms of government effectiveness, then, the public feels that CT measures are moderately effective and necessary. Kuzma asserts that this wary response could be a function of the nature of the terrorist threat rather than the public's belief in the government's ability or willingness to stop potential attacks (Kuzma, 2007, p. 94). It appears that the American public assumes that the conflict will be of long duration and that U.S. defenses will not entirely eliminate the possibility of further terrorist attacks.

These moderately ambivalent views are mirrored in the public's perception of intelligence reform. While a fraught topic among academics, blue-ribbon commissions, and policy analysts, intelligence reform does not seem to have much traction with the public at large. One of very few polls on intelligence was conducted in December 2004, the same month as the passage of the Intelligence Reform and Terrorism Prevention Act (IRTPA), asking respondents whether they approved or disapproved of the bill. The results showed that 34 percent approved, 15 percent disapproved, 26 percent were not sure, and 25 percent had not heard of it.[4] The ambiguous results of this poll reinforce two things: The details of intelligence reform are still mainly discussed at the elite level, and question framing can have a tremendous impact on analysis of public attitudes. If this question had been framed more broadly to include, for example, a larger question on the relationship between ter-

[4] FOXNews/Opinion Dynamics (2004b). The polling data drawn from this and related surveys should be viewed as potentially influenced by framing effects. The polling industry must gather and measure data on issues about which some respondents know very little. For a discussion of the problems of "manufacturing" public opinion, see S. Best and McDermott (2007).

rorism, intelligence failure, and reform, it might have yielded a more definitive response.[5]

In general, the public tends to separate the issues of state from personal concerns. In terms of the complexities of threat perception, a wide range of studies have pointed to the fact that individuals separate their own personal concerns and anxieties from their perception of what affects the nation as a whole and thus what national policies they support (Huddy, Feldman, Capelos, and Provost, 2002, p. 488). Personal issues do not tend to influence how Americans perceive the government or larger policy matters. Perceptions of threat on a personal level tend to spike during or after an event, then readjust over time.

In a poll conducted on September 11, 2001, 58 percent of the respondents were somewhat or very worried that they or a member of their immediate family would "become the victim of a terrorist attack" (Huddy, Feldman, Capelos, and Provost, 2002, p. 488). Americans' personal fears about a terrorist attack had diminished within a month after the attacks on 9/11. The results of a Gallup poll conducted on October 3, 2001, pointed out that less than one-third of the respondents expressed a high level of concern about terrorism or safety in their communities (Lewis, 2005, p. 19).

Our conclusion from this analysis is that heightened terrorism-threat perception on a national level appears to correspond with support for national security policy measures. This is especially the case, of course, immediately following an event, when the public is more willing to accept strong security measures—even when the measures could limit civil liberties. A range of polling data has demonstrated that threat perception increases the public's willingness to allow the government a wider operational margin within which to enact policies aimed at shoring up national security (Huddy, Feldman, Taber, and Lahav, 2005, p. 605). The weighing of security versus civil liberties tends to tilt back toward civil liberties as time progresses and memories of the event fade.

These findings have interesting potential ramifications for the acceptability of a domestic CT intelligence agency. The public still per-

[5] My thanks to Paul Pillar for this suggestion.

ceives a threat of terrorism, though that perception affects lifestyles and personal behavioral patterns very little. It appears that there could generally be support for security policy measures, based on an apparent relationship between this type of support and a national or collective perception of a terrorism threat. Further, in official rhetoric, the post-9/11 period has continually been referred to as a "break from the past," a "new security environment," or "new normal historical context," suggesting attitudes of change, new beginnings, and lifestyles permanently altered by the threat of terrorism (see Davis and Silver, 2004b). This, combined with the threat-related anxiety cited by Herron and Jenkins-Smith (2006), could indicate a public willingness and flexibility to try new policies, breaking with the status quo. If anything, the long sequence of reform efforts in the intelligence community has demonstrated that change is possible and acceptable, if a bit challenging at times.

Having said this, threat perceptions and support for security measures vary as threat perception changes. Media communication and perceptions of government capability and integrity—or malfeasance—influence individuals' opinions. While there is cautious support for government security measures and institutional reform initiatives, the variability of the data demonstrates that care and sensitivity must be used in transmitting to the public what these measures are, why they are important, and what trade-offs are necessary to make them effective. Transparency of method, objective, and governance are key to maintaining the relationship between the public and the decision-maker in this context.

The Balance of Civil Liberties and Security

This section focuses on the appropriate role of domestic intelligence in a democracy, focusing particularly on the thorny issue of the public acceptability of potential challenges to civil liberties and privacy. It does so in the context of considering the lengths to which the U.S. government is—and should be—empowered to respond to the type of ambiguous threat represented by terrorism. This is not untrodden terri-

tory: Throughout U.S. history, in times of national security crisis, civil liberties have been curtailed in exchange for perceived greater security, the balance between liberties and security generally being restored after each crisis.

The question here is how to gauge the perceived appropriate trade-off between civil liberties and security. This issue is not as clear-cut as it may seem at first glance. As Peter Gill presciently wrote, the issue is not appropriately defined as a *balance metaphor*: The public should not accept this "balance" as such, but rather should require an understanding of proportionality of response to the "nature and size of the security threat" (Gill, 2002, p. 314). How does one gauge the response that is appropriate in terms of how and whether intelligence-gathering should be allowed to infringe on privacy or civil liberties in the name of security? At an even more basic level, how does one gauge the extent of a threat when the threat is ambiguous and evolving?

In general, the public responds to the question of recalibrating the balance between civil liberties and security in the direction of security immediately after an event—in this case, a terrorist attack. As with a sense of personal threat, however, the pendulum swings back in the direction of civil liberties fairly quickly. Strikingly, polling data from the immediate post-9/11 period indicated that the public was roughly evenly concerned that the government would *not* respond to the security threat as it was about infringement on civil liberties (Lewis, 2005, p. 24). The poll asked, "What concerns you more right now? That the government will fail to enact strong, new antiterrorism laws, or that that the government will enact new antiterrorism laws [that] excessively restrict the average person's civil liberties?"[6] While neither side carried a clear majority in response to this question directly after the attacks, polls conducted in January 2002 and June 2002 regarding civil liberties and security elicited responses favoring civil liberties (Lewis, 2005, p. 23).

According to the poll numbers, the public perceived a sacrifice of civil liberties as necessary only immediately after the attacks on

[6] The source of the polling questions was Princeton Survey Research Associates and CBS News/New York Times (2002). Lewis (2005, p. 23) discusses the results at length.

9/11. One must differentiate among data that focus on a more general willingness to provide leeway to the government in ways that could affect future civil liberties issues and data on views of specific security measures. Elicitations on civil liberties depend on the context in which respondents are questioned and how concrete the trade-offs are between civil liberties and security in the questions. Are civil liberties considered in the abstract, or are concrete sacrifices mentioned? And for what, exactly, are individuals told they are exchanging their civil liberties? The phrasing of what constitutes the "good" received in exchange for the diminished civil liberty makes a difference in the person's response.[7] These data suggest that the public is more willing to accept specific security measures when polling questions refer to concrete policies than when questions use abstract terms, such as "giving up civil liberties" (Lewis, 2005, p. 24).

In terms of concrete CT measures and intelligence, it is often mentioned that there is a fear that the techniques commonly associated with foreign intelligence—such as warrantless investigations, surveillance, interrogation, and detention—could be used against Americans (Martin, 2004, p. 13). Civil libertarians argue that shifting the focus from crime to broader preventive measures based on intelligence collection could also allow for a domestic intelligence agency to focus on politics, race, political belief, or ideology as a basis for surveillance and investigation (Cole, 2003). A fear also mentioned often in the debate about a domestic intelligence agency is that these methods will raise the specter of past CIA and FBI abuses. In this vein, there is a fear that what the government does elsewhere could be used against Americans at home, with the dividing line becoming increasingly murky.

When asked to rank the personal importance of government surveillance, 73 percent of the respondents thought the issue was very or somewhat important (Pew Research Center for the People and the Press, 2006). More specifically, in terms of attempting to elicit critical responses, another poll posed the following question: "Do you approve or disapprove of the way George W. Bush is handling . . . govern-

---

[7] For a discussion of the importance of concept definition and question wording to the reliability of survey data, see S. Best and McDermott (2007, pp. 7–9, 11).

ment surveillance of US citizens?" Thirty-nine percent of respondents approved, while 52 percent disapproved, and 9 percent had no opinion (CNN, 2006). In a February 2006 poll, however, citizens were asked, "Overall, thinking about the possibility of terrorist threats do you feel the U.S. (United States) law enforcement is using its expanded surveillance powers in a proper way, or not?" (Harris Poll, 2006) with 57 percent of the respondents indicating that law enforcement was using its powers in a proper way and only 40 percent viewing law enforcement as not doing so.

To investigate what the public considers appropriate in terms of specific security countermeasures, we analyzed the polling data associated with several specific *types* of CT measures. In March 2006, 1,000 adults were asked about the FBI's additional authority to conduct surveillance and wiretaps and to obtain records on terrorism investigations. The question was posed in a way that presented arguments on both sides of the issue: "Supporters said this was necessary to fight terrorism. Opponents said it went too far in compromising privacy rights. Do you think this additional FBI authority should or should not be continued?" (ABC News/Washington Post, 2006a). The results were as follows: Sixty-two percent said that it should be continued, and 37 percent said that it should not. A poll conducted in 2007 asked respondents whether they felt that the government was doing enough to protect civil liberties in the fight against terrorism. Those results were evenly balanced, with 48 percent on each side (Washington Post–Kaiser Family Foundation–Harvard University poll data presented in Duke, 2007).

This outcome suggests a complex and mixed view of appropriate levels of invasiveness when it comes to specific countermeasures. Generally, the public is willing to allow law enforcement a margin when conducting investigations focused specifically on terrorism. It does, however, also point out that opinion is nuanced: A measure's perceived level of invasiveness affects its acceptability.

Another study, conducted between November 2001 and February 2002, focused on five specific CT proposals in order to assess the pub-

lic's willingness to accept more-stringent security measures.[8] The first question asked about the public's willingness to accept increased security in public places, such as shopping malls and government buildings. The result was 88.8 percent in favor or strongly in favor of these measures. A second question showed that 96.3 percent of the respondent population was in favor of increased security at critical infrastructure facilities. These results are fairly intuitive and abstract; there is minimal apparent loss of freedom or privacy in exchange for the positive good of security.

Two further questions were concerned with more personal and invasive measures and led to answers swaying in the other direction: The question, "Should passengers be banned from carrying luggage aboard airlines?" showed 61.7 percent opposing or strongly opposing and 38.3 percent favoring or strongly favoring. These results are similar to those for the final question: "Should police be allowed to stop people at random on the street and search their possessions?" Opposing or strongly opposing these measures were 73.9 percent of respondents, in contrast with 26.1 percent in favor or strongly in favor. Another question asked about the acceptability of national identification cards, with 42.5 percent opposed or strongly opposed and 57.6 percent in favor or strongly in favor (see Joslyn and Haider-Markel, 2007, pp. 318–319).

In some cases, there has been contradiction as to which trend—support or opposition—is, in fact, dominant among the public. The contradiction could arise from question format or questionnaire methodology. Further, the cyclical trend of threat perception clearly affects what the public is willing to accept in terms of the possible infringement of civil liberties as well as whom people will accept as the party responsible for the infringement. When queried on the role of the U.S. President, for example, in terms of conducting surveillance, polling data weighted toward the negative: lack of support. Law enforcement, however, still seems to hold public respect in terms of perceived appropriate use of additional powers and use of surveillance tools (see Lewis 2005 for a discussion of this dynamic).

---

[8] These data were drawn from Joslyn and Haider-Markel (2007, pp. 318–319).

Public support for specific CT methods tends to lean toward law enforcement measures, even though these measures may infringe on privacy rights. It must be pointed out that a theme throughout these polling data is greater permissiveness when words like "terrorism" or "terrorist" are used. This could explain the variability of response, particularly in terms of civil liberties questions. As a 2006 ABC News poll pointed out, when asked whether federal agencies were intruding on Americans' privacy rights in their investigations of terrorist activities, 61 percent answered that they were, while 35 percent thought that they were not, and 4 percent had no opinion (ABC News, 2006a). The follow-on question, whether these intrusions on some people's privacy rights were justified, elicited the following response: Fifty-four percent stated that the CT measures were justified, while 40 percent said that they were not justified, and 6 percent had no opinion (ABC News, 2006b).

This introduces an interesting secondary line of inquiry: How do people feel about the targeting of particular social or racial groups—to which they do not belong—for CT investigation? The data trends show a similar response to those that included words such as "terrorism" and "terror," words that quite obviously are intended to demonstrate to the respondent that he or she is not intended to be included in the group investigated. The results of a Cornell University poll published in December 2004 pointed out that almost half of all Americans believed that "Muslim-Americans are a threat and their civil liberties should be curtailed." Further, 27 percent of those interviewed supported mandatory registration of Muslim Americans, while 29 percent felt that it was appropriate for undercover agents to infiltrate civic organizations with heavily Muslim membership.[9] Similar data gathered from polls conducted in 1995 and 1996 point to the public's willingness to support wiretaps and infiltration if that surveillance is targeted toward the "other"—in this case, two questions focused on "suspected terrorists" and "possible terrorist groups," respectively. In both cases, support for these measures ranged between 69 and 76 percent (Kuzma, 2007, p. 96).

---

[9] Cornell University polling data discussed in Simon and Stevenson (2005–2006, p. 51).

As a sweeping generalization—but one grounded in data—those who do not tend to be targets of intelligence and law enforcement attention also tend to have a benign view of the subject of invasive countermeasures. Thus, reactions of groups more likely to be targeted by security efforts to the threat of terrorism and appropriate responses can diverge significantly from the statistical norm of the population, which generally does not feel exposed to potentially harsh or invasive investigation. This makes obvious sense, but what it introduces to the operational debate is worthy of mention.

Generally, according to the analysis presented in this chapter and the data discussed in others, the public tends not to engage very vociferously in debates about law enforcement or intelligence. A recent example of public reaction to a proposed security program—the Los Angeles Police Department's (LAPD's) program that involved mapping the area's Muslim communities—however, introduces an alternate argument: that public engagement can occur when the focus is on a specific coherent issue—such as racial (or other) profiling—and that this engagement can affect policy choices when it is organized and well articulated. The proposed LAPD program entailed pinpointing—mapping—predominantly Muslim neighborhoods in the region using census data and other demographic information and assessing their isolation and thus perceived vulnerability to extremism. Based on this map of communities, police would target the areas for study—examining cultures, languages, and demographics in order to facilitate LAPD community outreach. The final objective of this program was to integrate these perceived enclaves into broader mainstream society. The proposed program drew tremendous outrage from regional Muslim organizations and the American Civil Liberties Union (ACLU). Within several days of being revealed on the front page of the *Los Angeles Times*, the program was quashed.[10]

While this project was short-lived, the concept behind it reflects other cross-cutting efforts used by potentially comparable domestic intelligence units—such as MI5 in the UK. It introduces interesting

[10] For a discussion of the project and the community response, see MacFarquhar (2007) and Winton, Watanabe, and Krikorian (2007).

dynamics, however, in the U.S. context: dynamics that are illustrative of the issues that a domestic intelligence agency would have to address in order to be effective. These include questions of the acceptability of demographic targeting, the importance of transparency and open discourse about the objectives and methods of investigation and surveillance, and appropriate and active oversight in order to ensure accountability and public trust.

Further, the mapping project demonstrated that regional historical relationships with law enforcement would have an impact on how specific populations would potentially respond to a domestic CT intelligence agency. In Los Angeles, there is an entrenched distrust of intelligence-led policing—particularly among minority groups and especially focused on the intelligence unit of the LAPD.

While a focus on one urban area in the context of this volume is undoubtedly too narrow, the public reaction to the proposed program in Los Angeles and its very quick cancellation (within several days) points to the influence that the organized public may have on intelligence activities. Understanding complex regional and demographic reactions to law enforcement and intelligence could yield dividends in terms of forecasting public response to a domestic intelligence agency.

Public Trust and Credibility

Although this chapter has focused extensively on changing public perceptions of the threat of terrorism, this concept must be understood as firmly placed within a political context. Perceptions of threat and government effectiveness in responding to that threat link together with public trust to determine how the public views the balance between security and civil liberties. This relationship also helps determine what security-policy choices the public is most likely to support. In the 1970s, in the wake of the Watergate scandal and the revelations of the Church Committee, the public had very little trust that decisionmakers would make appropriate choices regarding issues that could affect their civil liberties. After the attacks on September 11, conversely, the public was much more willing to trust that the government would respond appro-

priately to the threat. This trust led the public to support, generally, the security policies generated immediately after the attacks, some of which were potentially both invasive and precedent-setting, such as the USA PATRIOT Act and the Protect America Act.

As Davis and Silver point out,

> At every level of trust in the federal government, increased sense of threat led to greater willingness to concede some civil liberties in favor of security. And at every level of perceived threat of terrorism, the greater people's trust in the government, the more willing they were to concede some civil liberties for security. (Davis and Silver, 2003, p. 4)

Public trust allows a margin in which the government can ask the public to allow restrictions on their civil liberties (Davis and Silver, 2004a, p. 30). The polling data provide an indication of how the public feels about secrecy—when and where secrecy is considered appropriate and what creates distrust in necessarily opaque government activities. Public trust in the government rose to record levels directly after the attacks on 9/11. It reached levels not seen since the 1960s (Chanley, 2002, p. 469). "As trust in government increases, citizens' support for expending public resources is also expected to rise" (Chanley, 2002, p. 470). An interesting point here is how attention can be shifted from domestic concerns to international threat:

> When public attention shifts from concern about domestic policy issues such as health care and education to concern about issues of foreign policy and threats from abroad, trust in government may increase as the nation pulls together to address international concerns or defend national security. (Chanley, 2002, p. 470)

Trust correlates with a public commitment to using public resources to solve problems that the nation faces (Chanley, 2002, p. 470). It also corresponds to rising levels of national threat perception. When the public identifies terrorism and national security issues as the most important issues it faces, public trust goes up. When the perceived threat diminishes, so does trust in government. According

to Chanley's analysis of polling data on this issue, public trust diminished incrementally in October, November, and December 2001. This decrease was paired with a decrease in the public's view that terrorism, defense, and foreign-policy concerns were the most important problems that the United States was facing (Chanley, 2002, p. 479).

Crucially, for the effective operation of intelligence, "Political trust . . . is the judgment of the citizenry that the system and the political incumbents are responsive, and will do what is right even in the absence of constant scrutiny" (Blind, 2006, p. 4). It transcends partisan politics and the delimitations of ideology (Blind, 2006, p. 5). One component of political trust focuses on *institution-based trust*—that is, trust that refers to the perception of specific political institutions. Political trust is linked to credibility as an indicator of the public's perception of what constitutes solid policymaking. Credibility as a concept is drawn from the economics literature and refers to the public response to *accumulated* good policymaking. That is, trust is banked as the public sees evidence of solid results from policymakers' or organizations' decisions and actions. This concept of credibility is obviously quite complicated when it comes to intelligence and security. The public cannot know every detail of an intelligence or law enforcement operation; thus, public trust and a sense of institutional legitimacy must bridge this gap. While Jeffreys-Jones was writing about the CIA when he made the following statement, the sentiment would apply equally well to a potential domestic intelligence agency: He defines *legitimacy* of an intelligence agency as "the degree to which the American people accept the Agency and its work as *necessary*, and as constitutionally and legislatively authorized" (Jeffreys-Jones, 2003, p. 5; emphasis added).

The question of the appropriate levels of openness regarding intelligence has been a subject debated since the 1970s, when the pendulum swung in the direction of oversight, accountability, and transparency. Since then, oversight of clandestine operations and budgets and openness of the budget of the intelligence community overall have been

issues of debate.[11] Although the Church Committee began the process of "opening" intelligence, the cycle of intelligence transparency and opacity responds to changes in the threat environment and in policy decisions. In terms of the current security environment, openness about intelligence and law enforcement developments could lend a great deal of credibility to these enterprises. This is particularly the case if a domestic intelligence agency is to be introduced to a society long accustomed to a division between activities acceptable "over there" and those allowed in the United States.

The relationships between secrecy, transparency, and intelligence operations are quite complex in a democracy, even when the public is generally supportive of CT and law enforcement actions. Along these lines, there has been an effort on the part of both the CIA and FBI to open their activities and engage with the media. Both have public-affairs offices, and the CIA, especially, has published books, reports, and other materials containing previously classified material, adding some transparency to its operations (Hulnick, 1999, p. 470).

In the context of CT, most importantly, this openness could help build public trust, which could help diminish the inevitable psychological ripple effects of a terrorist attack. Secondarily, openness about a new agency could assuage public doubt that has arisen in the wake of such programs as the Total Information Awareness (TIA; later, Terrorism Information Awareness) program developed by the Defense Advanced Research Projects Agency (DARPA) and the warrantless surveillance program led by the National Security Agency (NSA). Ironically, it has been mentioned quite often that the TIA program could have been overseen effectively and managed to deal responsibly with the data that were provided to it. Shutting the program down based on outrage and lack of information—in addition to poor choices of both branding and leader—merely pushed these types of programs underground

[11] See L. Johnson (1989, pp. 91–93) for a discussion of the executive authorization of covert missions. See also Treverton (2001) for a discussion of broader intelligence issues, such as government openness about the intelligence budget.

or caused them to be relabeled and kept out of the public eye.[12] Public trust could be tried by the exposure of clandestine programs directed toward U.S. citizens and activities that remain ambiguous and illegal in the public eye, such as extraordinary rendition, CIA prisons abroad, and increased FBI surveillance of Americans based on their associations or civic activities.

In terms of methodology in this chapter, it is important to point out that there are ambiguities and conflicting outcomes in polling data like those used here about public threat perception and views of security policies. Timing, ambiguous question formulation, and methodology can all affect the reliability of the results. Further, there has been an absolute deluge of surveys related to 9/11 and terrorism. Many of these surveys point in different directions, although the trends highlighted in this chapter tend to run throughout the majority of the material. These data are difficult to aggregate and assess because different questions under the broader umbrella of, for example, "civil liberties" and "security" elicit different responses, tipping the balance one way or another depending on the specific issue (Davis and Silver, 2003, p. 3).

Finally, once again, although issues of security and terrorism absorb the energy of policymakers and those who support those policymakers, there is minimal public engagement with them by anyone beyond elite audiences. While public concern seems to be moderately high on an ambient level and has remained high since the mid-1980s, terrorism until 9/11 did not seem to have had much traction as a political issue among the public. Finally, even after 9/11, terrorism as a daily concern faded fairly quickly from view, remaining generally the purview of the media, policy analysts, academics, and decisionmakers.

Public Perception and the Portrayal of Intelligence

Having considered public threat perception and views of security measures, we now turn to a brief examination of a different layer of the rela-

[12] See TAPAC (2004) for a discussion of privacy trade-offs and DARPA programs, including TIA.

tionship between intelligence and public opinion. This section explores how post-9/11 intelligence and law enforcement CT activities are portrayed in the media and what impact this portrayal could have on the public's perception and acceptance of a domestic CT intelligence agency. The media are an important conduit for information—whether accurate or not—on intelligence activities. Coverage of these issues is broad, ranging from media-distributed allegations of intelligence and law enforcement misdeeds, such as the existence of CIA prisons and extraordinary rendition, to political dramas relating to intelligence failure and failure to reform. Other recent portrayals are fictional, using the agencies and their CT activities as the basis for television shows, such as *24*, and movies, such as *Rendition*.

These portrayals could—for better or for worse—fill in the "gap of ambiguity" that is characteristic of the secret operations of intelligence. They can also sway political opinion about what the intelligence community is doing and what people think is appropriate behavior for intelligence entities. This can have ramifications for public perception of administration policy statements regarding these issues—and thus public trust—as well as for how acceptable a domestic intelligence agency would be in these circumstances. Interestingly, while the debates about a domestic intelligence agency have occurred mainly at the policymaker or academic elite level, media portrayals of CT and intelligence are where these issues are presented to a much broader public.

One high-profile example of the blending of reality and fiction in domestic CT issues was the Heritage Foundation–organized panel, "*24* and America's Image in Fighting Terrorism: Fact, Fiction or Does It Matter?" that united producers and actors from the hit show *24* with DHS Secretary Michael Chertoff to discuss issues of perceptions of terrorism and decisions about U.S. security policy. The panel addressed questions of how closely related the show's portrayal of CT operations is to the "real thing." While the panel discussion elicited vague answers relating to problems of "imperfect information" or "unpalatable alternatives," a more defined data point for exploring how media portrayals shape public perceptions of intelligence and CT activities is the fact

that *24* features a torture scene in almost every episode—the first five seasons of the show depicted 67 torture scenes.[13]

The issues introduced by this show are not simply about television standards of violence; they run deeper in terms of public perception of acceptable CT methods. The portrayal on *24* of security trumping the rule of law in American society and of torture as an acceptable tool for intelligence operations has even penetrated the ranks of the military. A dean at the U.S. Military Academy at West Point noted that the show portrays the sacrifice of law in exchange for national security as a positive value. The effect is, according to him, "toxic" (Mayer, 2007, p. 66). He mentioned that the television show's representations of torture are affecting how military personnel perceive the limits of their duties in operations abroad. Others have commented that U.S. Army interrogators use methods seen on television against the detainees assigned to them. Additionally, while depictions of torture are not strictly a post-9/11 phenomenon, the depictions of the *torturers* have changed. Now the torturers are the "good guys"—intelligence officers fighting terrorists with tactics of terror (Mayer, 2007, p. 66).

These portrayals may or may not affect interrogators' use of torture in their operations, but they do demonstrate a changing notion of acceptable CT methods. While television's impact on behavior is the subject of a different type of study, it can be asserted that viewing repetitive scenes of torture could normalize the extreme behavior depicted in them. As an extension, the availability of these images could affect the public's perception of what activities a domestic intelligence agency involved in CT operations would be authorized to perform, regardless of the reality of this perception. Preconceptions and fictional portrayals will fill the gap when no information is forthcoming. Once again, public trust and the credibility of law enforcement and intelligence in the United States will depend on clarity in an agency's adherence to the rule of law, transparency to the extent possible, and a clear public security value being provided by a new agency's mission and work. Again, this point has particular traction because the public is not engaged

[13] Farhi (2006). See also Heritage Foundation (2006) for text, video, and discussion of the event; the count was provided by Parents Television Council, quoted in Regan (2007).

in issues of intelligence. If there were more local-level concern, there would be more dialogue. As it is, if domestic intelligence is a topic solely for policymakers and academia, television will provide one of the few public windows into that discussion.

Conclusions

Analysis suggests that, while the public does not have great anxiety regarding the threat of terrorism at the individual level, in the aggregate, the perception is that the terrorist attacks on 9/11 did mark a definitive change and alteration of American institutional and political culture. This turning point could be used to redefine appropriate measures and structures to deal with the terrorist threat, including the creation of a new domestic intelligence agency.

Based on available polling data, it appears that the public is moderately disengaged from the logistical issues of national security and that individuals' concern with the matter of terrorism, in particular, tends to oscillate (Pillar, 2001, p. 202). Individuals tend to separate broader policy issues from their personal needs and fears, including their fear of terrorist attacks. This could be a function of natural personal self-involvement and focus on familiar and personal issues but also the result of a general sense of a lack of articulation of security and intelligence requirements and options. In contrast to answers to broad polling questions, specific circumstances can crystallize public opinion and lead to the failures of specific programs—such as TIA or the LAPD community-mapping project—showing that fundamental concerns can have immediate impact when groups are motivated to participate. The public is relatively ambivalent but also mercurial and reactive to threat, communication, and the dread that arises out of perceptions of inappropriate, nontransparent government behavior in an open democracy.

For the current study, the fundamental public-policy issue likely to shape the public acceptability of a new domestic CT intelligence agency will be articulating clearly what role the agency will have, what legal and oversight structures will direct its activities, and what respon-

sibility this entity will have to provide a level of transparency to the public. While the public has not been overly concerned about the reorganization of the intelligence community, engagement and expectations would probably change in the face of another terrorist attack. Alternatively, if Americans perceived that a new agency would cost them in terms of civil liberties, extensive efforts would have to be made to clarify which specific oversight and legal mechanisms would be employed to provide accountability, particularly given the secrecy that would inevitably shroud many of the organization's activities. This would include careful analysis and control of specific countermeasures—such as surveillance and searches—but also methodologies for choosing whom to investigate, specifically ensuring that individuals who fit a specific profile are not targeted in a manner unbefitting a society based on openness and respect for civil liberties and diversity.

The Church Committee investigations of the mid-1970s uncovered abuses that were the result of an "enormous unrestricted fear about the American people."[14] In that period, the threat was radical, politicized student groups. Now, terrorism drives threat perception, and the global nature of the current conflict has created tensions of religion, culture, and race. In both cases, intelligence and law enforcement operations turned toward the domestic polity. The result in the former case was abuse and, eventually, national reflection and reactive reform. In the latter case, there is room to increase sophistication, sensitivity, and appropriate communication with the public when it comes to institutionalizing domestic CT intelligence.

---

[14] Walter Mondale quoted in L. Johnson (2004, p. 6).

CHAPTER FIVE

The Law and the Creation of a New Domestic Intelligence Agency in the United States

Jeremiah Goulka with Michael A. Wermuth

The idea of creating a new domestic intelligence agency raises a host of legal and constitutional questions. This chapter discusses the institutional and structural legal issues involved in creating a new agency. We examine several legal issues that would arise if the President or Congress should decide to create a new domestic intelligence agency. First, we discuss whether Congress or the President has the power to create a domestic intelligence agency, as an independent agency or as part of an existing agency, and whether it can transfer functions or units of other agencies to a new or existing agency. Resolving that there is no constitutional barrier to creating a new agency, we then discuss the framework legislation that would govern how to create a new agency. Finally, we discuss various specific legal issues that would arise relating to oversight, personnel, powers, and finance.

This chapter does not address the myriad questions of civil rights and civil liberties that arise in the context of domestic intelligence because they are distinct from the legal questions associated with creating a new agency and how to do so. Civil rights and civil liberties questions are addressed in our colleagues' chapters on the history of domestic intelligence, the public acceptability of a domestic intelligence agency, and privacy issues in intelligence.

Given the events of recent years, domestic counterterrorism (CT) intelligence is frequently viewed as a policy area with inherent tensions and trade-offs between maintaining security and protecting civil rights

and liberties.[1] As our colleagues' chapters on the history of domestic intelligence and the social acceptability of a domestic intelligence agency demonstrate, public opinion on CT measures swings like a pendulum. In the weeks immediately following a significant fear-inducing incident, there is frequent outcry for robust new preventive powers, investigations of failure to prevent the incident, and aggressive prosecution of perpetrators. As time passes, public concern swings back toward an emphasis on civil rights and liberties.

Different points of view regarding the current system's success in this balancing act may lead observers to support or oppose the creation of a domestic intelligence agency. If an individual holds the opinion that the Federal Bureau of Investigation (FBI) is not capable of effectively carrying out the domestic intelligence mission inside the borders of the United States (due to its law enforcement focus and training, inadequacy of its counterintelligence [CI] or CT career tracks, or other reasons), then a new agency might offer an alternative. Opinions that domestic intelligence functions are too dispersed among intelligence agencies, from the FBI to the Department of Defense (DoD), may lead to proposals for a single new agency. Similarly, if one holds the opinion that the FBI or other government agencies have, in their operations, exceeded constitutional or legal constraints that protect civil rights or liberties, a new agency may seem appropriate, especially if such a new agency could inculcate an organizational culture that is adequately attentive to civil rights and civil liberties concerns. Others may hold that civil liberties are best protected by competing agencies or investigators trained in constitutional policing practices and, accordingly, oppose the creation of a new agency.

Significantly, these are essentially questions of organization, management, coordination, and culture, but not questions of law. Ensur-

---

[1] RAND analysis in 2003, provided to the congressionally mandated Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (also known as the Gilmore Commission), concluded that "[r]ather than the traditional portrayal of security and civil liberties as competing values that must be weighed on opposite ends of a balance, these values should be recognized as mutually reinforcing." The full analysis was included as Appendix E in the commission's fifth and final report to the President and the Congress (Gilmore Commission, 2003).

ing that any agency conducting domestic intelligence activities protects both security and civil rights and liberties is an operational issue, influenced by governing laws and policies, actual operational practices, the agency's leadership and professional ethos, and its employees' characteristics and degrees of professionalism. In the context of this study, it is important to note that the *decision* whether to create a domestic intelligence agency will not, on its own, influence domestic intelligence practices. If a decision is made to create a new agency with a clear intent to expand or curtail intelligence powers, that motivation may shape the practices of the new agency. However, whether such practices would violate their governing legal framework—or whether the current legal framework for regulating these activities is appropriate—presents separate legal and operational questions that have little to do with the creation of a new agency. Further, the decision itself will not affect the legal authorities that guide domestic intelligence activities. Whether governing-agency regulations transgress their empowering statutes and whether executive orders or statutes transgress the Constitution and its civil rights and civil liberties norms are legal questions that have little to do with the creation of a new agency.

Should Congress or the President decide to pursue building a new agency, it might be opportune for them to take a fresh look at the body of law that creates and governs surveillance powers and other intelligence activities to consider its propriety, constitutionality, and efficacy.[2] Otherwise, a new agency would operate under the same constitutional and statutory framework that governs the agencies that currently conduct domestic intelligence operations. We do not address those considerations, or the vast literature discussing them, in any detail in this chapter. Instead, we address the legalities and procedures for creating a new federal agency.

---

[2] Congress occasionally reviews surveillance laws. See, for example, "US Congress Reassesses Surveillance Laws" (2007).

The Legality of Creating a New Federal Agency

The legal and constitutional issues that arise when creating a new federal agency are not new and have been addressed before, most recently in creating the Department of Homeland Security (DHS), the position of Director of National Intelligence (DNI), and the Office of the Director of National Intelligence (ODNI), and, in the not-too-distant past, in the division of the Department of Health, Education, and Welfare into the Department of Health and Human Services and the Department of Education. There is no doubt that it is legal to create a new agency, but there are some constitutional and statutory provisions that may guide its creation and shaping.

Constitutional Considerations

The text of the Constitution itself provides only minimal guidance on creating or restructuring federal agencies (A. O'Connell, 2006, pp. 1708–1709). To the extent that the drafters anticipated the creation of executive departments, they largely left "design decisions to the two political branches . . . with limited judicial review" (A. O'Connell, 2006, p. 1708). A few elements of loose guidance can be found. The Necessary and Proper clause grants Congress the power to "make all laws which shall be necessary and proper" to execute the powers provided by the Constitution, while the Take Care clause requires the President to "take care that the laws be faithfully executed" (U.S. Const, art. I, §8, cl. 18; art. II, §3). The Appointments clause requires Senate consent for presidential nominations but empowers Congress to delegate appointment powers for subordinate officers to the President or heads of departments (or courts) (U.S. Const., art. II, §2, cl. 2). These provisions enable the creation of government bodies to execute the laws made pursuant to the Constitution.

Congress and the President may disagree as to which branch of government is the appropriate one to create or reorganize an agency (A. O'Connell, 2006, p. 1708, n. 309). Separation-of-powers principles will apply to this political struggle. Given that domestic intelligence is a national security function, the Constitution tilts the balance of power toward the President by virtue of the Commander in Chief clause (U.S.

Const., art. II, §2, cl. 1). Even so, intelligence agencies have been created and reorganized both by the President alone (through executive order) and by Congress with the President's signature (through statute). For instance, Congress created the Central Intelligence Agency (CIA) in the National Security Act of 1947, but President Harry Truman created the National Security Agency (NSA) via a classified memorandum (Pub. L. No. 235, 80 Cong., July 26, 1947, as amended, codified at 50 U.S.C. § 401 et seq.; A. O'Connell, 2006, p. 1709, n. 315). President George W. Bush created the National Counterterrorism Center (NCTC) by executive order, then Congress recreated it, altering its shape, in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (EO 13354, August 27, 2004; Pub. L. No. 108-458, December 17, 2004). IRTPA also created the DNI and ODNI, into which Congress placed the NCTC.

Should the President choose to issue an executive order creating a new domestic intelligence agency, there is some judicial precedent for interpreting the scope of the President's power to do so. An exegesis on the President's relatively broad powers in the national security arena is beyond the scope of this chapter, but we do note that the President would likely need to abide by the framework established in Justice Hugo Black's concurrence in the Supreme Court's decision in *Youngstown Sheet and Tube v. Sawyer* (343 U.S. 579, 72 S. Ct. 863, 96 L. Ed. 1153, 1952). Justice Black provided a tripartite test for presidential power to act by executive order, finding maximum presidential power where "the president acts pursuant to an express or implied authorization of Congress" (bolstered by the Take Care clause). The President has adequate power in "a zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain" (likely governed by "the imperatives of events and contemporary imponderables rather than on abstract theories of law"). Executive power is at its "lowest ebb" when the President "takes measures incompatible with the expressed implied will of Congress . . . for then he can rely only upon his own constitutional powers minus any constitutional powers of the Congress over the matter" (343 U.S. at 635–38; see also Masse, 2005, p. 2, n. 2).

Statutory Considerations

Efforts to create a domestic intelligence agency may be governed by what Garrett (2005) terms "framework legislation." Framework legislation governs how Congress, the President, or the executive branch may promulgate laws and rules in certain contexts. Regarding Congress, these laws "establish internal procedures that will shape legislative deliberation and voting with respect to certain laws or decisions in the future" (Garrett, 2005, p. 717). An example would be the Administrative Procedure Act, which creates procedures for administrative rulemaking.

The relevant piece of framework legislation for creating a domestic intelligence agency is the Reorganization Act of 1977, as amended (see 5 U.S.C. § 902 et seq.). The act empowers the President to reorganize the bureaucracy in certain ways, subject to congressional approval by joint resolution. Congress must consider the proposal on an expedited basis and approve or disapprove of the entire package without making changes to it (5 U.S.C. §§ 908–912).

The act allows the President to reorganize the bureaucracy in several ways:

> (1) the transfer of the whole or a part of an agency, or of the whole or a part of the functions thereof, to the jurisdiction and control of another agency;
>
> (2) the abolition of all or a part of the functions of an agency, except that no enforcement function or statutory program shall be abolished by the plan;
>
> (3) the consolidation or coordination of the whole or a part of an agency, or of the whole or a part of the functions thereof, with the whole or a part of another agency or the functions thereof;
>
> (4) the consolidation or coordination of part of an agency or the functions thereof with another part of the same agency or the functions thereof;
>
> (5) the authorization of an officer to delegate any of his functions; or

> (6) the abolition of the whole or a part of an agency which agency or part does not have, or on the taking effect of the reorganization plan will not have, any functions. (5 U.S.C. § 903(a))

Accordingly, the act allows the President to eliminate or consolidate agencies, but it does not allow the President to submit reorganization plans

> (1) creating a new executive department or renaming an existing executive department, abolishing or transferring an executive department or independent regulatory agency, or all the functions thereof, or consolidating two or more executive departments or two or more independent regulatory agencies, or all the functions thereof; . . .
>
> (4) authorizing an agency to exercise a function [that] is not expressly authorized by law at the time the plan is transmitted to Congress;
>
> (5) creating a new agency [that] is not a component or part of an existing executive department or independent agency; . . . (5 U.S.C. § 905(a))

The act accordingly distills the President's options for creating a domestic intelligence agency into two avenues. The first option is to submit a reorganization plan to Congress. This offers the benefit of expedited congressional review and no legislative tinkering, at the cost of limiting the type of agency to a nonindependent agency without cabinet status, and Congress could refuse to endorse the plan. Any change to the reorganized agency's power would have to be addressed in separate legislation.[3] The second option is to simply work with Congress to create an independent agency, possibly with cabinet status and adjusted powers, via the usual legislative process. DHS was cre-

[3] It might be possible for the President to create a new agency by a classified executive order, but this would be inadvisable. It might contravene the Reorganization Act, and it would certainly provoke a public furor when news of its creation and existence inevitably makes its way into the press.

ated through this latter option in the Homeland Security Act (HSA) of 2002.[4] Given the political contentiousness of domestic intelligence issues, the pendulum swing of public opinion toward the protection of civil rights and liberties, and the George W. Bush administration's efforts to expand executive powers, the second option would likely be more politically viable than the first.

Specific Legal Considerations

Should a new domestic intelligence agency be created—through whatever means—there would be several legal considerations to address. Many of these will have political ramifications among varying constituencies, and many will incur costs.[5]

Doing Business As: Procedural Business Concerns for a New Agency

Creating a new agency would present many of the basic legal issues that any new or successor organization would face. These will vary according to how an agency is created—from scratch, with some organizational units transferred from existing agencies, or entirely of transferred units. Property would need to be purchased or transferred from prior organizations; leases might need to be reexecuted. Contracts and ongoing business matters would need to be revisited. Litigation would need to follow the transferred units. Federal agencies have been created and reorganized many times in the past, so these experiences would need to be examined to help guide how these and many other legal tasks should be addressed.

---

[4] Such a statute may still require a reorganization plan, as did the HSA § 1502. The Reorganization Act's limitations on agency independence and powers could be offset by provisions in the statute creating the new agency.

[5] Despite the Reorganization Act's concern with efficiency and cost, reorganizations are expensive and do not appear to save significant amounts of money in the long term (5 U.S.C. § 901(a)(2),(3),(6), 2006; A. O'Connell, 2006, p. 1709, n. 317, citing Fisher and Moe, 1981, p. 306).

Leadership

The leadership structure of a new agency, especially one created in response to a crisis, attracts considerable scrutiny. As noted, the Constitution requires Senate confirmation for senior presidential appointments but allows Congress to delegate appointment of subordinate federal officials to the President or to heads of departments (U.S. Const. art. II, § 2, cl. 2). This raises separation-of-powers concerns. The Appointments clause does not provide neat guidance as to what types of roles are senior enough to demand Senate advice and consent. In practice, negotiations between the President and Congress would be necessary to resolve this if the agency is created by statute. If the agency were created by reorganization plan, since the Reorganization Act forbids the creation of new independent agencies, all officers would ipso facto be subordinate to the department head. Hence, such officers may not require Senate confirmation according to the Appointments clause, though the Senate might still demand confirmation.

The examples of the NSA and DHS are enlightening. NSA was created in a classified memorandum as a subordinate unit of DoD. No appointments to its leadership require Senate confirmation (although all receive routine Senate confirmation of their promotions to higher military ranks). Instead, the memorandum provides that "NSA shall be administered by a Director, designated by the Secretary of Defense after consultation with the Joint Chiefs of Staff" (NSC Intelligence Directive No. 9 § 2(c), Oct. 24, 1952, revised Dec. 29, 1952).[6]

Because DHS was created through statute as a new independent executive department, its top leadership must be appointed subject to Senate confirmation.[7] How much of its senior leadership would require Senate advice and consent was the subject of a separation-of-

---

[6] The directive further provides that "the Director shall be a career commissioned officer of the armed services on active or reactivated status, and shall enjoy at least 3-star rank during the period of his incumbency."

[7] There is a narrow exception to Senate confirmation of incumbents of reorganized units. If a new agency is created entirely or partly through reorganization and Senate confirmation is required for the leadership of reorganized units, Senate-confirmed incumbents of reorganized units need not be reconfirmed, even if there is a change in title, so long as the reorganized position involves the same or lesser duties (Marshall, 2005).

powers/checks-and-balances dispute. Members of the Senate opposed the first version of the HSA because it would have made less than half of the department's senior leadership subject to confirmation. The HSA as passed requires Senate confirmation of 22 of the 27 most senior members of the department.[8]

Beyond the power of appointments, the shaping of the leadership architecture itself attracts political attention because it speaks to power, accountability, and responsibility. Discussions of IRTPA and the commissions that inspired it focus on reorganizing the leadership of the U.S. Intelligence Community (IC), pointing to the importance of creating a new DNI who would not be distracted by running an agency and being the government's analyst-in-chief, as was the former role of the Director of Central Intelligence, and whose power would not be watered down by multiple layers of reporting authority between the DNI and the President (Treverton, 2005, p. 6; 9/11 Commission Report, 2004, p. 409). This impression was reinforced by requiring Senate confirmation for the DNI as well as for the director of the CIA (IRTPA, Pub. L. No. 108-458, 118 Stat. 3638, § 1011(a)). The powers of the leadership also attract attention, such as access to intelligence, the ability to share intelligence with others in the IC, and management powers over budget and personnel. These are discussed in the next section.

Agency Powers

As mentioned in the preceding section, discussions of creating a new domestic intelligence agency are intertwined with varying opinions on the current domestic intelligence system's success or failure at maintaining an acceptable balance between national security interests and civil rights and civil liberties interests. Hence, the scope of authority to conduct surveillance and other activities would likely occupy much of the political discussion of a proposed new agency. Without specifically discussing what a potential agency's powers might or should be, or

[8] Thessin (2003). HSA § 103(d) provides that the President can appoint the director of the Secret Service, chief information officer, chief human capital officer, chief financial officer, and Officer for Civil Rights and Civil Liberties without Senate confirmation.

comparing any such recommendation with the current structures and processes, we note that any changes to authority to conduct various domestic intelligence activities would have some relationship to how a new agency is created.

If a new domestic intelligence agency is created via the Reorganization Act, the new agency's powers must be identical to the sum of its reorganized parts (5 U.S.C. § 905(a)(4)). Separate legislation would be necessary to change the agency's powers. However, if the agency is created by statute, that statute may provide for expanded or constricted operational powers.

It is worth noting that molding the scope of a new agency's powers must be done with care. Lawmaking is an arduous process that is not easily revisited. The future utility of a new agency will be limited if the scope of the agency's operational and budgetary powers is too limited; if the place of the new agency within the overall framework of the IC is unclear or in conflict with the 16 existing IC agencies; and if the comparative authorities of the DNI, the leader of the new agency, the cabinet official into whose department the new agency might be placed, and the attorney general or FBI director for activities that are not transferred to the new agency are not resolved. These are lessons from the creation of the DNI, who controls only approximately 20 percent of the IC budget and has direct reporting authority over only one of the 16 IC agencies (the CIA), the rest of which are located in other cabinet departments (Dorschner, 2007; Hulnick, 2007; "Security," 2008). IC and executive branch officials and lawyers, as well as legislators, continue to devote significant efforts to expanding or limiting the DNI's authority (R. Best and Cumming, 2008; G. Miller, 2008).

Outside of statutory means, the President may exert considerable influence in shaping intelligence powers and practice. Many intelligence authorities were created by executive order, so the President could issue new orders to shape the agency's power (within constitutional and statutory bounds), no matter how the agency was created.

Agency regulations would follow reorganized units from their prior agency to the new agency, just as laws and regulations typically apply to successor agencies, but a new agency would have the power to conduct new administrative rulemaking processes. Any new admin-

istrative rules would, of course, be subject to the rulemaking process created by the Administrative Procedure Act and the limitations of the Constitution and governing executive orders and statutes. However, according to the doctrine of administrative deference created by the Supreme Court in *Chevron U.S.A., Inc. v. Natural Resources Defense Council*, courts would defer to the agency's interpretation of issues that its governing statutes fail to address or address ambiguously—so long as the interpretation is reasonable or otherwise legally permissible (467 U.S. 837, 1984).

Accountability

Whatever powers a new domestic intelligence agency may enjoy, keeping reins on the agency will be a primary concern. Accountability presents a challenge in any context, but it is a particularly difficult challenge in the context of national security. Accountability in government is often an aspiration pursued through some combination of internal management, inspectors general, internal and external audits, congressional oversight, transparency rules requiring disclosure to the public, personnel rules, and the threat of civil or criminal penalties. Accountability rules are generally designed to promote legitimacy and appropriate behavior. In the intelligence context, it is a commonplace that secrecy requirements limit the amounts and types of information that may be released to the public or specific governmental bodies (see, e.g., Sales, 2007; Bruce, 2004).

The political context that would most likely surround the creation of a domestic intelligence agency would make accountability a priority. Secrecy requirements limit transparency to the public through national security privileges and exemptions to sunshine statutes, such as the Freedom of Information Act.

Given that transparency to the public would be at best limited, in order to maximize public trust for such an agency, governmental accountability measures would need to be trenchant and visible. This might involve the creation of a strong or independent inspector general or ombudsperson. One critique of the HSA was the extent of discretion it gave the DHS secretary to limit inspector general investigations; another critique was sacking the inspector general for being critical of

DHS management (Stanhouse, 2004, n. 79 and accompanying text; B. Ross and Schwartz, 2004). Hence, there would be a need for an ombudsperson with significant autonomy.

Even if a strong, independent office of inspector general were created, it would still be an executive branch position. Checks-and-balances principles suggest that legitimacy and public trust might be promoted through robust congressional oversight. Ensuring that these principles are realized would require a hard look at that oversight.

Currently, congressional oversight of intelligence activities is spread across 17 committees (A. O'Connell, 2006, n. 26 and accompanying text). Any particular component of the IC or its activities usually falls under the jurisdiction of more than one committee in each house (A. O'Connell, 2006, n. 33 and accompanying text). This redundancy and competition in congressional oversight is well recognized. One of the 9/11 Commission's five major recommendations was "unifying and strengthening congressional oversight to improve quality and accountability" (9/11 Commission Report, 2004, pp. 399–400, cited in A. O'Connell, 2006, n. 38 and accompanying text). Specifically, the commission recommended that Congress either create a joint committee on intelligence modeled after the former Joint Committee on Atomic Energy or establish a committee in each house with the power to both authorize and appropriate for intelligence agencies and activities (9/11 Commission Report, 2004, p. 420). The WMD Commission (2005, p. 20) took a different tack, recommending that

> the House and Senate intelligence committees create focused oversight subcommittees, that the Congress create an intelligence appropriations subcommittee and reduce the Intelligence Community's reliance on supplemental funding, and that the Senate intelligence committee be given the same authority over joint military intelligence programs and tactical intelligence programs that the House intelligence committee now exercises.

The HSA (§ 1503) stated that it was the "sense of Congress that each House . . . should review its committee structure in light of the reorganization of responsibilities within the executive branch by the establishment" of DHS.

Though the occasional proposal for change has been forwarded, there has been little significant change. Anne Joseph O'Connell (2006, p. 1710 et seq.) attributes this to an unwillingness to give up turf. No change followed passage of the HSA other than the creation of *another* committee, the House Select Committee on Homeland Security, which features an Intelligence Subcommittee (Cohen, Cuellar, and Weingast, 2006, nn. 105–107 and accompanying text). The 9/11 Commission Report—and the political context surrounding it—prompted some change in the Senate, including promoting its Intelligence Committee to category A status with a new Oversight Subcommittee, establishing the Intelligence Subcommittee of its Appropriations Committee, and renaming the Governmental Affairs Committee to the Committee on Homeland Security and Governmental Affairs (A. O'Connell, 2006, pp. 1713–1714). Congress did not follow the 9/11 Commission's primary recommendations, however, as they would have involved considerable concentration of powers in a new joint committee or individual standing committee in each house (Grimmett, 2006, pp. 3–4; A. O'Connell, 2006). IRTPA provides no reorganization of the committee oversight structure, though it does focus some degree of DNI oversight in the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence.[9]

This review suggests that overhauling congressional committee oversight of domestic intelligence—described by the 9/11 Commission (2004, p. 420) as "dysfunctional"—is frequently discussed but rarely implemented. Should a domestic intelligence agency be created through statute, it will be a challenge to fashion effective oversight that the public perceives to be effective. Then again, O'Connell suggests that some degree of redundancy in committee oversight may provide benefits (A. O'Connell, 2006, pp. 1733–1734).

---

[9] Neither the House nor the Senate has a regular standing committee on intelligence. Select committees, typically temporary, usually have no legislative power (such as receiving or reporting on proposed legislation). Standing committees are permanent structures that are created by statute or the rules of the House or Senate (Davidson and Oleszek, 2004, p. 201). The House and Senate Intelligence Committees are hybrids (A. O'Connell, 2006, p. 1662, n. 27 and accompanying text).

Personnel

Federal laws create a complex web of human-resources and civil-service rules. If a new domestic intelligence agency is created by statute, those rules can be amended. The HSA provides significant leeway for a transitional five-year period to waive or modify civil-service protections. These include granting the DHS secretary flexibility in adjusting pay, performance evaluation, discipline, and employee appeals, and granting the President authority to exclude DHS from coverage under the Federal Service Labor-Management Relations Statute (HSA §§ 841–842; Thessin, 2003, n. 59 and accompanying text). Enabling such amendments to civil-service rules would create a complicated political balancing act between staffing flexibility and incentives on one side and labor relations on the other.

A new domestic intelligence agency would likely involve transferring the FBI's National Security Branch (NSB) or some of its parts to the new agency. Even if civil service protections were to be waived for the new agency during the transition period, these protections would still apply at the FBI. Forced transfers from other FBI units to the NSB, or denials of transfer applications out of the NSB into law enforcement units, in the lead-up to reorganization might lead to lawsuits based on employment law, civil rights, or retaliation provisions of the U.S. Code.

Conclusions

It is clear that the President possesses the power to create a new domestic intelligence agency, alone or with Congress. Should the decision be made to do so, several specific legal issues would arise, such as how to create the agency, how to empower it, how to staff it, and how to make it accountable. The political context of creating a new agency would likely determine how some of the legal questions would be resolved. Whether the agency would be granted greater, lesser, or the same surveillance powers as those possessed by the agencies that currently perform domestic intelligence operations, due care would need to be taken

in the architecture of leadership and accountability to promote the agency's legitimacy and the balance of security and liberty.

PART II

Exploring Different Approaches for Thinking About Creating a U.S. Domestic Counterterrorism Intelligence Agency

Describing the U.S. context in which a new domestic intelligence agency would find itself and exploring the types of models for such an agency that can be found abroad can contribute to considering the pros and cons of creating such an agency in the United States. While such descriptive and comparative information can provide a foundation, however, it is not enough to suggest the "right answer"—if such an answer even exists—for public-policy decisions. Indeed, because of the interplay of interests and views both of the threat of domestic terrorism and of the tangible and intangible costs associated with government surveillance and other intelligence activities domestically, balancing the considerations that are involved in deciding whether a new intelligence agency is in the national interest is difficult. Moreover, informing policy debate requires more than simply descriptive information.

To explore different ways of thinking about the policy choice of creating a domestic intelligence agency, another element of RAND's research effort focused both on the options and choices involved in building such an organization and some ways of thinking about the costs and benefits of doing so. The chapters in this section therefore examine four areas:

- The first chapter examines different organizational models for what a new domestic intelligence agency could look like. In policy debate, those words have been used to describe a variety of changes in the structure of government and intelligence policies. Informed debate requires being clear about what is meant so that

deliberation is not confused by use of the same words to mean different things.

- The second chapter examines different organizational, policy, and technological options for carrying out intelligence missions while protecting individual privacy and civil liberties. While the tension between improving security and such intangible values is often viewed in shorthand as a trade-off, this discussion seeks to break out of that tendency and think through available ways to pursue both simultaneously.
- The third chapter explores how to think about developing measures or metrics for domestic intelligence activities, including measures of both what policies are trying to accomplish and the elements that shape public acceptability of intelligence activities. Using metrics to guide improved performance in the public sector has become a focus in many areas. While their application in intelligence is problematic for many reasons, the structured thought involved in considering ideal metrics for domestic counterterrorism (CT) activities can be useful in thinking through the otherwise abstract trade-offs that must be made in crafting security policies.
- Finally, and most speculatively, the last chapter in this section explores the application of a technique normally used in regulatory analysis or studies of the costs and benefits of more-traditional government programs to thinking about changes in domestic intelligence policies. We use cost-effectiveness analysis to frame questions about how effective a new domestic CT intelligence agency would have to be for its benefits to justify its costs—not just the resources involved in creating it, but much less tangible costs associated with its effect in such areas as personal privacy and civil liberties. Like our exploration of metrics, these techniques do not produce a final answer on the value of creating a new domestic intelligence agency but provide an additional way in which to structure thinking and debate.

CHAPTER SIX

Weighing Organizational Models for a New Domestic Intelligence Agency

Genevieve Lester and Brian A. Jackson

Throughout most of the chapters in this volume, the creation of a new domestic intelligence agency has been treated as a singular action, and many of the practical details of what creating such an agency might mean have been left unexplored. In this chapter, we explore several alternative design options for how a new agency could be organized. The discussion addresses structure, institutional characteristics, and fit with the specific U.S. intelligence and law enforcement context.

Some scholars have used insights from organizational-theory literature to assess how well intelligence organizations have adapted their missions and mandates to absorb the requirements of the dynamic, post-9/11 security environment (Zegart, 2007, 1999).[1] Others have applied organizational concepts drawn from engineering, risk analysis, and safety to issues of intelligence and homeland security (Sagan, 2004; *Risk Analysis*, 2007). In this chapter, we build on these efforts by applying organizational and public-administration concepts to the problem not only of adapting existing organizations but also of potential *creation* of an organization in the domestic intelligence arena.

A discussion of all of the organizational and management options applicable to the design of a domestic counterterrorism (CT) intelligence agency could proceed in multiple directions—as we have seen in the media—and potentially run to thousands of pages. We limit our discussion here to a snapshot of what we consider the most salient ana-

[1] The classic text that provides the analytical basis for these assessments is Allison (1971).

lytical and design issues, in terms not only of the greater discussion but also of the particular focus and requirements of this volume.

Organizational Design and Domestic Intelligence

The current domestic intelligence system in the United States is highly decentralized. As was described in Part I, a RAND effort to map domestic intelligence activities using open-source information identified a wide variety of efforts by many organizations across levels of government and in the nongovernment and private sectors. In assessing current activities and exploring what might change if a new domestic agency were created, we used a set of five domestic intelligence capabilities to enable us to capture the primary requirements for successful CT intelligence:

- collection capabilities for gathering information
- analysis capacity to identify and assess the data
- storage to retain relevant information for future use
- information-sharing and transfer mechanisms to move either raw collected data or analytical products to the individuals and organizations that need them
- capability, authority, and willingness to act on the information.

Currently, U.S. domestic intelligence capabilities are spread across many organizations. As a result, success in preventing terrorism depends not just on the performance of individual organizations, but also on how the entire system works together. In response to this structural dynamic, a variety of recent reform initiatives have focused on increasing information-sharing, interoperability, and communication between agencies, as well as the fusion of intelligence and law enforcement information between agencies and levels of government (see Chapter Three).

The creation of a new domestic CT intelligence agency could be a departure from the current approach to domestic CT efforts. How significant a departure it would be, however, depends on exactly what is

meant by "creating a new intelligence agency," since the apparent simplicity of that statement obscures the fact that it could refer to any one of a range of possible policy actions. A new agency could be structured in an almost unlimited number of ways, depending on—among many factors—the organizational objective driving formation of the agency. For example, its organization could differ depending on whether the new agency would be intended to be additive (e.g., a new organization intended to supplement the intelligence structures currently in place) or transformative (involving substantial reorganization or elimination of some or all of the current domestic intelligence system). Any of the design alternatives mentioned here would, at a most basic level, require choices regarding which functions (collection, analysis, data storage, information-sharing activity, and authority and capability to act) would be centralized within the new structure.

On a more detailed level, specific organizational properties could be emphasized to a greater or lesser degree depending on which organizational model is chosen for the new agency, or even if a combination, or hybrid, of models were chosen. For example, some designs put emphasis on gauging and reinforcing the resilience and adaptability of an agency or of the overall national domestic intelligence effort, particularly in terms of response to the dynamics of emerging threats. Other designs could focus more heavily on transparency than secrecy, emphasize linear efficiency more than resilience, or value centralized organization more than diversity and regional-level fusion initiatives. These are just a few of the possible characteristics that would have to be considered when assessing how a potential agency should be organized.

To gain insight into the feasibility of a domestic CT agency, we explored a range of organizational and structural options. First, we looked at three options that would require subordinating an agency to a current organization. As potential sites for the new organization, we examined the Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), and Department of Homeland Security (DHS), respectively. Second, to push this analysis further and explore the implications of different design choices, we constructed a set of idealized models of what a newly created agency might look like and how much change in the current domestic intelligence enterprise (Figure 3.1 in

Chapter Three) might be involved in its creation. The intent of these models is not to present them as actual options for consideration but rather to use them as heuristics to guide thinking. The models are a conceptual exercise to help us explore the salient analytical characteristics that each potential alternative structure would affect.

As a final note of context, the purpose of this type of analysis is not to add unnecessary complexity to the current discussion but to explore the implications of the wide range of organizational-reform proposals that have been suggested since 9/11. Organizational reform tends to be viewed as a simple and politically acceptable solution to perceived failures in performance, one that can assuage a range of critics immediately. Organizational change is, however, much more complex than it can seem at first glance (Posner, 2006, p. 105; see also Betts, 1978). The outcome of changes undertaken since 9/11 has so far been somewhat ambiguous, and organizational reform tends, generally, to atrophy over time.[2] Further, reform tends to focus on short-term and immediate concerns. The analysis in this chapter extends the time frame, describing short-term constraints and effects as well as exploring how different possible designs of a new agency might adapt and change over time.

Adapting the Status Quo

While introducing an entirely new agency dedicated to domestic CT intelligence is one option, some proponents of domestic CT intelligence reorganization argue that an effective approach to streamlining domestic intelligence activities would be to create a domestic intelligence service within an existing agency. The most relevant options could include placement within the FBI, CIA, or DHS.

Federal Bureau of Investigation

Placing an agency within the FBI has been the subject of much discussion—due mainly to the fact that many insiders consider this option to be a straightforward and potentially cost-effective approach.

---

[2] Atrophy concept drawn from the work of Richard K. Betts, particularly Betts (1978).

The FBI currently has responsibilities for criminal law enforcement, domestic CT, and domestic counterintelligence (Richelson, 2008, p. 158). With the significant post-9/11 changes in its mission and activities, the FBI is the primary locus of domestic CT intelligence activities in the United States. Thus, it is argued that the FBI could easily take on enhanced domestic CT intelligence responsibilities that would be associated with creating a new agency within the FBI. According to the argument, enhancing domestic CT intelligence capabilities would be a mission refocus but could still be somewhat less disruptive than other options to the FBI's other activities[3] and the intelligence community's (IC's) CT mission as a whole (Posner, 2006, p. 94).

There is a range of ways that this service could be designed within the FBI. Probably the most realistic option would be to unite all FBI personnel dealing with international CT, foreign counterintelligence (CI), and security countermeasures into a service that would report to the director of the FBI and, through the director, to the attorney general (Cumming and Masse, 2004). The focus would thus be on continuity—both through the use of existing personnel and structures and through the continued relationship with the attorney general, intended as that relationship would be to assuage civil liberties concerns.

This model could also help tighten the link between federal, state, and local intelligence operations by reinforcing the relationship between a centralized analytical hub and the numerous spokes (or decentralized components)—the joint terrorism task forces (JTTFs) and field-office intelligence and law enforcement activities—that constitute the FBI structure (Cumming and Masse, 2004). Opponents of this proposal could argue that law enforcement and domestic intelligence should be separated, allowing both to flourish in dedicated environments and reinforcing the demarcation of responsibilities, given real civil liberties concerns. The argument against placing such a new organization

[3] Such concerns would presumably be parallel to those that have been raised about the FBI's CT activities crowding out other law enforcement activities (Shukovsky, Johnson, and Lathrop, 2007). See also FBI (2008, p. 4-123) and Goodwin (2004). A similar trend can be observed, albeit in an international context, for participation of MI5 in the United Kingdom in criminal investigations (Fidler, 2006).

within the FBI also rests on the view that the professional cultures of intelligence and law enforcement do not mesh easily. Law enforcement's case-based, retroactive approach clashes with the sweeping, preventive, and longer-term activities of the IC (see Posner, 2006; Treverton, 2003; Sims and Gerber, 2005). The post-9/11 changes made by the FBI have been aimed directly at meshing law enforcement and intelligence activities, though it is not clear whether the concerns that have been voiced by outside observers have been fully overcome.

A moderate variation of this suggestion was taken up by the WMD Commission, which stated among its recommendations that a National Security Branch (NSB) should be created within the FBI. The service was to include the FBI's CT and CI divisions as well as the Directorate of Intelligence. In response to these recommendations, this service was created from three FBI divisions on September 12, 2005, in accordance with the provisions of the Intelligence Reform and Terrorism Prevention Act (IRTPA) (Richelson, 2008, p. 159). The NSB currently contains the Counterterrorism Division, Counterintelligence Division, Directorate of Intelligence, and WMD Directorate. The NSB is not entirely focused on the mission of CT, however, as the Directorate of Intelligence continues to be responsible for ordinary criminal intelligence as well as national security intelligence. Both the CT and CI divisions also still have law enforcement responsibilities.

To link the FBI's new CT intelligence mission more closely to the IC, the Director of National Intelligence (DNI) has budget authority over the FBI's national intelligence activities. The DNI also has specified authority to concur in the appointment of the executive assistant director for the NSB (EAD-NSB) (FBI, 2006a). While the change has marked a step in the direction of streamlining domestic intelligence, it does require both the CT and CI divisions to maintain their current structures, responsibilities, and, importantly, their conduct and management of investigations into CT and CI.

The changes that the FBI has made since 9/11 are part of the argument that creating a broader domestic intelligence effort within the FBI would be more straightforward and cost-effective. However, the extent of the success of the efforts to change the FBI's focus to prioritize

the intelligence mission among personnel is not yet entirely clear.[4] For example, Field Intelligence Groups (FIGs) have been introduced to the FBI field offices not only to guide the intelligence cycle on a regional level but also to imbue the offices with an increased sense of the intelligence mission. But questions have been raised about how effectively the FBI and other law enforcement organizations have been building and using intelligence-analysis capabilities (see, e.g., DOJ Audit Division, 2007; DOJ OIG, 2005a, 2005c). The same concerns mentioned earlier about case-based focus and divergent collection cultures as well as underspecialization due to the mesh of law enforcement and intelligence missions are prevalent in this discussion. On a more theoretical level,

> [w]hile it is easy enough to change the formal architecture, it certainly takes real time to change the set of people in the firm and the networks among them, to redefine the fundamental beliefs they share, and to induce new behavioral norms. Yet these may be the most important elements to the realization of the strategy. (Roberts, 2004, quoted in Posner, 2006, p. 36)

The shifts that have already been made at the FBI would certainly be steps in the broader process involved in creating a more autonomous domestic intelligence agency within the FBI. The full extent of those changes—i.e., how much additional change would be required to actually create a new agency under the FBI—remains an open question for outside analysts and observers.

Central Intelligence Agency

A second organizational suggestion is to place a new domestic CT intelligence agency under the CIA's purview. The rationale for this approach is the argument that combining domestic and foreign intelligence operations could mesh operational cultures effectively. One of the most persistent arguments against the FBI's role in domestic intelligence has been this idea of professional cultural dissonance between

[4] For example, discussion in October 2007 congressional hearings reported in M. Johnson (2007).

its law enforcement and intelligence roles. Separating domestic intelligence from its law enforcement role and subordinating it to the purview of intelligence professionals could be a solution.

In this context, the domestic and foreign intelligence analysts would be able to share information effectively—the wall thought to stand between the two disciplines and sets of organizations would not exist almost by definition, and analytical personnel with similar skill sets would be colocated and empowered to act together.[5] Information-sharing—seemingly the mantra of the post-9/11 world—would be facilitated, as would more centralized and integrated information storage (Jervis, 2006, p. 6). Finally, the traditional structures of congressional oversight could be applied to the new, combined organization, responding to fears that a domestic CT intelligence agency withdrawn from U.S. Department of Justice (DOJ) responsibility would not be appropriately accountable or fully observant of the legal constraints on domestic intelligence activities.

Having said all this, there is probably no more controversial choice on the entire spectrum of alternatives than involving the CIA in explicitly domestic CT intelligence activities.[6] At a very basic level, public perception of the nature of the CIA's clandestine operations and the recent controversy regarding extraordinary rendition and CIA prisons would likely exacerbate public fears regarding potential domestic intelligence abuses. Recalibrating perceptions of operational activities in a domestic context would require reforging the CIA's charter in the public eye. It would require commitment to building and reinforcing public trust, credibility, and accountability through more openness and transparency than what is generally associated with foreign intelligence activities. It could be very difficult to create a domestic intelligence subunit that would be transparent enough to address fears of CIA operations based on historic abuses, semicurrent horror stories, and the eternal

---

5 *The wall* refers to the legal restrictions on sharing information across the line between intelligence and law enforcement.

6 The comments of John MacGaffin (2003), formerly of the CIA, are illustrative: "[I don't], and wouldn't for a moment, think the CIA should do [domestic intelligence]. It would be a terrible idea within the United States."

myths that fill the gap created by secrecy (see also Chapter Four) while maintaining the security needed for effective intelligence activities.

U.S. Department of Homeland Security

The third organizational alternative, creation of a subunit of DHS, introduces its own challenges. On the one hand, it makes a great deal of sense to subordinate a domestic intelligence agency to the newly created agency, which already has the function of combining most efforts on homeland security and preparedness. DHS currently possesses analytical capabilities that could be transferred to domestic intelligence efforts—including intelligence and analysis, risk analysis, and threat assessment efforts, such as its Homeland Infrastructure Threat and Risk Analysis Center (HITRAC). Further, a domestic intelligence agency could forge links with the intelligence components of the other DHS subunits, such as U.S. Citizenship and Immigration Services (USCIS) and the U.S. Coast Guard (USCG).[7] These ties could be invaluable in the information-sharing community that is the focus of many post-9/11 intelligence-reform endeavors.

One of the assumptions of this approach would be that intelligence would be separated from law enforcement capabilities, though the range of law enforcement roles carried out by DHS subunits would mean that this was not a certainty (see, e.g., U.S. House of Representatives Committee on the Judiciary Subcommittee on Crime, Terrorism, and Homeland Security, 2004). A culture of prevention could meld well with the culture of intelligence (Posner, 2006, p. 12). DHS membership could therefore solve some problems but could also introduce others: How would the necessary relationships be built that would allow the new agency collection capability were it to be subordinate to DHS? What relationship would be built with law enforcement organizations outside the agency? What would the timing be in terms of handing cases off to a law enforcement agency? It is feasible to think that DHS could be more adaptable to a new mission. The agency itself is an innovation, and, as its mandate was developed in the wake of the attacks on 9/11, one of its core missions is preventing terrorism. A less

[7] Aspects of this argument are drawn from Posner (2006).

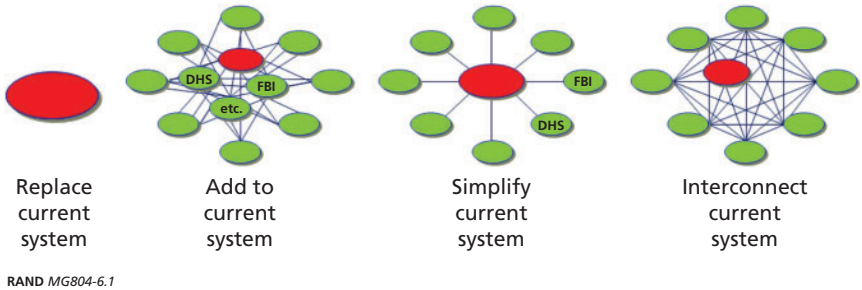
entrenched organization, such as DHS, could potentially be both more adaptable and more resilient in the face of emerging threats than the somewhat rigid post–World War II creations of the FBI and CIA.

On the other hand, the creation of DHS has demonstrated how complex the forging of a hybrid organization out of multiple agencies can be. While certainly possible, the costs have been enormous, and the process has not been smooth. Some of the failures of the current subunits within DHS, especially the Federal Emergency Management Agency's (FEMA's) response to Hurricane Katrina, have raised major questions about the department's effectiveness. Further, meshing cultures to break down stovepipes has been problematic, so it is unclear whether a domestic intelligence agency would be able to benefit from information-sharing and coordination implicit in the suggestion to place it within DHS. A domestic intelligence agency would be inserted into this fray and would have to scramble for funding and attention in competition with the disparate agencies and subcomponents that already make up the department (Posner, 2006, p. 124).

Alternative Models for a Domestic Counterterrorism Intelligence Agency

Having discussed briefly the options for subordinating a potential domestic intelligence agency to an existing IC entity, we now discuss alternatives for creating a stand-alone domestic CT intelligence agency. In our analysis, four general, idealized models were considered and are illustrated in Figure 6.1. The models help us explore the salient characteristics that each potential alternative structure would affect. In the figure, the options for a new domestic intelligence agency are presented as stand-alone organizations—that is, each model has its own bureaucratic structure, hierarchy, and institutional culture and would not be part of a cabinet-level agency. Finally, we have differentiated the models from one another somewhat artificially. As we describe later, some characteristics of each overlap with each other. As mentioned previously, the value of such models is highlighting different

Figure 6.1
Idealized Models for a New Domestic Intelligence Agency



organizational characteristics that might be associated with alternative ways of creating a new agency, rather than as distinct options for doing so.

Replace the Current System

Other chapters in this volume have explicitly pointed out that policymakers do not have a blank slate for creating a new domestic intelligence agency, given new and legacy efforts (see Chapter Three). That said, the simplest model for a new domestic CT intelligence organization would be to wipe the slate clean of current activities and attempt to build a single entity consolidating all of the capabilities needed to pursue the mission of domestic CT intelligence. This proposition is somewhat difficult to conceptualize, given the currently highly complex and interconnected domestic intelligence enterprise. In this hypothetical case, all domestic CT intelligence activities would be centralized, and this agency would handle all aspects of domestic CT intelligence issues internally. This would entail, ostensibly, conducting the entire set of intelligence activities described earlier, from collection to action. Centralization would require a robust hierarchical bureaucracy and close relationships with regional and local structures. The agency's relationships with other federal-level agencies would be lateral and ongoing, rather than sequential—for example, there could be collaboration with the CIA on joint domestic/foreign intelligence issues, but there would no longer be a need to hand off information to a law

enforcement agency as the final stage of an intelligence investigation. The entire process could occur internally.

This model is unworkable on a practical level for a variety of reasons, not least of which is that the many organizations that would have to be subsumed to provide it with the full suite of needed capabilities would, in many cases, still be necessary to other non-CT missions. An example of this would be law enforcement capability, since arresting and prosecuting individuals is a key element of acting on intelligence to prevent terrorism. In this hypothetical extreme, an entirely centralized domestic intelligence agency would need to be able to act on intelligence throughout the country, implying that it would contain the equivalent of policing capabilities from the federal level (e.g., subsuming the FBI) to the state and local levels. Though centralization focused on this single mission would simplify domestic CT intelligence considerably, it would neglect the range of other law enforcement roles such agencies have that have nothing to do with CT. As a result, it provides an illustration of both the limits to how much could practically be centralized and the difficulty in teasing out CT domestic intelligence activities from these other, related missions in the context of either building a new agency or reorganizing current ones. Such a fully centralized model would also be inconsistent with the U.S. federal system of government and, as the disruption associated with the founding of DHS demonstrated, would have enormous financial and practical transaction costs if attempted.

While easy to dismiss as a design option for practical reasons, on a conceptual level, a fully centralized model is useful for analytical purposes because it highlights several key issues. Centralizing some domestic intelligence activities could be an attractive approach to helping to address some of the larger challenges facing intelligence operations. Centralization could help streamline the process of gathering and processing intelligence, cutting down on task overlap and duplication with other agencies or components. The process could be made efficient and cost-effective by minimizing redundancy. Further, centralization and bureaucratization can introduce standard operating procedures that can smooth and improve the efficiency of domestic intelligence processes and address some of the problems of consistency

that have been raised about current efforts. In theory, the positive elements of hierarchy, bureaucracy, and division of labor could be fully utilized—in this case, linear processing, efficiency, and straightforward pathways for communication and authority.[8]

Centralization of operations would also make oversight more straightforward, since a more limited and focused structure can oversee the entirety of the nation's effort. Bureaucratic centralization can provide a focal point for responsibility and thus a direct mechanism for accountability. A centralized domestic intelligence agency could make use of oversight mechanisms similar to the ones in place now; wide-ranging structural innovation would not be required.

Information-Sharing. Information-sharing in this model would become an issue of intra-agency information-sharing rather than the frequently more difficult interagency variety, with its many difficulties of procedure, software, document classification, and uneven relationships among information sharers. Centralization would also allow resources to be concentrated; at least theoretically, the most effective leadership and best qualified personnel could be brought together. This contrasts with the current system, in which many independent organizations must be staffed, given resources, and coordinated with their appropriate counterparts. Centralization in this context can make it possible to impose consistency and quality control on activities. This can help maintain uniform quality of collection and analysis because centralized storage facilities can purge incorrect or inappropriately collected data.

Adaptability and Change. While, as has been proven historically, there can be many benefits to centralizing intelligence efforts, there are, quite obviously, also drawbacks. Consistency can be a *weakness*, particularly when the goal of the organization is to address a dynamic threat that changes over time. The centralized bureaucratization and hierarchy that could offer efficiency could also limit institutional adaptability and resilience, as well as hinder the incorporation of alternative analytical perspectives (Wilensky, 1967, p. 58).

---

[8] Frederickson and LaPorte (2002). This argument also draws from the classics of Max Weber (see, e.g., Weber, 1947).

On a broader organizational level, adaptability or change tends to be a function of how porous the borders of that organization are (Scott, 2002, p. 123)—for example, how open is the organization to external input, and how does it react to this information? In the context of intelligence, this could include a range of inputs, from consumers to members of Congress responsible for oversight to the public to the countermeasures required in response the threat itself. A fully centralized domestic intelligence agency would not require openness to other organizations in terms of work product—it would be fully contained. This could, thus, raise questions about transparency and could affect institutional learning and change.

Transparency and Public Perception. Openness is not a characteristic often or conventionally ascribed to organizations carrying out the intelligence mission. Protection of information is a functional necessity when it comes to guarding the technical core of any enterprise, but it becomes even more central when it comes to guarding classified and sensitive information with security implications. As organizational theorist W. R. Scott (2002, p. 123) points out,

> Organizations construct and reconstruct boundaries across which they relate to the outside world. Between the outside world and those outside there is not one barrier, but many, and for most kinds of organizations these barriers become higher and more impenetrable as we come closer to the organization's technical core.

While difficult to predict a priori whether it actually would, by providing the ability to more consistently impose security and other restrictions, centralization could also reduce the transparency of national domestic intelligence efforts.[9]

Although intelligence reorganization is less of a trenchant issue in terms of public opinion, a fully centralized domestic intelligence agency—depending on how it was portrayed—could stoke public

[9] This potential reduction in transparency could mitigate potential benefits in terms of public acceptability that might be gained by more-centralized oversight of intelligence activities.

anxieties about a potential increase in invasive measures (for example, surveillance). This could be the case particularly if it were perceived as opaque, inaccessible, and not minded by appropriate oversight. Whether these concerns were reasonable would be borne out by how the agency was run—e.g., greater centralization could make oversight more straightforward and, by limiting the diversity inherent in a complex and decentralized system, increase transparency. While quite clearly unrealistic, this model highlights issues of centralization efficiency that could contribute to the mission of domestic CT intelligence. It also marks an end-of-the-spectrum state that can serve as an indicator for other, less extreme versions of centralized domestic intelligence efforts. One such option is introduced in the next section.

Add to the Current System

From a bureaucratic perspective, the simplest *path* for forming a new domestic intelligence organization would be to add a new domestic agency on top of the existing intelligence, law enforcement, and homeland security community. This model would introduce an agency primarily responsible for domestic CT intelligence, but it would not affect or remove components of any of the agencies that exist in the current system. The agency would be stand-alone and would have its own budget, leadership, and bureaucratic structure. It would also have its own analytical personnel, who would be recruited and trained entirely vis-à-vis the work of this agency. The idea to just drop a whole new agency into the already complex domestic intelligence enterprise (Figure 3.1 in Chapter Three) is unrealistic for a different set of reasons than attempting to drastically simplify that system as discussed earlier[10] but is similarly useful for analytical purposes.

In contrast to the fully centralized agency described in the previous section, a question raised by this model would be which capabilities would be included in this new organization (versus those that already exist in other organizations with CT missions or activities)

[10] Though this model might seem easy to dismiss out of hand as impractical, individuals with whom we spoke expressed the concern that, in reaction to a future terrorist attack, a new agency might be established precipitously, creating just this situation.

and how the relationships to current efforts would be established. This federal-level agency could be a central hub for domestic CT intelligence activities and could be responsible for maintaining relationships with organizations at the state, regional, and local levels. It could be configured in numerous ways, and we do not explore each possibility here. We, do, however, unpack what we view as a fundamentally important issue when we address the controversial question of whether the law enforcement function should be separated from the domestic intelligence responsibility. This issue has arisen in terms of subordinating the new agency to current law enforcement institutions, such as the FBI, and is salient to questions of how to design an entirely new, additional agency.

A concrete example that could illustrate some of the characteristics of this conceptual model is the National Counterterrorism Center (NCTC). The NCTC was added to the IC in 2004 to provide a central IC organization for operational planning and joint CT intelligence analysis (see Masse, 2004, 2005). Staff drawn from at least 10 intelligence agencies are colocated at this center, including large segments of the CIA's Counterterrorism Center and the FBI's Counterterrorism Division, with the intention being that *issue* focus and joint collaboration can strengthen CT operations by bringing a wide range of intelligence tools and disciplines to bear on the problem of terrorism (Masse, 2004, 2005). This change created a new entity in the overall CT intelligence system, though it should be noted that the creation of an entirely new agency focused on domestic intelligence would be a much more substantial addition than was the case in creating the NCTC.

Institutional Responsibilities and Culture. The addition of a new agency would allow for the creation of an entirely new institutional culture, one not affected by the mores of the entrenched national security and intelligence organizations, trying as they are to adapt to the post-9/11 environment. With a coordinated mission, advancement based on mission-specific goals, and training and leadership focused on the CT mission, the bureaucratic clashes of joint law enforcement/intelligence operations could be avoided. However, though creating a new agency within the current enterprise would provide the opportunity to build a purely domestic intelligence culture in the organization, to be effective,

it would have to have strong relationships with both law enforcement and other organizations that already exist.

With law enforcement separated from intelligence, procedural relationships would have to be established. All of the same questions of boundaries would still exist and on multiple governmental levels. For example, when would a case be passed on to the appropriate law enforcement body? How would intelligence sources be protected? How would jurisdiction be defined? Would cases be passed on only to other federal-level law enforcement, or would the new agency deal directly with regional and local agencies? The direction of these relationships is not just an academic point: The efficacy of this new agency would be contingent on the smoothness of these relationships. If smooth flows of information are not established, the new agency would simply add another stream of information and another bureaucratic culture and would not add any value in terms of focus or expertise to the IC at large.

Changing culture through combining representatives from a range of agencies is an effort fraught with complications. For example, the mix of agency cultures within the NCTC has not been entirely successful at producing a blended environment, a problem exacerbated by the fact that the staff detailed to the NCTC operate under their own home-agency authorities and thus are not truly integrated into a new agency (see Masse, 2005). A key piece of effectiveness in this model would be personnel-related: establishing recruitment and training programs focused on gathering new analytical staff and training them in the particular culture and mission of the additive agency.

Duplication and Redundancy. While a new agency would add the benefits of mission focus, dedicated bureaucracy, and a culture that could develop around the mission of domestic CT intelligence, this new agency could add problems of duplication to the existing IC. Duplication is a complicated concept in this context: It can add problems in communication and efficiency and complicate current problems of turf wars and competition over scarce resources. It is generally argued in organizational-theory literature that redundancy is negative and leads to waste and inefficiency (Landau, 1969, p. 348). On a policy level, duplication can slow down the decisionmaking process when policy-

makers are forced to pore through multiple variations of—in many cases, similar—recommendations.

On the other hand, in the context of intelligence analysis, duplication can aid accurate decisionmaking by allowing the policymaker access to a range of opinions and assessments. For example, if agencies are expected to challenge each other's analyses, they can tease out, explore, and weed out faulty assumptions that would otherwise get tunneled to the top of the decisionmaking process when there is no external criticism.

Duplication, or redundancy—viewed through the lens of the traditional safety measures derived from engineering practices—can serve as a fail-safe in the high-stakes world of security and homeland defense. Duplication or redundancy can have a range of benefits—for example, to the safety of engineered systems, such as aircraft carriers, automobiles, or nuclear reactors. Systemically, redundancy can reduce the pressure of possibly having to perform despite accident or failure. Redundancy "accepts the inherent limitations of any organization by treating any and all parts, regardless of their degree of perfection, as risky actors" (Landau, 1969, p. 350). Key to the assumptions underlying this argument is the fact that the parts of the system must be independent of one another so that the failure of one does not impede the effective operation of another. It could thus be argued that duplication and redundancy could assist with reliability, adaptability, and resilience in response to breakdown or—in the case we are discussing here—emerging, dynamic threat.

Unfortunately, there are broader negative aspects to redundancy and duplication. Duplication or redundancy can cause other organizational problems, such as shirking responsibility or the diffusion of responsibility leading to no one, in fact, getting a job done (Sagan, 2004, p. 940). An extension of this argument points to the problem of overcompensation as a potential outcome of redundancy (Sagan, 2004, p. 944). While this can mean risky behavior for an individual, in the context of an intelligence agency, it could engender sloppy work. If simply adding a new agency to the system is seen as a cure-all, other necessary IC reforms may not be taken seriously or undertaken at all.

Information-Sharing and Coordination. In thinking about how implementing such a model might affect key challenges for domestic intelligence, the value of simply adding an agency to the current system is not clear. On an information-sharing level, while an additional hub for information transfer might increase the chances of information flowing, it also creates opportunities for disagreement, requiring that organizations that receive information from multiple sources (e.g., local police forces connected to more than one hub organization) deconflict the data streams. While duplication can help keep a system from failing entirely, the existence of parallel systems operating in multiple organizations also creates the potential for information-sharing failures. The existence of data systems in multiple organizations makes it more difficult to track down erroneous data and to keep the amount of data in the system about members of the general public within acceptable bounds.

Oversight. The existence of multiple, parallel (potentially duplicative) activities may also complicate oversight, as new oversight pathways and responsibilities would have to be established and made credible and efficient. The creation of an additional agency could increase the responsibility of the current congressional-oversight bodies or require a new institution to take responsibility for overseeing the new agency's activities. Considering how long and complicated the process was to institute the House and Senate Permanent Select Committees on Intelligence in the 1970s, there is little optimism that an appropriate mechanism could be established that would instill public trust and command the appropriate level of respect and credibility from the new agency's leadership.

Simplify the Current System

The formation of a new domestic intelligence organization could focus on simplifying the complexity of the current IC and providing a more centralized focus of activity for domestic CT activities. Similar to the logic that underpinned the creation of DHS, the argument for simplification would be that taking domestic intelligence activities that are ongoing in multiple organizations (see Figure 3.1 in Chapter Three) and combining them into one could be beneficial. The implications of this

model are perhaps the most ambiguous of the hypothetical alternatives discussed here. Much of the success or failure of such a model would depend on the entities incorporated into the new agency as well as the degree to which the new agency had responsibility for each component of the intelligence cycle. The simplification model would make the new agency the core of the domestic intelligence effort but could preserve related roles for other, existing organizations. Once again, decisions would have to be made about the full scope of capabilities that would be centralized in the new agency as well as to what degree they would be integrated into it.

For the most centralization, the domestic CT intelligence functions of existing agencies could be reassigned to the new agency.[11] Alternatively, more-modest implementation of this model could transfer some current domestic intelligence functions to the new agency but provide it only influence rather than full control over the remainder. For example, analysis, data storage, and responsibility for information-sharing might be vested in this single hub organization, but it might still have to rely on others—such as regional organizations—for information collection and operational capability.

Simplification could help reduce bureaucratic bloat through increased linear efficiency and hierarchical organization. It could streamline activities and reduce duplication. It could also focus activities on an issue area, much like the NCTC does, by colocating the personnel and information relevant to the domestic CT intelligence mission. However, the challenges encountered in forming DHS—the most ambitious similar effort in recent years—underscore the potential costs and disruption involved in such a simplification effort.

Information-Sharing. By providing a central actor for domestic intelligence activities, this model could offer the opportunity to impose some consistency in the actions of other organizations in the system. The central hub organization could theoretically act as a filter for information shared through it to ensure quality and consistency and limit the amount

[11] Taken to the extreme, simplification of the current domestic intelligence enterprise could be essentially the same as the hypothetical path of fully replacing the current system described earlier.

of conflicting information passing through the system. The central node could serve as a point for oversight of the entire system, potentially helping to balance competing national values. Conversely, if the action of the central hub creates an unproductive chokepoint for information-sharing, it could degrade the effectiveness of the entire system.

Other strengths and weaknesses of this type of model depend on how much consistency of action and centralization the hub agency creates. To the extent that the spoke organizations collect, analyze, or act on information differently, there will be diversity in how the system parts function. This diversity could be a strength in responding to adaptive adversaries as previously discussed in relation to other models, informing intelligence activities with local knowledge and insight, and producing a layered intelligence defense from the diverse efforts across the nation. However, it could also be negative if differences in quality across the spokes hurt overall effectiveness or if improper behavior damages the legitimacy of the national domestic intelligence enterprise.

Culture and Change. A complication of this type of hybrid model—uniting, as it could, subunits of other agencies—is the complexity of the mesh of institutional cultures. DHS has already experienced growing pains in terms of attempting to develop a common culture, mission, and language. The stovepipes that complicated effective analysis before 9/11 still exist in DHS, although the department is gradually breaking them down. A hybrid could fuse the range of cultures introduced by the subunits, or it could remain atomized, acting not as a coordinated, single entity but as a hydra of domestic intelligence efforts.

A simplified domestic CT intelligence agency could introduce—and duplicate—the problems that DHS faced. Operational terminology, standard operating procedures, intra-agency information-sharing, and incentive structures would all have to be streamlined in this model. Fusion initiatives at the local and regional levels could be models of how this could function. However, at least so far, the outcome of work in that arena, particularly in terms of information-sharing, is ambiguous. Unifying components of entrenched federal-level agencies would be significantly more difficult. Finally, a hybrid domestic intelligence

agency would overlap with DHS responsibilities, leading once again to the complexities of duplication.

Interconnect the Current System

A different approach to constructing a new agency would involve tightening the existing connections among the units of the current system, rather than creating a full-blown new agency. In terms of the change involved, this model is less a deviation from the status quo than the other three. As has been mentioned throughout this volume, improving information-sharing and coordination among the organizations already involved in domestic intelligence and terrorism-prevention missions has been a major focus in the policy debate. The bases for highlighting information-sharing were the oft-mentioned information-sharing failure of 9/11 and the exigencies of a security environment characterized by a wide range of intelligence targets. This spectrum requires that far more actors be allowed access to sensitive information.

In founding a new domestic agency, promoting interconnection and coordination among currently active organizations could be the primary design goal. To create unity in the network, such interconnection would go beyond just information-sharing to coordination of collection and other activities of otherwise independent organizations.[12] One could envision a modest structure that would facilitate efficient technological interaction on the part of the rest of the domestic intelligence enterprise. This model would focus on linking agencies and enforcing information transfer. A version of this approach has already been the focus of such policy initiatives as the Information Sharing Environment (ISE), which proposes to break down the barriers to terrorism-information flow within the IC and between the IC and other relevant actors, such as law enforcement agencies and private-sector entities. Required as a provision of the IRTPA (2004), the ISE represents a

[12] The more decentralized the model that is chosen, the more important information-sharing and coordination (the glue that holds such systems together) become. If the component elements cannot link together effectively, the system might entirely fail to function.

> trusted partnership among all levels of government in the United States, the private sector, and our foreign partners, to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism against the territory, people, and interests of the United States of America. (ISE, 2006, p. xiii)

From another perspective, one practitioner we interviewed described such a model as analogous to the Joint Staff in the military, where the focus would be on ensuring compatibility and interoperability among different domestic intelligence organizations' activities.

Many initiatives already highlight the importance of incorporating local and regional activities into the decisionmaking process and of improving reciprocal information-sharing relationships between the federal and local/regional strata. Both of these components have been promoted through state and federal investment in fusion centers, where a range of law enforcement and intelligence officers are colocated in order to mesh intelligence data more effectively. The centers' responsibility is to fuse foreign intelligence with domestic information in order to facilitate improved policy decisionmaking on issues of CT, crime, and emergency response (Masse, O'Neil, and Rollins, 2007, p. 11).

In practice, the fusion centers are experiencing adjustment difficulties, including poor or absent communication between centers. Not all fusion centers have statewide intelligence systems. They also do not all have access to law enforcement data or private-sector information: "The flow of information from the private sector to fusion centers is largely sporadic, event driven, and manually facilitated" (Masse, O'Neil, and Rollins, 2007, p. 29). The problem of interoperability of systems that was widely criticized directly after 9/11 still exists. Because of the huge number of systems and the resulting duplication, reviewing incoming information is extremely time-consuming (Masse, O'Neil, and Rollins, 2007, p. 30). There are still difficulties in actualizing a two-way relationship with the federal government and with the private sector.[13]

[13] For a general discussion of the complexities facing fusion centers, see Masse, O'Neil, and Rollins (2007). For a discussion of the all-hazards focus, see Masse, O'Neil, and Rollins (2007, p. 29).

Beyond rhetorical commitment, on a bureaucratic level, this approach would require this new information-sharing effort to enforce standardization of classification—overclassification is still a problem—and support the standardization of software, procedures, and language. Relationship pathways would also have to be standardized—particularly as there is already some bitterness on the local level that information is perceived to flow only *to* the federal level but not as easily *from* the federal level.

As has been mentioned throughout this volume, a change in culture would also be required—one that does not just *suggest* the importance of information-sharing and a willingness of separate organizations to more closely link their activities, but rather enforces doing those things. An incentive structure that would reward sharing, cooperation, and joint work could be key; integrated completely, a new reward system could supplant the divide between law enforcement and intelligence in terms of what constitutes success.

Structure and Change. Something of an *all-channel network* of intelligence organizations, such an approach would have advantages of flexibility and adaptability, with multiple organizations able to concentrate their efforts on identified problems and potentially great diversity and experimentation in intelligence efforts as independent actors try new things. Such a structure fully eliminates the risk that any chokepoint in the system could hinder the ability to act, but it is also incompatible with approaches that try to apply consistent standards of action across the full domestic intelligence enterprise.[14] If efforts attempted just to maximize information-sharing, any data (of any level of quality) could flow through the entire network, producing major problems for organizations to deconflict the inputs received from other parts of the system.[15] There would be no obvious points for imposing filters to moderate how far information could go, potentially undermining attempts to preserve the privacy of individuals. The lack of

[14] See Markle Foundation Task Force (2002, 2003) for a much more complete discussion of some of these information-sharing concerns and challenges.

[15] Assuming an intelligent adversary that could recognize the value of injecting misinformation into the system, this could represent a significant vulnerability.

ability to impose enforceable guidelines for behavior across the system could also risk the actions of individual parts tainting the product—or the image—of the entire enterprise.

This level of decentralization has its own problems and complexities, however. Oversight and quality control would be difficult to maintain, and the relationship between producer and consumer of finished intelligence product could be further complicated by the numerous agencies involved in the process. The signal-to-noise problem has always been a complication of the intelligence-analysis process, and this linked structure and its augmented information flows would not provide a solution: Potentially both signal and noise would become more broadly disseminated among organizations.[16] Further, the issues of duplication just discussed would be exaggerated in this context. While this would allow for resilience and healing in case of failure, once again, the process would not be efficient, and the deluge of information could hamper the timeliness of information dissemination and, thus, appropriate decisionmaking.

Conclusions

This chapter introduces some of the analytical and organizational challenges that a new domestic CT intelligence agency could face. We have discussed potential options for reorganizing the current system as well as four potential alternatives for new organization of such a domestic intelligence effort. We have by no means exhausted the possibilities of either reorganization or design but have hoped, rather, to point to where friction points, issues, and problems could arise in creating a new agency.

---

[16] See Wohlstetter (1962) for the classic discussion of this particular issue.

CHAPTER SEVEN

Privacy and Civil Liberties Protections in a New Domestic Intelligence Agency

Martin C. Libicki and David R. Howell

Creating a domestic intelligence agency would likely represent a protracted effort to collect and analyze intelligence in the U.S. homeland. More domestic intelligence collection, in turn, means more information collected on individuals—certainly on individuals of interest, but putatively also on individuals who are not yet of interest but who might be labeled as such if more were known about them. More information collection, in turn, brings attention to privacy issues of the sort that merit consideration even in the absence of a domestic intelligence agency. In one sense, the balance between security and privacy can be measured by the number of terrorists[1] identified versus the number of innocent people whose personal details are "viewed" by agents of the domestic intelligence agency through data-intensive methods. Yet, if greater attention to domestic intelligence is not to lead to wholesale reductions in privacy, one might ponder which safeguards should be instituted when designing such a new organization to strike a new balance between security and privacy.

In considering the use of personal information in security applications, there are a variety of approaches that focus on addressing privacy concerns given specific missions that government organizations need to achieve. If a new domestic intelligence agency were created, its design, its policies, and its capabilities would have to be shaped by an explicit

[1] We use *terrorist* as shorthand for those in whom the domestic intelligence agency is interested. Some may not, in fact, be terrorists; they may instead be spies, violent revolutionaries, major saboteurs, or the leadership of powerful crime syndicates. That noted, trade-offs that may be reasonable for targets who *are* terrorists may not be reasonable for other targets.

consideration of what information it would have access to and what could be done with that information. In this chapter, we walk through what would be involved in that design process, first examining the changing nature of domestic intelligence and the legitimate domain of privacy rights, then reviewing the variety of options for protecting privacy in intelligence activities and assessing their pros and cons.

The Privacy-Relevant Nature of Domestic Intelligence

If, in retrospect, the Federal Bureau of Investigation (FBI) had learned a great deal about the habits, goings, and comings of Zacarias Moussaoui (convicted of conspiring to commit acts of terrorism), few people would have been terribly upset by the revelation. As a terrorist, it is likely that any complaint he might make that his privacy rights were being violated would not be compelling to most people. If, on the other hand, the FBI gained a similarly detailed knowledge about the habits, goings, and comings of everyone in Minnesota in the effort to find him, the outcry might well be deafening. Virtually no one else in Minnesota is a terrorist, yet information on these people would have been gathered and transferred to the FBI's storage files. Therein lies the crux of the security-versus-privacy dilemma.

Different investigative methods create different demands for personal information. As a rough approximation, they fall into three categories:

- *Specific:* A person of interest is identified, and information is sought on that individual. The information may include personal information about other people—e.g., the people he or she knows—but the emphasis and the organization of such information relates back to the specific individual of concern. In certain cases—e.g., looking through a complete flight manifest to find out whether the person of interest took that flight—one is unearthing information about large numbers of people, but data on everyone else can be easily discarded after being scanned without affecting the investigation.

- *Relational:* A person of interest is identified. Information is then sought on those who may have a connection with that person. Thus, knowing the name of someone on the terrorist watch list (at least back when it was of manageable size) and then tracing his or her contacts may reveal the names of potential terrorists who thus merit scrutiny. Jeff Jonas of Systems Research and Development (SRD), a firm started to protect the gaming industry from criminals, argues that one could have generated the names of all 19 hijackers by starting with two of them who were on the watch list and then seeing whom they were living with, sharing phone numbers with, or otherwise in close contact with (Jonas and Harper, 2006). Major telecommunication companies have reportedly analyzed their databases to support the federal government in tracking suspected terrorists (Lichtblau and Risen, 2005). Of course, such a method must be used with care. Given enough links, everyone would be on such a list.
- *General:* This methodology is based on the assumption that potential terrorism suspects can be identified by dint of the unique pattern of transactions in which they engage. In its most expansive form, this method entails collecting a large body of transaction information—phone calls, Web-surfing tracks, airline manifests, credit-card records, bank statements, and public records—and putting them in a large database. Data-mining techniques would be used to figure out which people's patterns are sufficiently unusual to merit further scrutiny in the form of, say, interviews, surveillance, and subpoenas. In recent years, this approach has been most closely connected with the Total (later Terrorist) Information Awareness (TIA) program. Although Congress killed the TIA program,[2] other actors in the intelligence community (IC) reportedly picked up many of its components. Its methods may return, especially if the scope of the data mining is more limited and the overall process does not attract attention to itself (Kelley, 2006; Harris, 2006a). The controversy has not stopped the federal

[2] Perhaps if the program had adopted a lower profile, humbler objectives, and a less well-known director, it would have survived.

government from acquiring large volumes of personal information from private-sector data aggregators (GAO, 2004c).

In our analysis, we assume that all three data-acquisition methods are in play throughout the entire spectrum—that is, from the specific through the relational to the general. Our analysis will concentrate on the general case on the presumption that more-restrained efforts can then be treated as lesser-included cases.

Gauging Privacy

One big problem in figuring out how to balance privacy and security lies in determining what exactly privacy is. Although a complete review of legal and other thinking on privacy is beyond the scope of this analysis, some summary observations are relevant for setting the stage for later discussion. The right to privacy is not legally absolute in the same way as freedom of speech. Speech is specifically mentioned in the Bill of Rights. Privacy has to be inferred from the Bill of Rights, either in specific contexts (e.g., freedom from unreasonable search and seizure) or as a penumbra implied by the Ninth Amendment (Dixon, 1965). Although First Amendment rights are rights to *do*, the right to privacy is the right to *keep others from doing* (i.e., collecting information on someone). The freedom to speak, once denied, can be restored. An individual's privacy, once violated, may well be violated forever, in the sense that the sensitive information, once released, cannot be unreleased. Largely, therefore, privacy, at least in legal terms, is determined by the courts.

The key criterion for determining what lies within the government's right to know and what does not is based on which acts afford someone a *reasonable expectation of privacy*—where *reasonable* hearkens to the Fourth Amendment's reference to unreasonable search and seizure. For example, for a police officer to overhear and take advantage of something one says in the middle of a police station is not problematic: One has no reasonable expectation of privacy there. Conversely, for a police officer to exploit technology to hear something one says

in one's automobile[3] when the windows are up may well be problematic, because one does have a reasonable expectation of privacy in that milieu. This test has practical value because it delimits zones, so to speak, in which one can communicate freely and in which one cannot. As long as the distinctions between these zones make sense and are clear, individuals will know how to regulate behavior in unprotected spaces while retaining sufficient opportunity to enjoy protected spaces. The types of information collection technology permits versus only those that are reasonable, however, is a slippery distinction to make. Before airplanes were invented, it was assumed that one had a reasonable expectation of privacy for activities carried out in one's backyard if it was hedged by tall fences (Krakovec, 1986). Now the matter is less clear (Block, 2007). Similarly, whereas landline phone calls may enjoy protected status, is the same true for those from cellular phones, which generate signals that even amateurs can intercept?

The issue at hand for the newer and more controversial methods of domestic intelligence (i.e., data surveillance) is how to define an individual's privacy rights associated with third-party transactions (e.g., bank accounts). Courts have generally ruled that unless the specific class of transactions is protected by law (e.g., as video rentals are), an individual has no reasonable expectation of privacy with such transactions. One cannot have a credit-card transaction without the credit card company knowing some details—and if the credit-card company knows, then nothing necessarily prohibits law enforcement from asking for or subpoenaing such information. Exceptions have been made in law for bank transactions, medical records (Pub. L. No. 104-191), phone-call records, and educational records, as well as video stores and cable-television selections—but the existence of such specific exceptions demonstrates that there are no general rights in law.

Computerization is one of those technologies that have helped complicate the privacy conundrum. Record systems, of course, predate computers—but what computers *do* permit is the ability to amass

[3] We use *automobile* rather than *house* because the Supreme Court has singled out the home as having a constitutionally protected status as a sanctuary. See Justice Antonin Scalia's opinion in *Kyllo v. the United States* (533 U.S. 27, 2001).

records automatically (e.g., checkout scanners that help correlate purchases with purchasers) and mix and match records across heterogeneous databases. The latter, however, may be legally problematic. Courts have made clear statements that access to a single stream of data does not imply similar rights to access to all of the data put together. As Daniel Solove has pointed out, aggregated data create a digital approximation of a person (a *digital person*) much more surely than does any disaggregated stream of data (Solove, 2001). Conversely, federal agencies have acquired personal data that data warehousers accumulate and organize by individual; the government's doing so has yet to be ruled legally problematic.

The best conclusion one can draw from this analysis is that whatever broad privacy rights are asserted have to be defended not as legally mandatory,[4] but as generally desirable.

Unfortunately, this just raises the second question: What aspects of privacy should be protected? Indeed, why protect privacy at all?

To pursue this discussion, we start with one definition of *data privacy*—an individual's right to control who sees information about him or her. We assume that, from a privacy perspective, more control is probably better, but we concede that an absolutist perspective comes at no small cost: Is society better off if individuals whose criminal records cannot be disclosed are permitted to assume positions of discretion and authority? Can insurance function if people do not have to reveal information about themselves? Forcing the government to ask people to release information about themselves would reveal the authorities' interest in such people; this would make further investigation far more difficult. It would be misleading to measure privacy by how often a domestic intelligence agency asks individuals for permission to view their records. If nothing else, seeking permission on a case-by-case basis is utterly impractical for carrying out data surveillance. Instead, we have to look at how often such records, are, in fact, seen by authori-

[4] Were the discussion about which rights are legally necessary, the proper policy question would be less one of how much deference to give privacy rights (something the courts would decide) than of how to ensure that actions that are unlawful because they violate privacy rights can best be detected.

ties that individuals prefer did not see them. This is particularly the case when such authorities are in a position to make prejudicial decisions about those whose data they view.

To understand the right to privacy we must ask, why are people reluctant to have others know things about them? This question admits of several answers. It is hard, for instance, to argue with the general, "it's just creepy" sentiment, and such sentiment cannot be ignored. But can one adduce anything more specific?

Many of the ill effects of unwanted data transfer revolve around issues of information *use* rather than *acquisition* (Birrer, 2005). That is, people in a position to make prejudicial decisions are armed with information that, some feel, should not enter into such decisions. The data may be wrong, or it may be misleading outside of its true context; the individual may have little or no opportunity to see (much less correct) mistaken data. Knowing that judgments are being based on certain data may inhibit activities that the government has no right or good reason to inhibit. Decisions made based on such data may be wrong, unfair, or otherwise problematic.

For a law enforcement agency, the problem is bounded, but hardly trivial. That is, for U.S. persons, due process governs judicial convictions, and information can be used in the courts only if it is deemed relevant as well as available for discovery. Unfortunately, the process by which someone becomes indicted (much less becomes a person of interest) is not transparent. Yet, the consequences of being indicted are hardly trivial; they are measured in terms of time, money, anxiety, reputation, and restricted movement, which may include jail time prior to any conviction. The best safeguards against abuse are the wise use of prosecutorial discretion and the possibility that too many indictments that fail to result in prosecutions would erode the credibility of the agency involved. Neither safeguard is so perfect[5] that it can be relied on to vitiate the privacy harm from letting officials have broad—let alone complete—information on persons. Finally, if the domestic intelligence agency had in its repertoire powers *other than prosecution*

[5] Not to mention that people may be wrongly convicted or, more frequently, persuaded to plea bargain rather than risk being convicted even when they are innocent.

to protect the national security, the degree of due process (or something analogous) associated with the use of that power would have to be analyzed as well and would likely bear on the level of concern about the types of information it was allowed to access, aggregate, and use.

Of a similar nature are abuses of what should be private information: It is distributed to others who can make prejudicial decisions, to those who know the individual in question, or to the masses (which matters most for public persons, such as celebrities). This case is simpler insofar as the secondary distribution is clearly a case of corruption and something for which there is no legitimate law enforcement or security rationale. That being so, the emphasis has to be on minimizing corruption and ascertaining what measures and controls would do so efficiently and effectively.

This leaves those privacy issues that arise when information is revealed to those who may not necessarily make prejudicial decisions. The desire to present oneself to others as one wishes to appear is a deeply rooted one. But which others? It is normal to feel uncomfortable walking down the street among perfect strangers and know from looking in their eyes that they know something embarrassing about you. However, what about individuals one is unlikely to meet but who had a voyeuristic interest in the information (Rosen, 2001)? What if embarrassing information were associated with one's name and not one's face? What if the other were somewhere accessible only through telecommunication and so would never be encountered? Finally, and most relevantly, what if this other were a computer and thus had no interest in the information as such?

The question about computers strikes at the heart of the matter. Initially at least, computers and not people will be the ones sifting and sorting through the haystacks of personal information looking for needles relevant to security. If, for instance, there are no serious privacy rights associated with a computer "seeing" information while there are if a person, however remote, sees it, then where to put the safeguards follows straightaway. To wit, the computer can see the data, but questions must be addressed when the data are to be transferred from the computer to a human being. Alas, this criterion is easier to state than to enforce, which we address in the last section of this chapter.

Elements of a Security/Privacy Trade-Off

So far, we have argued the following propositions:

- The security/privacy trade-off is most acute when considering the general method: gathering data about *everyone* to determine from transaction patterns who merits greater scrutiny as potential terrorists. It remains of great interest, whenever large classes of persons (e.g., all acquaintances of a known terrorist) are profiled to determine the likelihood that they are terrorists.
- Privacy concerns are strongest when those who can make or inform decisions about an individual see personally identifying information about that individual; next most strongly if the information is seen by others; and least if the information is collected but seen only by computers, not individuals.[6]
- Any security/privacy trade-off has to combine both necessary safeguards and reasonable techniques to ensure that the safeguards are adhered to.[7]

In working through the trade-offs, we assume that the general method is worthy of consideration. This, however, is by no means obvious. Little empirical evidence has been released to suggest that mining

---

[6] Might personal information seen by individuals who cannot possibly come into contact with the individual in question (e.g., contract employees in the third world) be seen as less invasive than that seen by domestic sources? Answering this may add complications without offering any clarity.

[7] The emphasis on *reasonable* is meant to avoid the infinite regress that arises from trying to satisfy the paranoid. Thus, while a reasonable scheme may assume that federal agents cannot be trusted to put the strictures that protect privacy above mission, it does not follow that a judiciously chosen third party cannot be entrusted with such a mission. Such a third party can fall outside the executive branch (or be vested in part of the executive branch, such as inspector general, with responsibilities that fall outside the executive branch). Or, it can be a third party not beholden to the executive branch (or at least a party that, if linked, has other reasons for carrying out its responsibilities). Conversely, however, such an entity has to be trusted to protect security equities, as well. Many techniques that selectively release information reveal the government's interests in an individual and, if released, could damage ongoing investigations. To the truly paranoid, of course, everyone is in cahoots, so no scheme that collects data at all can be trusted.

large bodies of data for signs of terrorist tendencies can generate a sufficiently compact list with enough terrorists on it who merit more-intensive investigation. The proposition that the relational method can produce good leads has a putatively more plausible rationale (based on long experience in traditional law enforcement investigation) but still raises issues associated with the general methods, albeit for a smaller population of nonsuspected Americans. There will also be reasonable instances in which federal officials, having gained intelligence that fingers a person with certain identifiable features (e.g., resident of St. Louis, never married, age 50, frequent traveler to Hamburg), may want names of people who meet that description and may thus need at least one-time access to enough data to make that determination. And, of course, the possibility is always there that completely innocent people can be mistaken for the guilty and lose their privacy in the face of a government investigation.

We will therefore examine several candidate methods that might reduce the apparent zero-sum nature of the security/privacy trade-off: *minimization*, *data-retention policies*, *data-storage policies*, *foreign nationals only*, *anonymization*, *automation*, and *discovery*. We initially assume that people follow administrative and legal rules put in place to oversee and control the government's use of personal data, but, in the last section, we examine some techniques to help ensure that they do. The fundamental goal of such candidate methods is to minimize potential intrusions on privacy without unduly hindering efforts to improve domestic security.

Minimization

The principle of minimization states that one should collect only the data one needs to carry out the specific missions for which the data are requested. If a decision can be adequately made using certain pieces of data, nothing else should be requested. In the Transportation Security Administration (TSA) example described in the preceding section, for instance, if one trusts the airlines—and the current no-fly rules *do* trust the airlines—it is not necessary to associate an individual with an itinerary. It suffices that TSA receive a passenger's name, sex, and birth decade to determine whether he or she is on the No-Fly List

and forward this determination to the airlines, which can then determine the flight that person was going to take. TSA does not have to know what flight the passenger is on, as long as the airlines do.[8] If TSA does not record the flight, it cannot pass it on to others, such as law enforcement officials, that individuals might be concerned about having knowledge of their travel activities.

This example shows, however, why this rule would apply *to everyone except the domestic intelligence agency.* TSA's mission, in this particular instance, is limited to making matches between passenger lists and the No-Fly List, and it is therefore straightforward to lay out the information required to do so. Conversely, because it is not clear what data are relevant to a domestic intelligence agency's efforts to profile terrorists, it is also unclear what information would *not* be relevant to such profiling. Until otherwise proven, a reasonable argument could be made that every plausible piece of information may be relevant to the domestic intelligence agency. Thus, it would be difficult to determine the minimum information required for this more general intelligence mission. Were the government seriously interested in applying general methods for seeking out potential terrorists in the overall population, then research may be called for to determine what data elements are highly unlikely to be useful in establishing profiles.

In this scenario, minimization would enter the picture by placing the burden of proof on the domestic intelligence agency to argue that a particular piece of information *would* be useful in distinguishing terrorists from nonterrorists. Such a requirement would force the domestic intelligence agency to generate a plausible rationale why, for instance, data on what individuals purchased in drugstores might be relevant. This may serve to limit the acquisition or at least use of certain data.[9]

---

[8] Which an airline can do either by running the tagged name against its total database of people scheduled to board one of its planes within the 72-hour reporting period or by encoding the flight information in its data to TSA and using the encoded flight information to match a no-fly passenger to passengers in its own database.

[9] Because acts of terrorism differ, indicators may vary by type of attack. For instance, the indicators for a terrorist attack using commercial airliners may be different from an attack using anthrax. The difficulty of anticipating every type of terrorist attack might therefore

Since much of the information usable in profiling would come from private sources, they, too, would have to practice minimization for such information to remain private. This would require that a broad mandate be applied to private business—something called for by the European Union's (EU's) privacy directive but, so far, incompatible with the structure of U.S. law.

Thus, while minimization may well be good practice all around, unless the burden of proof is on the domestic intelligence agency to show that a piece of data of adds markedly to the performance of the profiling software, minimization is unlikely to offer very much.

Data-Retention Policies

Under this method, data would be kept for limited periods and thereafter discarded. The basis for this approach is that limiting data retention can reduce the potential that information on individuals can pose a risk to their privacy—e.g., the embarrassing habits of one's youth pass into the memory hole after one has matured. Conversely, one can argue that old information has decreasing relevance to profiling, limited relevance to correlating intelligence with an identity, and almost no relevance to finding someone based on a set of characteristics. Thus, the increasingly irrelevant but still personally sensitive information from one's past is discarded.

Despite their advantages, data-retention policies are no panacea. Auditing issues are not trivial, since it is hard to know that every single electronic copy of some information has, in fact, been destroyed.[10] Unless the data retention period is measured in days rather than years, there will be enough data collected to characterize (or mischaracter-

---

argue for retaining information that may not be indicative of known terrorist attacks but may be indicative of unknown modalities. This, however, is a better argument for warehousing data with a third party that would be released only if the indicators for such an attack could be developed.

[10] The rule about destroying data may prevent the use of old information in court, but it is hard to prove that the domestic intelligence agency did not use such data to subpoena fresh, legitimate data. Serious attempts to enforce the data-storage rule would most likely require ensuring that the data never left the physical premises of a third party, which would, in turn, run its own audits.

ize) individuals even if the old data are dropped. Some old data, such as prior criminal records or names of schoolhouse chums, retain their relevance for current criminal investigations. Indeed, people rely on access to and use of some old data on themselves throughout their lives—for example, evidence of decades-old educational attainments.

Data-Storage Policies

Another approach, one recommended by the Markle Foundation Task Force (2006) study, is to leave data with the data holders and have the domestic intelligence agency poll their distributed databases as needed for its work. This has several advantages and disadvantages but hardly gets to the heart of the matter.

The only real advantage of such disaggregated storage is to reduce the odds of after-the-fact misuse. Such concerns are based on the logic that, if the data sit around in the warehouses of the domestic intelligence agency, it is only a matter of time before an overzealous, rogue, or corrupt employee finds some way to abuse the information. Whether even that problem is fixed by keeping the data somewhere else depends, in large part, on how one governs the domestic intelligence agency's access to data held by other entities. If access control is manual, suspicious requests for data may be rejected. If access control is automatic, it matters very little where the data sit physically; to anyone but the network administrator, the difference between local (really, quasilocal) and global storage is invisible. The mischief one can do if the information can be grabbed from another agency is identical to the mischief one can do if it is grabbed from the same agency.

The key is whether the agency (or corporation) that owns the data has and is willing to use methods to detect suspicious data requests and deny the data-diver information before the data are irreversibly transferred. This raises several questions. What kinds of rules can be used to define *abuse*? What algorithms are needed to implement such rules? What actions are triggered by such rules, and are they triggered automatically or only through human intervention? How can one be sure that such rules kick in before too much of the wrong data is transferred? Finally, if these rules can be codified, what prevents the domestic intelligence agency itself from implementing similar rules and thereby pre-

venting malfeasance over not only imported but also local and cached data (i.e., data retained in local files to limit redundant network traffic that would arise from repeated requests over the network for such data)?

The costs of implementing a remote data–storage policy are not trivial, especially if meant to govern data-mining operations. While calling large amounts of data over a network is getting continually less expensive, it is not yet free, especially if the network is expensively engineered to avoid problems, such as availability or security problems that plague the Internet. Latency issues (the lag time between request and receipt) may also get in the way of data-mining algorithms if not engineered precisely.[11] The larger the number of entities that have to be polled to build a correlation, the greater the likelihood that one may be unavailable for one reason or another (and it is unclear whether the urgent requirements of the domestic intelligence agency will restore service as fast as similar urgency by direct users might). Data-cleaning tasks (e.g., omitting duplicates, reconciling contradictory records from two agencies) are also difficult to carry out without wholesale transfer of data sets. This is particularly true when analytic data are generated by combining separate streams of primary data. The domestic intelligence agency, having gone to the trouble of cleaning or combining the data, may want to keep the results rather than have to regenerate them every time it wanted to go back to reanalyze the data.

On balance, therefore, this proposal seems to be a nonstarter. It would do nothing that could not be done by other means and would impose needless costs.

Foreign Nationals Only

While U.S. persons enjoy legal protections, and U.S. citizens vote, foreign nationals in the United States may be considered fair targets for data-mining purposes. Thus, in this alternative, these two classes of

[11] This applies if the relevant algorithms are run one record at a time. If the data are pulled in large chunks into the domestic intelligence agency, the latter can effectively take control of the data en masse.

individuals would be treated differently: Data would be retained for foreign individuals and not U.S. persons.

Focusing on foreigners (i.e., the population from which all 19 hijackers in the 9/11 operations were drawn) may facilitate data mining. However, anticipating as much, al Qaeda is working to recruit citizens of Western countries into its ranks even if it has had relatively little success in the United States (Mueller, 2005; Rosenau, 2005). Furthermore, although the consequences of snooping on people are much lower if these people are not U.S. persons, consequences do exist. The increasing burdens being imposed on those seeking to travel to the United States have caused a substantial and lingering reduction in how many come here for work, play, school, and extended visits (National Research Council Committee on Policy Implications et al., 2005; CBO, 2006).

The practical problem with this approach is distinguishing foreign nationals from U.S. persons without a national identification system. In some cases—notably, foreign travel (for which passports are required)—the distinction is fairly easy to make and fairly accurate, even for those who wish to evade scrutiny.[12] One can take the existing tracking system (i.e., Advance Passenger Information System, or APIS), discard data on U.S. citizens a week after the flight lands (TSA's proposed standard), and retain information on everyone else. But otherwise, transactions rarely require passports, and only a few require birth certificates or documents derived from them. If state-issued drivers' licenses are reengineered to include greater security and indicate citizenship status, transactions based on them may also be easily separated into those carried out by U.S. persons and those carried out by foreign individuals. However, the Real ID Act has faced substantial opposition from states based on projected implementation costs and privacy concerns (Grimmett, 2006). In addition, there is serious concern about the implications of requiring that citizenship status be displayed on licenses (EPIC, 2007). As for transactions in which citizenship is not

[12] Although U.S. passports are not completely immune to forgery, they are, nevertheless, fairly reliable. More likely to confuse U.S. authorities are faked passports of other countries.

directly identified, one would have to guess after the fact; one might be able to separate credit-card numbers into those known to be associated with U.S. persons, those known to be associated with foreigners, and those whose association is unknown. Thus, the first set of transactions (and all transactions with *n*th-order links to known credit cards, such as phone calls associated with a credit-card account) can be discarded. All in the second set can be retained. But what does one do with the second set, a set in which potential terrorists would want to be? If the data are discarded, one probably is losing access to the very data one seeks; if the data are retained, it is to the detriment of privacy rights of U.S. persons. If data are to be held in limbo while (hopefully automated) efforts are made to determine the status of those to whom they refer, then one cannot use such data without taking care that the data results are segregated as well.

Thus, unless the middle category of indeterminates can be sufficiently reduced, the approach of separating U.S. persons from everyone else cannot be strongly recommended.

Anonymization

This set of approaches recognizes that most individuals will be of little interest to the domestic intelligence agency unless and until their characteristics match some predefined template. If they do and the evidence can convince a disinterested third party that sufficient probability exists that the individual is indeed of legitimate interest, the individual's name would be released to human analysts.[13] Otherwise, data on the identity of such individuals are not presented to authorities (Sweeney, 2005). One recent example of this involved anonymizing facial images in video surveillance footage. Facial images could be unlocked by law enforcement only after obtaining a warrant, thus preserving the privacy of others present in the video (Newton, Sweeney, and Malin, 2003).

---

[13] One can debate who the third party would be and what a proper probabilistic threshold might be. Nevertheless, if the data were obtained constitutionally, there is no legal requirement that the third party be a magistrate or the threshold be 50 percent (i.e., probable cause).

The anonymization approach recognizes that profiles of individuals tend to involve transactions that occur in more than one place: the public record, phone calls, travel, credit-card transactions, and consumer purchases (as recorded by the retailer). Rather than call for, amass, and analyze such records by name (or similar identifier), the data are encoded so that one cannot tell to whom they refer. Thus, one would know that X was 40, never lived in one place for more than two years, made many trips to Pakistan, and purchased multiple trucks. Either this transaction record matches a terrorist profile, in which case X's name would be requested, or it does not, in which case X's identity would remain unknown.

Unfortunately, this method stumbles on three obstacles. First, without knowing X's identity, to know that the X to which one database refers is the same as the X to which another database refers requires that every data-providing institution use the same key to encrypt the name in the same way. This is not impossible but is hardly trivial. Anonymity can be protected using public-key cryptography with the key being generated by a third party; the public encryption key would be widely advertised, and the private decryption key would be used by the third party to translate a number back into a name.[14] Second, the name-identifier resolution algorithm cannot be used with encrypted data; once encrypted, the names *Ralph* and *Ralphy* would not necessarily look anything like one another. Other techniques, such as mapping similar and derivative names into a common template (e.g., every *Will*, *Willy*, *William*, *Bill*, and *Billy* would map to *William*), would have to be used—in the exact same way—by each of the thousands of data providers. Smart people, such as the aforementioned Jeff Jonas, are working the issue, but proven success is a long way off (Greene, 2006). Third, it may matter little whether the name (and, to be fair, social security number [SSN], address, phone number, and birthday) is omit-

[14] The third party would pass out one encryption key to everyone and retain the decryption key itself. Access to decryption services would require a particular finding (e.g., a matched profile) from the domestic intelligence agency, which would forward the encrypted name to the third party and receive the decrypted name back. Of course, the decryption key would have to be protected against all manner of threat, not least of which would be from the domestic intelligence agency itself.

ted[15] if all the other details are known. A famous study claimed to be able to identify 87 percent of the population in the United States based only on five-digit ZIP Code, gender, and date of birth (Sweeney, 2000). A recent attempt to replicate those methods found that 63 percent of the population could be uniquely identified using the same three fields of information (Golle, 2006). An overzealous investigator or stalker could take the various details and narrow down X's identity to a single individual by using successive processes of elimination.[16] It is not clear whether combining anonymous transaction data with public records available en masse from data consolidators would suffice to reveal personal identities.

Automation

An alternative and perhaps more reasonable approach would be to automate the data-analysis process completely by using real identifiers but release identified data for human inspection only when there is some likelihood that the individual is a terrorist. This approach assumes, as argued, that privacy can be harmed only by what a human knows and not by what a computer knows (unless the computer is making decisions without human intervention). If the two are provably separate—and can be counted on to remain so—then privacy, as such, is preserved.

Keeping such distinctions, however, means that algorithms applied to the data (i.e., to generate a list of persons of interest) must work without direct, by-name human intervention. This is hardly a problem if human intervention does little to improve the quality of the algorithms (and algorithms may be flawed with or without human intervention). However, humans are still better at spotting both positive anomalies (e.g., a series of transactions that simply do not make sense) and negative anomalies (e.g., a series of transactions that might trigger an automatic call-out but that a human can explain in terms of a benign or

---

[15] Or perhaps beyond fair. Age, ZIP Codes, and colleges attended, when combined with other knowledge, may well feed the profiling algorithm.

[16] Some additional protection may be possible by randomly injecting spurious data to throw off such cyberstalking, but at the cost of making the profiling algorithm more error-prone.

familiar pattern). This is particularly the case if the algorithm is built to generate large numbers of names that are matched into nontransactional data, such as news clippings, Web citations, or police reports, to be culled before generating a much smaller list of persons of interest. At this juncture, there is little public evidence to indicate whether human intervention in these algorithms adds enough to negate the argument for anonymity or for lowering the threshold at which data leave the machine for human eyes. Enforcing this distinction will not be trivial, but, as argued later, there are tractable methods for doing so.

The challenge here is figuring out which profiling methods work *without* being able to compare hits to real terrorists. Algorithms must be tested against large data sets in which individuals' identities may have to be revealed far more often than they are in actual investigations. Similar tests may have to be done to tune the identifier-reconciliation algorithms noted earlier. As a practical matter, there should be a bias toward minimization; in other words, the justification for looking at more than a handful of profiles should be explicit.

Finding a proper trade-off may be facilitated by the fact that those who test the algorithms need not be people who make decisions based on what the algorithms say, thereby removing at least one reason that revealing such data constitutes a privacy violation. This suggests that testing be assigned to a group at institutional, networking, and physical remove from the domestic intelligence agency. A further safeguard, if necessary, to see how well the algorithm works, may be to use anonymization for the identifier data associated with transactions and those that point to known terrorists before they are matched against one another.

Discovery

Would it help improve the privacy/security trade-off if individuals were informed of what the domestic intelligence agency knew about them? This is a three-part question: What type of information streams are being requested by the domestic intelligence agency? What specific information does the domestic intelligence agency have about an individual? What conclusions does the domestic intelligence agency draw from this information?

The argument for revealing what types of information the domestic intelligence agency collects is fairly strong. Such revelation, if honest, builds credibility into the data-surveillance process and provides a basis for public oversight of the domestic intelligence agency; it inhibits unwarranted suspicion. Revelation permits debate over which data should be collected; debate can result in acquiescence in certain aspects of the collection (in which case it can credibly proceed) or opposition thereto (in which case it should cease). The counterargument is that it reveals to terrorists (among others) what aspects of their lives are and are not being monitored. Such fears may be exaggerated, first, because terrorists tend to be paranoid and will not necessarily believe that a category of data is being abjured simply because the federal government so declares, and second, because the failure to collect on one stream of general information is no guarantee that information is not being collected on particular individuals.

If the general data streams being collected are declared, should individuals be able to see what such general information is? The case for doing so is at least as strong. The data may create errors that individuals can correct or at least explain to authorities (yet, by doing so, individuals may be making an issue of something that would have easily passed beneath the profiling algorithm's notice). It would assure almost everyone that what they saw is the topmost limit on the general information that the domestic intelligence agency had on them. Since few people keep detailed records on themselves, it would amount to a callable data repository from which they could manage their own personal and business affairs. Credit bureaus might complain about losing a revenue source (charging people to see what such bureaus know about them), but the legitimacy of that particular business line is already not without controversy. However, the domestic intelligence agency would have to implement sufficient security to check that an individual wanting to see his or her record is not an imposter and, as such, a possible data thief.

The case for revealing the profiling algorithm, which converts such data into indicators of interest, however, is far weaker. First, it *does* reveal which transactions are likely to trigger interest, just as knowledge of the computer-assisted passenger prescreening system (CAPPS)

will tell a potential hijacker what to do to avoid scrutiny. Second, it helps predict who will be the target of an investigation, something law enforcement officials are understandably very leery about doing. Conversely, many of the benefits of revealing the data to an individual, such as the opportunity to correct and explain errors or the personal data–repository benefit, simply do not apply here. Granted, outside oversight of the algorithms may help to weed out unnecessary data requests or sharpen its focus, but professionals working under an intelligence-agency aegis and security rules can provide this oversight as well.

Finally, selected individuals not beholden to the domestic intelligence agency ought to be given a certified précis of all the algorithms used that indicates on what data they draw and for what behavior they are searching. The purpose of this step is to inhibit mission creep. If profiling proves useful or even interesting, there will be a temptation to expand the ambit of the domestic intelligence agency to investigate a range of activities that, in turn, are said to justify further data surveillance.

Enforcement

Setting data-privacy rules is one thing; establishing procedures to ensure that rules are followed is another. Many of the standard approaches for governing data use in any context, such as the use of audits and charging an outside entity with rule enforcement, make similar sense for the domestic intelligence agency. Even if the authorized users of the databases are more fastidious, honest, and incorruptible than the average citizen, the potential for abuse is still significant. Rules that govern who can see what data should be explicit and precede the collection of data rather than being made up on the spot. One also hopes that audits and privacy oversight are accepted as part of the cost of having such broad access to the information.

Exactly how data rules are enforced will depend, of course, on what these rules are as well as on what technology is available in designing such systems. For the sake of simplicity, consider three problems:

- collection of data from the original owners
- transfer of data from computer to human

- use of the data once they are seen by humans.

How can systems prevent the acquisition of data that the domestic intelligence agency should not have in the first place? Technically, there is no foolproof way to prevent information from being requested and stored where no one else knows where it is.[17] In practice, however, public announcement of what data streams the domestic intelligence agency can legitimately and illegitimately request should put sufficient spine in private enterprises asked to hand over records sub rosa when they have reasons not to do so (Markoff and Shane, 2006). Here, it is transparency rather than audits that are likely to inhibit bad behavior.

An ancillary challenge is to ensure that the data streams enter the audited repository and nowhere else. One way to do this is to use encryption with the repository's key stored safely in hardware where no one outside the holding system can either read it or change it.[18] Thus, as long as the data generators are sufficiently diligent about encrypting the data (with the right key), diverting the data to a rogue repository would do nothing, since there would be no way to read the data so diverted.

Assuming that the data are transferred into a repository, access to which is mediated through profiling algorithms or authorized by-name or by-circumstance requests, the challenge is to ensure that information from the repository is not released some other way. Several options present themselves that can be used singly or in combination. One

[17] With terabyte storage available for personal computers, even very large data sets, such as a year's worth of domestic passenger-name records can be so stored.

[18] There are two ways to do this. One is to use asymmetric encryption on the data, in which public keys are passed out to all the data generators (e.g., phone companies) while the repository maintains the only decrypt key. Public-key encryption permits the encryption key to be universally distributed without serious fear that its possession will permit decryption. The decryption key is altogether different. Although the encrypt and decrypt keys are mathematically related, deriving the decrypt key from the encrypt key is so computationally time-consuming (assuming a sufficiently long key) as to be impossible, for all practical purposes. Since asymmetric encryption is processor-intensive, an alternative is to use symmetric encryption (both encrypt and decrypt keys are the same). The repository would randomly generate symmetric keys for every set of bulk transactions, and asymmetric methods would be used to transfer keys securely. Note that, if names are also anonymized, two separate encryption methods (and enforcers) may be involved.

option is to build the controls into the repository itself. Such controls would permit data to be accessed only in response to certain commands; this would enforce the prohibition against seeing personal data of individuals who are not provably of interest. Thus, it would not respond to requests for wholesale data downloads (e.g., everyone who spent more than $1,000 in telephone calls to the Middle East). A second option is to log requests to media that cannot be erased.[19] If access to the repository is governed by good security practices (limiting but, alas, not eliminating the risk that a rogue intelligence agent can pose as someone else) and these logs are actually read, a great deal of mischief should be inhibited. A third option is to place the repository in the hands of a third party separate from the domestic intelligence agency. The character of this third party requires careful attention. Putting a repository in the hands of a third party that can be corrupted, hustled, or bullied into betraying its trust would be worse than leaving the repository in the domestic intelligence agency (because each could point to the other as the source of the violation if caught). Conversely, if the third party is too cautious about releasing data, it could find itself the scapegoat for failures (e.g., slow response times) in the domestic intelligence agency.

Caveats

One important complicating factor in assessing the trade-off between privacy and security is that it is not a decision that the domestic intelligence agency can make and enforce alone. There are many reasons that the safeguards put in place within a single agency would not completely protect privacy. We note two of them. First, resolving identities correctly may well require the services of data consolidators and could thus open private information to them. Second, many of the data elements of interest to the domestic intelligence agency will require information from other government agencies.

[19] It is better if this process does an immediate write rather than hold such requests in its electronic buffer, which could be erased before being inscribed.

Identity Resolution

Part of the technical difficulty of aggregating information is determining to whom a name or identifier refers. We all leave behind bits of data with all our transactions, but we tend to leave them behind under different identifiers and monikers. This complicates aggregating all the information about one person, since it is not always clear whether two references to the same name refer to one person or two or more. To some extent, the use of other identifiers, such as SSNs, helps remove the ambiguity: They are unique (one number is not supposed to be issued for two people). But they can be fraudulently obtained and are frequently pilfered.

The importance of this problem cannot be overstated. Identifier resolution affects the collection of information on people who have no particular reason to evade scrutiny. Perhaps needless to add, a domestic intelligence agency is likely to spend the bulk[20] of its efforts on those who actively seek evasion. For the latter, the difficulties only multiply.

With rare exceptions, most of the information on us is information sorted by name; even the numbers we go by, such as the SSN, credit-card numbers, and passport numbers, refer back to a name. Alas, names are unreliable as unique indicators. First, many names are common to thousands of people. Second, people often use variations on their name: The first name in use can be the given formal name (e.g., William) or it can be informal (e.g., Bill, Willy), an abbreviation (e.g., BJ), a nickname (e.g., Shorty), or dispensed with in favor of a middle name (or show up as a last name in some languages). Middle names are used in some cases but not others. Last names can be altered by marriage or by the court. Names in languages that do not use the Latin alphabet (e.g., Arabic) have no commonly used transliteration into the Latin alphabet. Any attempt to look for a more flexible name-match algorithm (to increase the match percentage) will also increase the number of people who incorrectly have what appears to be the name of another person.

---

[20] Not everyone of investigative interest seeks to hide his or her identity. Terrorist financiers, for instance, may also be legitimate businesspeople who need a consistent, reliable identity to acquire their money in the first place.

Associating any one name with an unambiguous identifier will permit correlation only within the universe in which the identifier is used. Thus, financial and government records, generally keyed by a valid SSN, can be used to link name and SSN. Many other institutions whose transactions do not involve the federal government (e.g., private health insurers, cell-phone companies) and thus do not have a right to an SSN ask for one anyway. SSNs, however, commonly end up in the hands of data thieves, and the Social Security Administration receives tens of thousands of allegations of misuse each year (GAO, 2002a). Thus, for investigative purposes, they cannot be considered wholly reliable (Dempsey, 2005).

Institutions use other common identifiers, such as phone number or driver's license number.[21] Those who collect the institutions' data, however, would have no way of correlating such identifiers with an SSN unless supplied with a reliable crosswalk table—the existence of which raises all the issues noted.

So, it would seem that the dream (or nightmare) of a universal data repository of private individuals is a hopeless quest. Fortunately (or unfortunately), where there's a will and a wallet, there is frequently a way. Private data consolidators, such as Acxiom, ChoicePoint, or LexisNexis, have, for decades, faced the problem of correlating disparate data to a single individual. In response, they have developed sophisticated algorithms for correlating data chunks (e.g., a filled-out form) with particular individuals by looking for matches and near matches on names, addresses, telephone numbers, SSNs, and the like. Their results are not perfect; almost half of us have some serious errors in our credit reports. However, they must have had sufficient credibility to convince customers (e.g., loan officers, potential employers) to use billions of dollars worth of their services. After the September 11

[21] These days, with most providers using the address-limited Internet protocol version 4 (IPv4), many—perhaps most—users receive a new Internet protocol (IP) address every time they connect with their Internet service provider (ISP), so they lack permanent addresses in cyberspace. If and when the switchover to IPv6 takes place, the Internet address space will become much greater, thereby permitting every user to acquire a permanent address. Such an address could be a reliable identifier if implemented that way.

attacks, even the federal government turned to their data coffers and expertise to search for terrorists.

Hence the point of this section: Data privacy is not merely a matter of what federal officials and their computers see but may well be a matter of what data consolidators and their computers see. This assumes that the federal government will need name identifier–resolution algorithms but cannot or will not choose to develop its own. *If* a new domestic intelligence agency can acquire the algorithms used by data consolidators or can contract with them to bring experts in-house (and bind them by federal rules, such as those associated with the Privacy Act), then little complication arises from needing name identifier–resolution services. But will the data consolidators be so eager to relinquish control over the very capabilities that define their core competence? Or will they insist on taking the data in-house to resolve name-identifier issues on their own (e.g., the algorithms they have require data the government does not collect)? If the latter, what safeguards are needed to ensure that the information that the federal government was able to amass using its subpoena and national security–letter powers is not used to make other determinations, such as credit reviews, or does not wend its way into yet other hands? These are issues that have to be addressed in the overall question of balancing the needs of domestic intelligence with those of privacy.

Other Federal Agencies

Many other branches of the federal government will be the source of personal information that may or may not feed into the activities of a new domestic intelligence agency. The latter, after all, is unlikely to be a direct intermediary in the day-to-day lives of many Americans, much less most of them. Thus, the rules that govern the privacy trade-offs for this agency will, not, by themselves, protect privacy or enable domestic intelligence on their own.

Some federal agencies—notably the Census Bureau and the Internal Revenue Service (IRS)—have their own strict privacy and confidentiality rules. They are unlikely to offer or be compelled to offer their information to the domestic intelligence agency without drastic

changes in how (and thus how well[22]) they operate. Others, such as those that fund health care (e.g., the Centers for Medicare and Medicaid Services), tend to follow certain professional norms that would exclude mass turnovers of data for intelligence purposes, although they might do so for other ends, such as disease surveillance. Agencies that come under the Department of Homeland Security (DHS), however, are more closely attuned to the needs of domestic intelligence, and the use of their data may well be possible, particularly as their policies evolve. They include Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), and TSA.

TSA is of note because its approach to the security/privacy tradeoff has attracted attention. At present, flight manifest data are collected on international flights (to help ICE preview passengers whose actions may raise customs issues), but data for domestic flights are not seen by the federal government. Instead, the federal government gives the airlines long lists of all no-fly passengers and has them screen their ticketed individuals against this list in order to keep security risks off airplanes. TSA is proposing a new system, Secure Flight, which would have the airlines give TSA each passenger's name and proposed itinerary (possibly along with gender and date of birth) (Berrick, 2007a). TSA would then attempt to determine whether the passenger is on the No-Fly List. Were such information to be amalgamated for, say, an entire year, TSA would have a record of all the airborne comings and goings of tens of millions of passengers. Currently, Secure Flight is designed so that records are eliminated a week after the relevant flight lands. However, the privacy statement that accompanies the notice of proposed rulemaking (TSA, 2007) also states that such data can be turned over to law enforcement agencies pursuant to TSA's or law enforcement agencies' responsibilities under 5 U.S.C. § 552a(b)(1). Exactly what might constitute sufficient cause for TSA to turn over *all* of its records remains to be determined—but if a wholesale evasion of the Privacy Act to support widespread profiling were deemed counterproductive to TSA's original mission, a domestic intelligence agency

[22] On the premise that breaching the data fortresses of Census and the IRS will, when discovered, reduce the level of voluntary compliance with their inquiries.

may not get all it wants from TSA. Conversely, if the information is turned over to another entity, there will be a privacy risk, although how much of a risk depends on what other personally identifiable information *that* agency has.

The larger point stands: The domestic intelligence agency may make one trade-off between privacy and security, and those that feed the agency may make a completely different trade-off.

Conclusions

Trading off security for the nation and privacy for the millions is tricky, particularly if the reason for gathering the data stands on ground no firmer than the hope that terrorists and others can be identified through what is essentially profiling. Nevertheless, if one assumes that profiling is valuable and that it requires gathering data on large numbers of people, a reasonable trade-off may be possible. In this chapter, we have explored the basis of a policy for navigating privacy issues in a new domestic intelligence agency or, since intelligence collection could be broadened even without the organizational change of creating such an agency, how these issues could be addressed more generally.

The basis for the trade-off lies in making distinctions between (1) data that are gathered by computer and are never seen by human analysts (the lowest degree of violation), (2) data that are seen by people but not used in making decisions about the individuals whom the data reference (a higher degree of violation), and (3) data that are used in making decisions about people. The last is particularly problematic if people have little opportunity to challenge the data.

Leveraging these distinctions leads one to a trade-off that emphasizes keeping people and computers separate. In a plausible scheme, data would be requested from providers (e.g., phone companies) and transferred to a central, stand-alone facility in encrypted form. Algorithms would be applied to those data. Some algorithms would carry out general profiling; others would be specific to a particular characterization. Such algorithms would be tested on real but anonymized data with strong controls and sited away from the domestic intelli-

gence agency. The range of data requested would be announced, and individuals would be permitted to see what data existed on them. The algorithms would remain secret, although their basic parameters would be made available to ombudspeople. Data on individuals whose activities raise further interest would be released if a third party could be convinced that the probability of interest met some test (ranging from, perhaps, reasonable suspicion to probable cause). Such techniques as data minimization would be used to vet data requests, and auditing would be in general use as a safety measure. However, there would be less reliance on anonymization or off-site data housing as protections.

This constitutes one way to trade privacy and security off one another. There are likely to be others of equal plausibility depending on the nature of what is being sought, how far the domestic intelligence agency can or cannot be trusted, and the state of information-security technology.

CHAPTER EIGHT

Exploring Measures of Effectiveness for Domestic Intelligence: Addressing Questions of Capability and Acceptability

Brian A. Jackson

The basic mission of domestic counterterrorism (CT) intelligence is the *prevention* of terrorist attacks by identifying and disrupting the activities of small violent groups inside the country before they can cause harm. While that mission is straightforward to say, determining whether one way of pursuing it is better than another—e.g., whether it is in the nation's interest to create a new domestic intelligence agency or make other changes in existing activities—requires a reasonable way of defining what *better* means. Previous discussions in this volume have discussed different organizational and other options related to the design of domestic intelligence activities, each of which would have implications for how—and organizationally where—these different functions would be carried out. Choosing among them requires that analysts and policymakers have reasonable and systematic ways to assess the relative merits of different options and make trade-offs between various models' strengths and weaknesses.

But how do we judge whether one way of pursuing a mission is better than another? In thinking about the performance of government organizations, there has been a focus in recent years on the development of performance metrics or other measures of effectiveness to both assess proposed programs and contribute to managing ongoing activities. Performance measures assess how efficiently organizations carry out internal processes (e.g., how long it takes to perform key tasks) and—where possible—monitor how those organizations produce the outputs and achieve the outcomes the country expected when it created or funded them. In the ideal, the right metrics can tell decisionmakers

and the public what they are getting for the money they are spending on a given program and, if they are considering making changes to government activities, a structured way to think through why a different way of doing things might be better than what they have now.

The concept of performance metrics for intelligence is admittedly a controversial one. While there are ready examples of accepted *process* measures for what intelligence agencies do, those examples often do not link those processes to the outcomes (e.g., warning, prevented attacks) that intelligence efforts are seeking to produce.[1] There are also examples of binary yes/no–type metrics for specific intelligence functions in a domestic context.[2] The factors that influence an intelligence organization's success and failure at achieving those outcomes may seem so unpredictable that the concept of developing performance measurement at all may appear misplaced.[3] As is the case in most organizations, improper application of metrics or the use of metrics that do not truly reflect what the organization is trying to accomplish can do more harm than good. But, while we would concede that there are certainly difficulties in applying performance measures to intelligence organizations, it does not necessarily follow that those difficulties abrogate the value of thinking through what metrics for those organizations' activities might look like.

Systematic thinking about what organizations are designed to do and how they are trying to do it provides, at the minimum, a way of analytically linking processes to outcomes and seeking to specify what "better performance" means in a useful way. In the context of terrorism prevention, it is easy to use outcomes in isolation as a purported measure of performance (e.g., the fact that there have been no attacks over a time period being used to support a judgment that what one is doing

---

[1] For example, in this research project, case studies were developed of five foreign domestic intelligence agencies, including an examination of measures they used to assess their performance (Jackson, 2008).

[2] See "Information Gathering and Recognition of Indicators and Warnings" and "Intelligence Analysis and Production" in DHS (2007c, pp. 81–102).

[3] Similar questions have been raised about the development of performance metrics for activities like scientific research, in which outcomes are shaped by factors that are at least partially outside the control of the organizations doing the work.

to prevent them is working) but that provides no insight into whether some adjustment to what the nation is doing now or an alternative way of pursuing the same mission might be superior. In the context of this study, not drilling into how the outcome of "no recent major attacks" has been achieved and not assessing the performance of the different activities that have contributed to achieving it means that policymakers and the public lack the information needed to decide whether a new domestic intelligence agency would be better than the status quo or distinguish among different models for such an agency.

As part of our study, one strand of our research was therefore to think about what different performance measures for intelligence activities might look like, at a level of specificity that would be useful for distinguishing among different ways these missions could be pursued, and how metrics for intelligence processes (e.g., collection of information) could be linked to the outcomes they are intended to achieve (e.g., prevented attacks). This effort was approached *not* with the intent of producing sets of metrics that could be directly applied to new (or current) intelligence activities, but rather to guide our thinking about how different intelligence-policy choices—e.g., alternative designs of a new domestic intelligence agency—could be compared.

This chapter presents the results of that exploratory effort. It describes (1) a simplified model of five intelligence functions (information collection, sharing, analysis, storage, and action based on that information) that, linked together as a system, produce the outcome of preventing terrorism; (2) notional performance measures for those functions, building from first principles about the functions themselves up to how they are intended to combine with one another; (3) since our focus was on *domestic* intelligence, exploration not just of measures of effectiveness but of measures of *acceptability* for intelligence efforts to the publics they are trying to protect; and (4) concluding remarks about the applicability and utility of this sort of thinking to questions about the design of intelligence efforts.

Given the goals of the effort and the approach, the results have both strengths and weaknesses with respect to different applications that the reader should keep in mind:

- Though we look at individual intelligence functions, e.g., collection, our focus is on how they fit together as a system to produce the outcome of preventing terrorism. This helps to avoid focusing *only* on individual functions and the risk of optimizing their performance even though the system in toto lacks the capability to convert better component performance into improved overall outcomes. We see this as a strength of this approach.
- We seek to use similar measures for the performance of intelligence organizations and their acceptability to the public. As other chapters have discussed, public opinion about intelligence is linked to such factors as the perceived threat and the performance of those organizations. We believe that looking at both sides of this problem together is superior to treating security and the factors that shape public acceptability (e.g., privacy, civil liberties) as separate, to be traded off against one another. While we believe that drawing this parallel is useful, it does risk oversimplifying more-complex issues and concerns.
- Because we are looking at individual functions (e.g., information-sharing), our thinking about metrics is specific enough to help work through policy options that may differ only in the way they approach individual intelligence functions (e.g., comparing intelligence information–technology systems with joint centers or task forces for information-sharing in which the central differences are in the modes and potential efficiency of how that sharing takes place). Drilling down to the functional level also, in theory, makes measures more actionable, since they are linked to specific activities "on the ground." However, specificity also makes measurement more—in some cases, much more—difficult.
- Due to challenges of measuring values for intelligence metrics in actual organizations and systems, the way we approached this problem creates real limits in the measurability of some of the metrics we discuss. Because our focus was using metrics to think through analytic problems (rather than, for example, to perform direct program or other evaluations), we did not focus on ease or difficulty of measurement as we were exploring different metrics. On the one hand, this could be viewed as a strength, as it avoids

the risk of choosing metrics *because* they are easy to measure, whether or not they relate directly to desired policy outcomes. On the other hand, metrics that are not readily measurable are unlikely to ever be useful for program evaluation and management. Though a weakness—and one certain to disappoint readers looking for measures that can be immediately and broadly applied—these more theoretical measures that we describe can still be a valuable step toward developing metrics that are more readily measured. Making clear statements of what we would *like* to measure is a necessary step to finding proxies that we *can* measure but that still relate to the policy outcomes we are trying to produce.

As a result, we do not answer all the relevant questions about metrics for intelligence in general, nor even for domestic intelligence in particular. Metrics can be used in a variety of ways ranging from program evaluation to much more modest tools to help structure and think about particular policy problems. With respect to policy evaluation, what we present here is, in the words of one peer reviewer, "a framework for *beginning* analysis" rather than the final word on appropriate metrics. However, for the purposes of asking policy questions like those in this study, such metrics still have value as a framework for analysis of policy choices and their potential effects.

The Need to Think About Intelligence Activities as a System for Linking Processes to Desired Outcomes

The first step in thinking through measures of performance for CT intelligence is to articulate the activities involved in achieving the desired outcome and identifying how they fit together. To prevent terrorist attacks domestically, intelligence and law enforcement organizations must be able to distinguish individuals, groups, or activities that pose a threat from those that do not. The ability to do so is tied to both the *sensitivity* of intelligence efforts (their ability to detect threats successfully) and their *specificity* (the ability to *not* identify nonthreats as hostile). Because just knowing that someone poses a threat or that an

attack plan is under way may be insufficient to keep an incident from happening, success is also tied to the ability to act effectively—and to act quickly enough to make a difference. From a broader policy perspective, the goal is to be *sensitive*, *selective*, and *effective* at an acceptable cost, so questions of intelligence policy relate not just to the capabilities of the intelligence system but also to how *efficiently* it delivers those capabilities.

As a result, it is useful to view the totality of domestic intelligence as including five components:[4]

- collection capabilities and required authority to gather information
- analysis capacity to identify and assess the data
- storage to retain relevant information for future use
- information-sharing and transfer mechanisms to move either raw data or analytical products to the individuals and organizations that need them
- capability, authority, and willingness to act on the information.

This general set of components captures the ingredients required for intelligence organizations to be successful.[5]

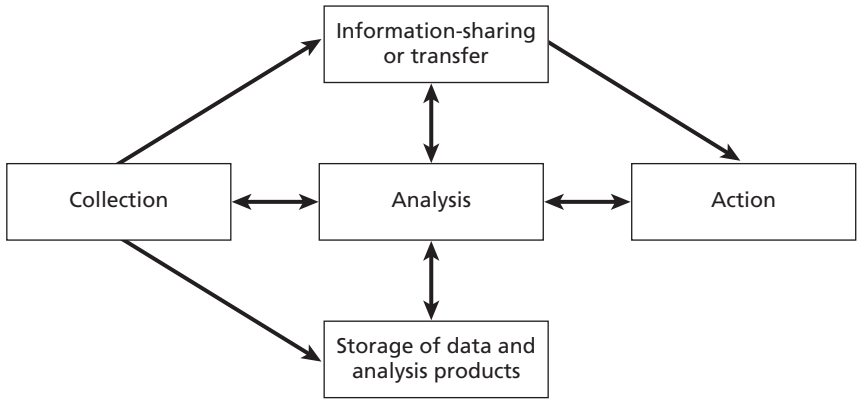
However, intelligence should not be viewed as a chain of these five pieces or its performance as the sum of the performance of each of the components in isolation. Though consistent success does depend on all five elements, feedback occurs between the different components (Figure 8.1).[6] For example, there is feedback between analysis efforts and what information is collected, what stored information is drawn

[4] A similar breakdown of intelligence-agency functions to enable consideration of metrics is available in Behrman (undated).

[5] In breaking down the process of intelligence activities into these stages, we have drawn on our and other previous work looking at how organizations learn. In our previous work, we applied a similar model to learning by terrorist groups (see Jackson, Baker, et al., 2005a, 2005b, pp. 179–190 and references therein).

[6] Because the goal of domestic CT intelligence is explicitly disrupting terrorist plots and likely must involve organizations outside what is labeled the intelligence community (IC),

Figure 8.1
Simplified Model of the Functions Making Up Intelligence and Counterterrorism Efforts



RAND *MG804-8.1*

on to inform current analysis, and so on. As a result, each piece should be viewed as part of a more complex intelligence and CT system rather than as a link in a linear chain of activities.

Our use of the word *system* is intended to emphasize that the outcomes of domestic intelligence efforts depend on how all these elements complement and integrate with one another. The fact that the system's performance depends on the performance of all of the parts means that payoffs of investments in one part of the process will be driven in part by the characteristics of the rest of the system—i.e., if the system cannot act on intelligence, major investments to raise the effectiveness of information collection may not actually translate into a commensurate increase in the performance of the overall system.[7] The absence of any of these ingredients can hamstring an intelligence effort, producing perverse outcomes where key data are not collected, information is collected but not examined until it is too late, the lack

this construct differs from the *intelligence cycle* used to describe the activities of traditional intelligence organizations.

[7] This systems view of these processes is echoed in Dempsey and Flint (2004) with respect to devoting resources to using commercial data in domestic intelligence efforts as compared to investments in other parts of this system.

of a memory of stored information makes it difficult or impossible to make sense of new data, or the truth about an individual or organization is known but never acted on. Overall effectiveness depends on the pieces of the system linking together and functioning as a whole, not just performing well on their own.

Exploring Potential Measures of Effectiveness for Domestic Intelligence Activities

To assess alternative proposals for a domestic CT intelligence agency, ideally, a policymaker would have quantitative metrics for the CT performance of current intelligence activities that could be used to assess how performance might change under different policies. As described in the opening of this chapter, in practice, it may or may not be possible to *measure* CT intelligence performance in this manner,[8] but the starting point for our analysis was the development of a set of ideal performance measures for each intelligence function that focused on what each was trying to accomplish and how accomplishing it contributed to the performance of the entire five-function system.

To craft the metrics, we attempted to distill the range of concerns surrounding domestic intelligence down to what drives its performance. We focused initially on the tactical goals of domestic intelligence (e.g., identifying individuals or organizations with violent plans and acting to interrupt their activities) and how the five component functions in Figure 8.1 related to those tactical goals. The measures that result can also be applied to more-strategic intelligence activities,

[8] For example, in the current version of the Department of Homeland Security (DHS) target capabilities list, which includes domestic CT intelligence functions, the majority of performance measures are binary yes/no–type assessments of activities (DHS, 2007c). In that document, measures are included that address each of our intelligence functional areas in various ways—e.g., that "information provided by all sources met predefined standards for accuracy, completeness and consistency" (p. 84) or that "intelligence related to high risk infrastructure or an acute threat was prioritized and reported as soon as it was observed" (p. 85). The document also incorporates by reference other standards and guidelines that include measures and requirements for analytic accuracy that are consistent with the more idealized and abstracted measures we describe here.

such as threat assessment, though what it means to act on the basis of such intelligence has quite a different meaning. As the metrics are introduced, their application to each of these branches of intelligence is introduced in parallel.

We incorporated measures that are directly related to CT outcomes (e.g., the fraction of hostile individuals or organizations of which intelligence agencies are aware at any given time, since the goal is not to miss terrorists in our midst) with elements focused on the *efficiency* of intelligence activities (e.g., the fraction of intelligence collected that that is about nonhostile individuals or innocent activities, since it would be inefficient to catch many innocent people or groups in preventive nets). Such efficiency measures are, in some cases, related to the cost of the effort as well as influencing potential effectiveness. Achieving intelligence outcomes in an ideal manner would correspond to maximizing our narrow metric assessing CT outcome while also minimizing our broader metric focused on efficiency. For the purposes of this section, these efficiency elements are discussed with respect to CT performance, though the reader will immediately see the relevance of such measures to questions about privacy, civil rights and civil liberties, and other concerns as well. We return to these issues later.

The following sections describe these ideal metrics for each intelligence function (summarized in Table 8.1).

Collection

Domestic intelligence activities cannot be successful if they cannot detect individuals or groups planning violent actions. As a result, a first measure for direct CT effects of intelligence efforts is *what fraction of the hostile actors or activities in the nation is the intelligence organization aware of at a given time*, where knowing about a larger percentage is superior to leaving a significant fraction undetected. With perfect intelligence, all adversaries would be known, making it possible to readily pick up any hostile actions they were in the process of planning or executing and correctly recognize those actions as hostile (see "Analysis," next in this chapter). Our framing of the metric based on the effect of intelligence on CT was deliberate; the goal is collecting on those actors

Table 8.1
Ideal Measures of Direct Counterterrorism Effect and Broader Efficiency and Effectiveness, by Intelligence Function

Intelligence Function	Direct CT Effect Measures	Broader Intelligence Efficiency and Effectiveness Measures
Collection	Fraction of hostile actors or activities in the nation of which the intelligence organization is aware	Fraction of collected information that relates to nonhostile actors and nonthreatening activities
Analysis	Fraction of hostile actors or potential threats on which information is available that are correctly recognized as hostile	Fraction of nonhostile actors, activities, or events on which intelligence agencies collected data that are misclassified as hostile
Storage	Fraction of retained data that are relevant to understanding potential threats and are both accurate and current enough to have value	Fraction of retained data that are not relevant to understanding potential threats or are inaccurate or sufficiently dated to be nonuseful
Information-sharing	Fraction of information available on hostile actors or potential threats that is shared within required time frames	Fraction of data or analysis products on nonhostile actors or irrelevant to potential threats that are shared beyond the collecting or originating organization
Action (capability, authority, and willingness to act)	Fraction of actors or activities classified as hostile or confirmed threats that are acted against effectively	Fraction of actions taken against nonhostile actors or in response to misidentified threats that result in unacceptable costs

who are hostile, not just collecting more intelligence. With respect to threat assessment, the breadth of coverage of potential threats is similarly important, though the focus might reach beyond specific actors to include other data and information needed to understand the threat environment.

Although the discovery of hostile individuals and organizations is the primary intended outcome of intelligence activities, using that alone to describe effectiveness provides only a partial picture. One way to ensure that all hostile actors are monitored would be simply to monitor everyone. In most contexts, this strategy would be impractical. Even assuming small resource costs for collecting information about any particular individual, those costs could add up quickly for large

populations.[9] If the results of broad collection efforts must be followed up by applying other resources (e.g., analyst time, tasking of police officers or special agents to carry out additional confirmatory surveillance), costs could add up quickly. Put another way, how tolerant an intelligence system can be of nonselective data collection depends on the costs of the subsequent analytical or operational filtering that must then follow to actually identify individuals, organizations, or activities of concern in that nonselective data set. If such efforts are inexpensive, the efficiency cost may be tolerable, but, if they are not, the efforts to follow up on what eventually prove to be nonthreats could waste scarce resources. This could reduce overall effectiveness by making it less likely that hostile threats would be quickly recognized—even if they are being collected on at the time. Similar arguments can be made about other functions.

Recognizing this, in the ideal, intelligence organizations' ability to *avoid* devoting information-collection resources to nonadversaries (or, in the case of intelligence threat assessment, gathering significant amounts of extraneous data) is also an element of their efficiency and effectiveness. A measure of this side of the equation is *what fraction of collected information relates to nonhostile individuals or groups and nonthreatening activities at any given time*, where the ideal goal is to maximize the fraction of hostile actors monitored while minimizing the fraction of information collected about nonthreatening individuals or activities, since doing so would produce the highest-value data.[10,11] Very broad collections on the general population would mean that a small fraction of collected data would relate to hostile actors and activities.

---

[9] Note that this formulation of a "value" trade-off between monitoring a smaller number of high-value individuals and capturing a large amount of information of limited usefulness is similar to an effectiveness measure for wire-tapping applied in Tsvetovat and Carley (2006).

[10] Even the ongoing monitoring of the innocent activities of known hostile actors imposes an efficiency price on intelligence systems. (The author acknowledges Paul Pillar for this observation.)

[11] The combination of these two measures is related to arguments made for the constitutional reasonableness of a search (see, for example, discussion of the National Security Agency, or NSA, warrantless surveillance program in Gellman, Linzer, and Leonnig, 2006).

In some cases, this might be necessary and could be a part of the process of learning how to recognize threats more specifically. However, it would require a later analytic investment to pull the signal from the noise in such a nonselective data set.

Analysis

For preventing terrorist plots, analysis is the "detection process" through which collected information is used to recognize an actor or activity as hostile. If the intelligence system is aware of a potentially hostile actor—i.e., information has been collected about that person, group, or their activities—the goal is to correctly *recognize* that actor as such. Analogous to other detection processes, the process should be sensitive (i.e., it should minimize false negatives), so the key positive measure of performance is *the fraction of monitored hostile actors or potential threats that are correctly recognized as hostile*.[12] In the case of more-strategic threat-assessment intelligence or other analyses of historical intelligence data, there is a similar demand to successfully recognize all relevant threats to reduce the likelihood that shifts in threat or the appearance of new threats will be missed.

However, the goal is also to minimize false positives—recognizing innocent actors or behaviors as hostile or nonthreats as threats. False positives are bad for the practical reason of wasting resources, but they have obvious civil liberties concerns associated with them as well. As a result, a counterbalancing efficiency and effectiveness measure is *the fraction of nonhostile actors (individuals or groups), activities, or events on which the intelligence organization collected data that were misclassified as hostile*.[13]

---

[12] Note that missing a hostile actor because no data had been collected about it would not reflect on the performance of the analysis component of the system, but of the collection component.

[13] The avoidance of such error is similarly relevant to strategic intelligence and threat assessment.

Storage

Considering measures for the storage component of intelligence activities is somewhat challenging, given the variety of uses to which such information can be put in analytical efforts and the variety of concerns associated with government organizations building and maintaining such databases. Stored intelligence information can be a key ingredient in analysis of both tactical and strategic intelligence. However, such information has value only if it is accurate and current.[14] Also, given that much intelligence analysis is a time-sensitive activity, such information is more valuable when it is not obscured in a database filled with unrelated, inaccurate, or otherwise distracting data. Such concerns about relevance, accuracy, and timeliness are no different for intelligence data than for most databases.[15] As a result, a positive metric for the storage function for intelligence efforts is *the fraction of the data that have been retained that are relevant to understanding potential threats and are both accurate and current enough to contribute to analytical efforts*.[16] What is meant by information "that is relevant to understanding potential threats" may differ a great deal among intelligence applications. In situations in which analysts do not yet know how to recognize particular behaviors as threatening or nonthreatening, information on broad populations may be relevant to determining how to do so (e.g., exploratory techniques, such as data mining, to try to pull weak signals from the noise of general-population behaviors). In other cases, in which distinctions between threatening and nonthreatening actors or activities are easier to draw, the differences may be clearer (e.g., keeping open and adding to files on individuals or groups that have no reasonable link to

[14] See English (2005) for a discussion of the quality of information (and use of metadata on information quality) as an example of measures that simultaneously reflect both intelligence capability and acceptability concerns.

[15] See Noblis (2007) for a much broader discussion of metrics that cover these types of data-quality concerns for operational information systems.

[16] See, for example, discussion in Posner (2006, p. 144) on shelf-life issues in intelligence data. We acknowledge that defining what the "right" shelf life is for data would differ across types of data, where some relevant to future threats might be useful for a long time, while other types of data on particular individuals (e.g., address information that would go out of date as people moved around) might have a much shorter useful life.

hostile activities). Though, in principle, a reasonable distinction—that stored intelligence data should be relevant to threat detection—this is not to say that, in practice, all will agree on the status of a particular piece or class of information or how "possibly relevant" is enough to justify keeping rather than discarding information.

Though accurate historical information helps analysis, inaccurate or outdated information could undermine intelligence success. A simple example is that storage of an incorrect or old address on an individual could mean that resources are tasked to monitor an irrelevant location. As a result, a counterbalancing efficiency and effectiveness measure relating to the storage of data is *the fraction of retained data that is not relevant to understanding potential threats, is inaccurate, or is out of date*.

Information-Sharing

Depending on the source or the way it was collected, the organization that first collects a piece of intelligence information may not be the right one to analyze or act on it.[17] Prevention success may therefore depend on how well information can get from one place to another. Because preventing terrorism is also time sensitive, the appropriate measure of benefit is *the fraction of the information available on hostile actors or other threats that is shared quickly enough that it can be acted on.* This measure applies equally well to tactical and strategic intelligence. A strategic assessment foretelling the appearance of a new threat is irrelevant if it is not delivered before the threat materializes.

Conversely, just as the inclusion of irrelevant information in intelligence databases could undermine success, broad sharing of information on individuals, organizations, and activities that are not hostile—or the sharing of flawed or otherwise unhelpful strategic intelligence—

[17] In our model of the domestic intelligence enterprise, information-sharing covers the sharing of information not just among federal agencies but also across levels of government and with other actors (e.g., relevant private organizations) with roles in domestic intelligence. With respect to the creation of a new domestic intelligence agency, information-sharing would still be required between that agency and the larger IC focused on foreign threats (e.g., Central Intelligence Agency, or CIA; NSA) to gain access to data relevant for domestic threat assessment and other activities.

could similarly risk overloading organizations and confusing their CT efforts. If important information is lost in a sea of irrelevant data, action on high-priority threats will likely be delayed. As a result, a counterbalancing efficiency and effectiveness measure for information-sharing could be *the fraction of data or analysis products on nonhostile actors or irrelevant to potential threats shared beyond the collecting or originating organization*.

Capability, Authority, and Willingness to Act

Actually preventing something requires not just knowing about it, but acting as well. This is achieved by acting against the individual or organization by altering the environment in which it operates (e.g., increasing security around its intended target), arresting individuals, or even using force. For broader strategic information on threats, action can include other changes in policy or operations to address or hedge to allow action in the future. Assuming that previous intelligence steps have identified hostile actors, behaviors, or other threats, the relevant measure here is *the fraction of actors or activities classified as hostile (or broader confirmed threats) that are acted against effectively*. For individuals or organizations identified as hostile, *effectiveness* is defined as action that disrupts their planned violent attack. Though strategic intelligence products, such as threat assessments, may not produce the same type of definitive action, such products are acted on in different ways. For example, in response to a change in the perceived threat, security postures at potential targets might be altered.

While quick and definitive action against hostile actors or activities is the ultimate preventive outcome, an argument similar to those made previously about the possibility of negative outcomes also applies to preventive action. Because it is unlikely that any collection and analysis system can be designed that will *never* misidentify an innocent person, organization, or activity as hostile, some actions will be mistargeted, and the concern becomes the consequences of that misidentification. When this occurs, the question is *what fraction of those actions taken against nonhostile actors or in response to misidentified threats results*

in unacceptable costs.[18] In the ideal, the costs associated with mistakes should be small and reversible so they can be readily remedied. Though this metric has clear implications from a civil rights and civil liberties perspective when action is taken against misidentified individuals or groups, it has intelligence-mission implications as well, since the aftermath of such mistaken action could significantly distract organizations from a focus on their core CT missions. The result of mistaken threat assessment could be changes in policy—potentially with substantial financial and other costs—that, while lacking civil rights and civil liberties concerns, could make the outcome very costly in other ways.

Interactions Among Measures

The success of the overall intelligence system relies on completing most if not all of the functions listed in Table 8.1 and illustrated in Figure 8.1. Prevention begins with collection but cannot be considered a success until effective action is taken. To this point, we have used this *system* language to emphasize that improving the outcomes of terrorism prevention relies on the success of all the steps, but it also has important implications for thinking about efforts to improve the performance of individual intelligence functions—and that such improvements cannot be viewed in isolation.

In thinking about the performance of the system overall, the central concerns are the sensitivity and specificity of its ability to detect and its effectiveness in acting in response to threats. A related factor is the cost of efforts in achieving acceptable levels of these characteristics. There are a number of ways in which sensitivity and specificity could be increased. For example, better analysis to recognize threats amid noisy data (e.g., where information on threats is hidden among much more information on routine activities) would be one way, but another would be to collect less noisy data initially so analysis is more straightforward. As a result, in pursuit of improved intelligence performance, there may be multiple options to achieve similar ends.

---

[18] While the ideal would be to not take actions against nonhostile actors, that is covered in earlier measures focused on not misclassifying innocent people or organizations as hostile.

Conversely, because overall performance of the system depends on how well all the pieces work together, investments in improving the performance of one might not result in a proportional improvement in the performance of the system overall. For example, though it might initially seem reasonable to attempt to monitor as many individuals as possible to increase the probability that all hostile actors are being watched, there are practical reasons that intelligence organizations might seek to limit monitoring of nonhostile individuals. Broad monitoring could reduce *overall* effectiveness by making it less likely that hostile threats would be correctly and quickly recognized—even if they are being monitored at the time. This type of argument could be applied to the use of data-mining technologies where they are being used to generate more leads for intelligence agencies to follow in an effort to find unknown cells. If the system is already strained following leads generated by other means, the generation of more leads will either saturate the system or mean that some leads will have to be ignored.[19] Similar arguments can be made about other functions as well. While broad and complete information-sharing might appear to be unequivocally positive, if important information is lost in a sea of irrelevant data, action on high-priority threats will likely be delayed.

---

[19] In an analysis of the British CT experience, an intelligence officer's views, reported by Michael Herman (2003, pp. 43–44), are instructive in this respect:

> [T]he job of the intelligence officer is to identify those strands that are worth pursuing and then to pursue them until either they are resolved, or they start to look flakey and not worth pursuing, or there is nothing more that can usefully be done. It is a risk management process. The number of potential leads that can be followed is virtually infinite. On the other hand, covert investigation is extremely resource-intensive and impinges on the human rights of the subject. The threshold for such investigations is therefore high and the number of investigations necessarily limited. Consequently many potential leads have to be discounted. Decisions on which leads to pursue are vital, but they are also complex and rich in judgement.

See also discussion in Martin (2004) regarding the balance between following leads and seeking to generate new ones.

Measurement Challenges

If information was available to populate each of the measures laid out in Table 8.1, it would be possible to assess the effectiveness and efficiency of current CT intelligence efforts or, for a proposed program, how much better or worse a different policy might be. Data for some of the measures could be gathered (e.g., information on the quality of data in intelligence databases or how quickly the system can respond to detected threats) but would have obvious security concerns. Other data (such as the fraction of hostile actors discovered) are unknowable in any exact way—though more-general indicators, such as the absence of attacks, can provide some insight. This reality means that, to assess their performance, intelligence organizations frequently must fall back on measures that focus on intermediate process measures, or metrics of the efficiency or effectiveness of the individual elements in isolation (e.g., fractions of intelligence-collection requests satisfied, not fraction of hostile actors detected), instead of linking their efforts to the outcome performance of the system as a whole.

However, even in the absence of the ability to directly collect data for these types of idealized measures of effectiveness and efficiency, they have utility for considering potential changes in intelligence policies, including the creation of a new intelligence agency. By thinking systematically through core functions and identifying specific outcomes for different domestic intelligence activities, they can provide a basis for comparing alternatives in a more rigorous—if still qualitative—way. For a proposed change in structure or function of intelligence activities, how do we think performance will be improved? Is the benefit of a new organization or initiative likely to be better effectiveness or improved efficiency (i.e., which set of measures is the basis for the case for change)? Is improved performance expected in just one intelligence function or across multiple functions? Even if the data are not available to make such arguments in quantitative terms, more-specific qualitative arguments—using a framework like that provided by the measures we discussed—can play a part in improving debate and policy choice. Metrics such as these also provide the starting point for identification of proxy measures that are more readily measured, a topic to which we return at the end of the chapter.

Beyond Measures of Effectiveness: Exploring Measures of Acceptability and Factors That Shape the Legitimacy of Intelligence Activities

Whether or not a new domestic intelligence organization—or any intelligence effort—is effective, the domestic or international public may or may not view its activities as *acceptable*. In spite of even provable and disclosable successes, if the public deems an intelligence program's efforts overall to be noncredible, illegitimate, or threatening, the program's activities will not be politically sustainable.[20] As a result, for evaluating potential changes in intelligence policies, thinking about what *measures of acceptability* might look like is as important as understanding what *measures of effectiveness* might be used to compare policy options.

Using the analyses and information presented in other chapters, we identified elements that have driven public concern about intelligence efforts. These issues and controversies provided the basis for exploring what measures related to the acceptability of intelligence activities might look like. Without repeating elements discussed elsewhere, we note that public debate of intelligence activities frequently involves such concerns as the monitoring of innocent people and the effects of that monitoring on their behavior and freedom, storage of information about individuals and the risks to their privacy from its disclosure, actions taken against individuals based on intelligence data, the costs those actions impose, and individuals' ability to challenge those costs through legal and other processes.

Without overly stretching our framework of measures presented in Table 8.1, many of these factors that have stimulated public debate on intelligence can fit readily into the second column of our framework of measures. Though we presented these factors in the previous section in terms of intelligence *efficiency*, they parallel issues that have been raised about intelligence efforts' effects on the public—and, therefore, issues that have served as catalysts for questioning the legitimacy of

[20] For example, interviewees during the study were split as to whether they thought public concern about privacy and civil liberties would make it difficult or even impossible to create a new domestic intelligence agency.

those activities. For example, while a measure like the fraction of monitored nonhostile individuals or groups that are misclassified as hostile (the false-positive rate for intelligence-analysis activities) is a measure of the *quality* of intelligence activities, it is also a measure of the potential civil liberties effects of those activities. Misidentifying an innocent person as a terrorist, whether by mistake or intention, is the first step in a process that could result in that person being denied their freedom, producing a civil liberties cost to them personally and on society as a whole. Similar arguments can be made regarding privacy and the fraction of the population monitored by intelligence activities, the information stored about individuals, and so on.

In examining our efficiency measures as a starting point for thinking about measures of acceptability for intelligence efforts, it is clear that how these measures relate to public opinions and concerns will likely differ among intelligence efforts. For example, for government organizations to store data that are not directly related to understanding current and future threats, people may care more or less based on what the data are and their sources. Differences in how they are stored (e.g., in personalized versus anonymized form) will also likely be a driver. As a result, though these measures provide a starting point for helping to think through these issues systematically, the particulars of their use in different cases will most likely differ.

It should be noted that, though covering many of the privacy and civil liberties concerns about intelligence, the measures of intelligence efficiency and effectiveness in the second column of Table 8.1 do not include *all* of the potential costs of intelligence that policymakers or the public might want to minimize or to include in a comprehensive set of intelligence metrics. For example, this analysis has been silent on financial costs. Society might be perfectly happy to accept less-selective intelligence (e.g., not minimizing the fraction of the total population being collected on) if doing so would reduce the cost of those efforts considerably—that acceptance would not be reflected here. Other relevant factors and concerns are likely left out by the simplification inherent in crafting this abbreviated set of measures.

Measurement Challenges

Just as collecting the data needed to make real measurements was a problem for using metrics of domestic intelligence performance, it is also a challenge in thinking about metrics of acceptability. In the first case, the question was whether the information necessary to measure or estimate the values of the metrics was readily available or knowable at all (e.g., the insurmountable problem of knowing how many terrorists have not been discovered). In this case, it is a question of what of that information is available *to the public* and, therefore, what citizens will use as the basis for their conclusions about intelligence activities.

While much of the data for assessing intelligence efforts' effects on the public are knowable—for example, based on analysis of how information is collected, past analytical success and failures, and how information is stored or discarded—it is not readily available to the public.[21] There are good reasons that some of this type of information cannot be broadly released. For example, disclosing the fraction of the population that is being monitored and in what ways might undermine the effectiveness of the monitoring effort.[22] Other data are periodically released (e.g., as a result of legislative or other reviews of intelligence activities when problems come to light or through the activities of internal oversight functions, such as privacy offices or inspectors general) but are not released on any regular basis.

While a lack of the necessary information might lead intelligence agencies to decide not to use metrics to assess their own performance, nothing prevents members of the public from drawing their own conclusions about whether intelligence efforts are acceptable based on whatever information they have. As a result, judgments about acceptability will not be driven by the *real* values of the sorts of measures we have described, but by *what the public thinks* those values are. In the absence of actual data to support those judgments, perceptions may

---

[21] See, for example, the remarks of David Cole (2003) on this issue.

[22] Note that it may matter *why* the public believes that secrets are being kept for their potential effect on judgments about intelligence legitimacy, credibility, and acceptability. For example, acceptance that secrets are being kept for good reasons will have a different effect than a belief that information is not being released to avoid embarrassment or political conflict.

diverge significantly from reality. For example, discussing the 2007 release of the CIA documents known as the "family jewels," describing past agency misdeeds, director Michael Hayden was quoted as saying that "when the government withholds information, myth and misinformation often 'fill the vacuum like a gas'" (Shane, 2007). As discussed elsewhere in this volume, if the conclusions drawn by the public based on that myth and misinformation result in major shifts in opinion or larger controversies, this can have major implications for intelligence organizations and the political sustainability of their activities.[23] Transparency and openness in intelligence activities, to the extent to which they can be pursued, are the obvious antidotes to this potential.

Further complicating matters is the fact that even the same value of a measure—e.g., what fraction of the general population is monitored—will vary in importance over time as public threat perceptions shift (see Chapter Four). When threats are seen as high and monitoring efforts are seen as producing protective benefits, even a high level of monitoring might be acceptable. At another time, the same activity might be viewed as unreasonably intrusive.

Conclusions

Comparing different ways of creating a new domestic intelligence agency—or making any significant change in intelligence policy—requires ways of assessing how the change will affect the ability to achieve the goals the intelligence enterprise is charged with pursuing. As part of our thought process for considering the creation of a new domestic CT intelligence agency, we explored how developing measures of what domestic intelligence efforts are trying to accomplish—

[23] For example, the major public reaction to the nature of programs like Total Information Awareness (later, Terrorism Information Awareness) (TIA) (TAPAC, 2004; Dempsey and Flint, 2004, p. 1461; Markle Foundation Task Force, 2006, p. 24), the Multistate Anti-Terrorism Information Exchange (MATRIX) (DHS, 2006c; Markle Foundation Task Force, 2006, p. 24), and the computer-assisted passenger prescreening system (CAPPS) II (Markle Foundation Task Force, 2006, p. 24) that contributed to their significant modification or termination.

and the broader effects of those efforts on society—might contribute to analysis.

In our exploration of potential measures of effectiveness, we broke down intelligence activities into specific functions so we could think more specifically what success meant for each of them, but, at the same time, we focused on how each function contributed to intelligence outcomes. For example, our notional metrics for collection were not focused just on gathering more information but on gathering more information about hostile actors and activities as selectively as possible. Even without considering whether or not the notional metrics are measurable in practice, the framework they provide for thinking through policy changes is useful. Put simply, supporting the argument that creating a new domestic intelligence agency will strengthen the nation's CT performance requires (1) laying out which of these metrics will be affected by doing so and (2) how an organizational reorganization will improve them. For example, consider the following:

- Do we think creating a new agency will result in the country recognizing a greater fraction of the hostile actors and their activities within U.S. borders? If so, how? It is difficult to make an argument that organizational change alone would immediately make collection significantly more effective or better targeted. Is the assumption that reorganizing will improve collection capability actually an implicit assumption that a new agency would be doing *more* collection than is going on currently? If so, the benefit being attributed to creating a new agency should more accurately be viewed as being the result of expanding collection, not reorganization. There are other ways of broadening collection (if that was the desired policy change) that do not involve creating a new intelligence agency.
- Do we think performance would be better because information-sharing—that now has to happen among many organizations at all levels—would be improved in a new agency? Again, if so, how? How certain are we that sharing of information among the components of one organization would be better than sharing among different organizations? Even if we assume that sharing would be

better, would the effect be enough that it would affect overall CT outcomes?

- Such a framework of measures, coupled with an understanding of the realities of the U.S. system, can also potentially help simplify thinking about organizational and other changes. For example, whether or not a new agency was created, taking action against suspected terrorists in the United States will almost certainly remain a law enforcement matter rather than being vested in a newly created intelligence agency. As a result, whatever benefits might be expected from creating a new agency, an improved ability to act against suspected adversaries would most likely not be a contributor.

Similar questions—and follow-up questions—could be posed about the other functional areas as well. This qualitative application of the metrics could similarly be used to compare potential alternative models for a new agency, such as those discussed in Chapter Six. For example, the attractiveness of a model focused entirely on information-sharing compared to that of other ways of reorganizing or simplifying the domestic intelligence enterprise would depend how great a contributor improvement in that area would be to better overall performance. Rather than being used empirically to score different policy options, the metrics instead act as a framework for asking questions about particular policies (e.g., do we think that this change will have more effect on collection or on analysis?) or a structured way in which to compare one policy to another (e.g., does policy change A potentially improve more of the metrics than does policy change B?).

Assessing the relative effectiveness of intelligence options is one part of policy analysis, but—particularly in the domestic arena—understanding the public acceptability of policies is another. In the review of the literature on those issues (see Chapter Four), shortcomings in available polling data—and how responses to the questions that are asked relate to actual views on complex intelligence issues—are a problem. When polls ask broad, general questions about abstract issues, such as the balance between security and civil liberties, it is not always clear how to relate the responses to specific policies. Making

the abstract, composite activity of intelligence more tangible by breaking it down into its component functions was useful for framing *analytical* questions about different policy options. Doing so would seem similarly useful for framing more-tangible poll questions for assessing public views about intelligence activities and for measuring public perceptions about both the scope and effectiveness of current CT efforts. Developing more-structured and concrete ways to measure what members of the public think their government is doing and how they feel about it could make it possible to get away from trying to divine trends from the tea leaves of periodic poll questions on broad topics, such as threat, security, privacy, and civil liberties.

But what about the more ambitious goal of crafting readily measurable metrics that could be used for evaluating intelligence activities and assessing policy alternatives *quantitatively* rather than *qualitatively*? Though some of the metrics discussed here are not measurable themselves, they could be viewed as a step toward the development of measurable proxies for the underlying metrics of interest. It may not be possible to have a real-time empirical measure of the fraction of the data in a database that relates to hostile actors or threats, is accurate, and is current, but data-quality indicators based on use or routine auditing (e.g., what is the oldest piece of data that has been retrieved and used and what fraction of the data is older than that? How many entries have been established during routine analysis or audit to be incorrect in a period, and have those entries been corrected or purged?) could provide insight by inference. Similarly, while real-time measurement of whether analysis has misclassified some hostile actors as nonthreatening is clearly impossible, the results of analytical quality-control processes, lessons learned, and—if they occur—terrorist actions taken by individuals of whom intelligence services were aware could provide retrospective indicators for this measure. If such assessments and processes occur systematically over time, some inferences could be made about trends in the system's detection performance.

In considering how one approach to domestic intelligence might be compared with other possible ways of pursuing the same mission, we examined how crafting performance metrics for these activities might guide thinking. We did not craft metrics that could be picked up

directly and applied in all of the contexts in which intelligence organizations' performance might be a concern. However, we did not set out to do so. Rather, the structure inherent in breaking down what intelligence agencies do into a workable set of functions and assessing how the performance of those functions contributes to achieving the desired outcome of terrorism prevention—and what *better performance* might mean for each of those functions—is instead useful for other purposes. In the context of this study, this sort of thinking could be applied to help in qualitative—though systematic—comparisons of different ways in which domestic intelligence could be structured. However, such thinking could also provide a starting point for developing better and more-measurable metrics that could make other contributions to understanding and improving intelligence performance.

CHAPTER NINE

Exploring the Utility for Considering Cost-Effectiveness Analysis of Domestic Intelligence Policy Change

Brian A. Jackson

As part of weighing a proposed change in public policy, analysts frequently attempt to calculate the policy's expected benefits and compare them to the expected costs of making the change. A focus on cost-benefit–type analyses has been prominent in a variety of policy areas, with the intent of ensuring that public policies achieve the goals they are intended to and do so at an acceptable cost. Though the use of these techniques is more common in regulatory areas, the extensive changes in policy that have occurred since September 11, 2001, in response to the threat of terrorism have led to calls to apply cost-benefit assessments in the homeland security area as well.[1]

In some cases, truly quantitative cost-benefit analysis is possible (e.g., for modifications in regulations in which both the outcome of the change and the costs of implementing it can be anticipated with some certainty). In others, difficulty in assigning values to important effects of policy change makes such rigorous cost-benefit comparison impossible. In such cases, however, even a *qualitative* cost-benefit approach can be useful to discipline thinking and ensure that important policy effects are not being ignored when considering whether a particular change is attractive and how its positive and negative effects will be distributed.

[1] For example, deliberations at the Office of Management and Budget in the Executive Office of the President in 2003 discussed in Skrzycki (2003) and Andrews (2003).

Counterterrorism (CT) intelligence is such a policy area in which the exact calculation of costs and benefits is difficult if not impossible. However, while it may be impossible to construct an exact balance sheet capturing the full range of benefits and costs associated with creating a new domestic intelligence agency, the structured thinking of cost-benefit analysis and related techniques can still be useful. As in previous chapters, which sought novel ways of examining policy decisionmaking regarding domestic intelligence and the potential creation of a new domestic intelligence agency, as part of our overall analysis, we examined how approaches derived from cost-benefit analysis might be applied, at least qualitatively, and the value of the analytical process they involve for considering these types of policy changes.

This chapter presents our qualitative cost-benefit approach to domestic CT intelligence activities by (1) examining the types of benefits and costs that are associated with intelligence actions, (2) exploring how values for both might be estimated for different types of costs and benefits, and (3) using those values to apply the technique of break-even analysis to think about the balance of the costs and benefits of intelligence efforts or specific changes in those activities.[2]

What Types of Benefits and Costs Are Associated with Domestic Counterterrorism Intelligence Activities?

The starting point for any cost-benefit–analysis effort, whatever the policy area, is identifying the relevant costs and benefits involved. Determining what effects must be accounted for in analysis is part of defining the problem and identifying what is involved in solving it: Ignoring important components on either the cost or benefit side of the policy equation risks producing outcomes in which policies either will not accomplish their intended ends or will do so at a cost that diverges considerably from expectations. Given the range of effects of

[2] It should be noted that, while we have framed this discussion as focused on exploring the creation of a new domestic intelligence agency, this approach is a general one and could be used to weigh other changes in intelligence policy as well.

many policy changes, it is often not possible to include every conceivable cost or benefit in such an analysis. Because of the breadth of effects that creating a new domestic intelligence agency is likely to have, that is the case here. Identifying major costs and benefits and systematically deciding which to include or exclude is therefore an important part of framing the policy problem for consideration. The costs and benefits we identified as illustrative both of their variety and range of magnitudes are discussed briefly in the following two sections. Some factors identified are general ones that would apply to many types of intelligence-policy changes, not just the creation of a new agency (e.g., benefits from improved terrorism-prevention capability). Others are more specific to reorganization.

Benefits

For CT intelligence activities, the basic benefit that is being sought is the *prevention of terrorist attacks* that would occur in their absence. Terrorist attacks themselves involve significant direct costs, such as physical damages to structures or vehicles, individuals injured or killed, and the costs of the disruption to life and commerce they produce. Terrorism can produce other costs as well, including expenditures for preparedness measures to respond to attacks that are not successfully prevented and costs associated with changes in individual or organizational behavior because of the perceived threat of future terrorist attacks.[3] These more indirect costs are shaped by individuals' perceptions of the security environment (e.g., personal behaviors can differ considerably if the assumption is that terrorism is a rare event versus an expectation that an attack will occur tomorrow) and by trust in the government organizations that are charged with preventing terrorism.[4] To the extent that effective intelligence activities—or visible security, policy, or changes in domestic intelligence activities—reduce the per-

[3] For a review of the economic costs associated with terrorism, see Jackson, Dixon, and Greenfield (2007).

[4] A more extensive discussion of how public views of security and changes in behavior can produce substantial additional costs of terrorism is included in Jackson, Dixon, and Greenfield (2007).

ceived need for other expenditures or limit otherwise costly behavioral changes, these should also be viewed as policy benefits.

Although an intelligence activity may be focused on the threat of terrorism, it is possible that it could *contribute to achieving other government missions*. CT intelligence efforts seek to identify individuals or organizations planning or preparing for future violent action. Beyond the fight against terrorism, intelligence collection by government organizations plays roles in detecting and gathering information about other illegal activity, including individuals or organizations involved in violent crime, narcotics trafficking, money laundering, smuggling, or other illegal activities. Indeed, intelligence efforts have been a central element in government targeting of such activities for many years.[5] As a result, even if an intelligence effort was put in place and focused primarily on the threat of terrorism, it could produce benefits in these other areas as well.

Depending on the specific CT intelligence activities being assessed, *indirect benefits* could also accrue distant from the initial intent of the programs' or organizations' mission areas. For example, one element of recent homeland security activities has been a focus on strengthening identification requirements both inside the country (e.g., the Real ID program) and at the nation's borders (e.g., passport requirements that are part of the Western Hemisphere Travel Initiative). While tightening identification requirements might reduce the ability of individuals with violent intent to remain anonymous, enter the country, or obtain trusted positions that would enable them to cause further harm (e.g., the Transportation Worker Identification Credential, or TWIC, program), it could provide other benefits as well. For example, the Associated Press reported that the requirements that travelers have passports to travel among the United States, Canada, Mexico, the Caribbean, and South America produced opportunities to catch noncustodial parents who were delinquent in child-support payments ("Passport Rule Helps Collect Child Support," 2007). Other possible benefits for

[5] See discussion in Chapter Three, which covers the role of intelligence activities across a range of missions.

strengthening identification requirements include reducing the potential for identity theft.

Costs

In considering the costs of intelligence activities or major changes like the creation of a new agency, the easiest costs to assess are those that actually have *budget outlays* associated with them. Government activities have annual costs associated with them that can be accounted for directly by the purchases that are made and people who are employed to carry them out. New intelligence efforts have a broader range of tangible direct costs. Purchasing a new technology or starting a new intelligence activity will have monetary costs associated with it, including those associated with making needed purchases and hiring appropriate staff.

Creation of new policies or programs may also have *transition costs* if, for example, staff for the effort are drawn from other current activities or if existing organizations must be reorganized to make way for the new effort. The founding of a new intelligence agency at the national level would be a significant change in the current domestic intelligence enterprise, and whether it was created de novo or built from existing pieces of current intelligence agencies or activities, it would have significant transition or transaction costs associated with it. Some of these transition costs may be tangible and easy to estimate. Others may be more abstract, such as reductions in the effectiveness of current efforts as a result of the upheaval required to make changes.[6]

Though direct costs of intelligence efforts can be substantial, many of the concerns raised about the price of improved security activity focus not on what it costs financially, but on more abstract and intangible metrics. To provide the basis for this part of our analysis, we identified a set of costs based on a review of the academic literature and public debate surrounding intelligence activities.

---

[6] The recent formation of the Department of Homeland Security (DHS) from elements of many independent agencies represented a very large-scale example of such a reorganization and is broadly viewed to have involved substantial transition costs.

As described in previous chapters, a central concern regarding intelligence activities is their effect on *privacy*. Views of what privacy entails differ, ranging from the idea that individuals or organizations should have the ability to converse or act in complete anonymity to much more limited definitions. From most viewpoints, privacy is inherently reduced by the collection and storage of information, whether those activities are carried out by the government or by other organizations or individuals. This implies that there is an inescapable privacy cost associated with many types of intelligence activities.[7] Admittedly, individuals and organizations differ considerably in the disutility or damage they perceive from different types of activities. However, to the extent that individuals and organizations see the gathering and recording of information on their activities as negative, it must be considered as one of the costs of intelligence activities.

The effect of intelligence activities on *civil rights and civil liberties* is another area of concern. The potential cost of intelligence efforts in this area can be quite direct and relatively easy to see—for example, the civil liberties impact on individuals and groups if the result of intelligence collection and use is the detention or arrest of innocent people or discrimination against individuals or members of particular ethnic or religious groups. In other areas, concerns about the effects of intelligence on civil rights and civil liberties are less tangible and more difficult to assess. For example, civil liberties organizations and analysts have raised concerns about a chilling effect from communication monitoring or information collection on individuals' willingness to exercise their freedom of expression, dissent, or assembly.[8] Individuals uncomfortable with government monitoring may also be less willing to seek the assistance of law enforcement organizations or other government agencies. This issue has been

---

[7] Although, as discussed previously, approaches do exist to reduce those costs for some intelligence activities.

[8] Solove (2006, pp. 493–495; see also discussion in Taipale, 2004) writes,

> Not only can direct awareness of surveillance make a person feel extremely uncomfortable, but it can also cause that person to alter her behavior. Surveillance can lead to self-censorship and inhibition. . . . [T]here can be an even greater chilling effect when people are generally aware of the possibility of surveillance, but are never sure if they are being watched at any particular moment.

raised in the context of debate of internal enforcement of immigration laws by state and local law enforcement and whether such efforts will lead illegal immigrants to fear calling the police if they are victims of a crime.[9]

Although many discussions of domestic intelligence activities focus on their impacts on U.S. citizens or residents, their *effect on the United States' reputation overseas* can produce real costs as well. Since September 11, 2001, changes in U.S. visa policies and an increase in the information gathered on foreign nationals at the border (e.g., collection of fingerprints upon entry to the country) have altered the experience of individuals coming to the United States to visit, work, or study. If those changes in views result in reductions in tourism and other cross-border economic activity, they will produce costs of their own.

It is also the case that a change in policy or organization like the creation of a new domestic intelligence agency will have *indirect governmental costs* that may be difficult to anticipate. Just as intelligence activities could create indirect benefits in achieving other government missions, new intelligence organizations or policies could increase friction in government action that might produce added costs. For

---

The impact of a chilling effect has also been invoked with respect to members of intelligence organizations, to describe the effect on intelligence practices after the reforms of the 1970s were imposed:

> The constraints embodied in the newer rules created a new atmosphere that had "a chilling effect" on police intelligence operations. . . . The rules created a minefield in the midst of what was a murky business anyway. . . . [I]f a decision fell anywhere in a grey area, [leadership] vetoed it to be on the safe side. . . . Under the newer rules, a wrong decision could mean criminal prosecution. Previously, such matters were handled administratively (within the law enforcement agency). . . . Uncertainty and fear provoked overreaction. Investigators no longer did things they in fact were allowed to do. . . . It is not merely a matter of error or overreaction on the part of the investigators. The atmosphere affected everyone. (Wildhorn, Jenkins, and Lavin, 1982, pp. 100–101)

The similarity of the description to the potential chilling effect of intelligence on individuals' exercise of their rights is striking.

[9] While frequently raised in terms of immigration and law enforcement organizations, similar arguments could be made with respect to the involvement of other public organizations, such as fire departments or emergency medical services (EMS) personnel in intelligence efforts (see, for example, discussion in Salyers and Lutrick, 2007, or Petrie, 2007).

example, if a new intelligence agency creates one more organization with which existing agencies must coordinate policies or adds an additional voice that can veto changes in ongoing activities, that friction could reduce the effectiveness of other intelligence—and, potentially, nonintelligence—efforts. In the process of policy development and coordination, the costs associated with having an additional organizational actor at the table can be more than the transition cost of buying a larger table and adding an extra chair.

Similarly, when we walked through the potential benefits of a CT policy, an indirect benefit that we highlighted was a reduction in demand for other security and preparedness measures due to the increased feelings of safety caused by the new policy or organization. That reduction is indeed an unambiguous benefit if those increased feelings of safety are well grounded and based on the effectiveness of the policy change. However, if people feel safer simply because a change has been made rather than due to an actual change in the risk, the inaction stimulated by the change in perception might produce longer-term costs even if expenditures are reduced in the short term.

Summary of Cost and Benefit Types

In our exploration of the potential costs and benefits of a significant change in domestic CT intelligence, such as the creation of a new agency, our goal was not to identify every possible cost and benefit. Because of the scope of our analysis and the complexity of the potential effects of the policy change, such a high-resolution examination was beyond the scope of our effort. Instead, we sought to identify a set of illustrative costs and benefits (summarized in Table 9.1) that demonstrated the potential variety in both their nature and their scale. Our thinking about how these costs might be estimated and assessed is discussed in the remainder of the chapter.

Table 9.1
Summary of Illustrative Costs and Benefits of Intelligence-Policy Change

Benefit Types for CT Intelligence–Policy Changes	Cost Types for CT Intelligence–Policy Changes
Prevention of terrorist attacks	Direct and transition costs
Reduction in indirect costs from perceived terrorist threat	Additional budget outlays for new policy or activity
Security and preparedness expenditures	Costs required to transition from current to new policy
Costs from changes in individual or business behavior	Indirect or intangible costs
Contributions to achieving other government missions	Privacy reduction
Indirect benefits	Curtailment of civil rights and civil liberties (direct and indirect)
	Effect on the United States' reputation overseas
	Indirect governmental costs

How Can the Benefits of Domestic Counterterrorism Intelligence Activities Be Estimated?

The central benefit that domestic CT intelligence activities are seeking to produce is to reduce the threat of terrorism to the United States. As a result, the absolute measure of what these activities are worth is driven by the reduction in terrorism risk and the corresponding value of that risk reduction. Measuring events that have been prevented is difficult, however, particularly since intelligence efforts may deter as well as directly prevent terrorist action. Given these uncertainties, how can we estimate the benefits of CT policies?

In previous work examining the costs and benefits of regulations intended to reduce the risk of terrorism, RAND researchers used the results of probabilistic risk modeling to estimate expected losses from terrorism on an annual basis (LaTourrette and Willis, 2007). These estimates rely on models created for the insurance industry and use physical modeling of different attack types to estimate dollar costs associated with physical damages, injuries, and fatalities and some types of business interruption. Coupled with overall estimates of the threat of terrorism, these costs can be used to calculate expected levels of terrorism risk in

dollar terms. Because of uncertainties in the scope of the terrorist threat and the types of damages different attacks can cause, these models can provide the basis for estimates of ranges of potential losses from terrorism that can be used to define potential benefit ranges for CT policies.

Using one probabilistic terrorism risk model supplemented with additional analysis of dollar costs associated with injuries and fatalities from terrorist attacks, LaTourrette and Willis (2007) produced an estimate of *expected annualized terrorism losses between $1 billion and $10 billion*, which has been applied in analyses of proposed security regulations. This is not to say that this level of losses would be expected *every* year but that, over longer periods, the *average* yearly losses would fall in this range.

However, although such models capture many of the types of losses terrorist attacks can cause, they do not capture the entire picture. For example, such models specifically exclude values for targets that are not insured (e.g., prominent government buildings) but that could be costly (in a variety of ways) if attacked. Furthermore, the costs produced by attacks are not the only costs associated with terrorism. Reactions to the fear of future terrorist attacks are also potentially costly. One category of these costs is changes in behavior (e.g., reductions in consumer or firm spending because of fear of future attacks and loss of trust that the government can protect the nation) that can produce consequences that spread through the economy. In addition, the fear of future terrorist attacks can also lead to the demand to spend on security measures—including more intelligence activities. The resulting expenditures are also a significant cost of terrorism. This is an important component of the total economic burden of terrorism: Estimates of the costs associated with the September 11, 2001, attacks have indicated that the annual costs of security, including increases in federal homeland security expenditures and CT expenditures at other levels of government and the private sector, dwarf the costs of the attacks themselves.[10]

If intelligence efforts are perceived as effective, they could reduce the likelihood that individuals will change their behavior in response

[10] See Jackson, Dixon, and Greenfield (2007) for a review.

to fear of terrorism. This would represent an additional stream of benefits produced by a change in intelligence policies, albeit one that is hard to quantify.

Arguments could be made that intelligence activities could either reduce or increase the demand for security expenditures. If intelligence is viewed as reducing the total threat, other security measures (e.g., airport security or hardening of public buildings) may seem less necessary. On the other hand, since intelligence activities produce and disseminate information about potential threats to the country, it could also increase the demand for additional security measures.

Because RAND's previous efforts to estimate the average annual losses from terrorism did not capture the full range of potential benefits described here, for our analysis, we have chosen to examine a broader possible benefit range than the previously cited $1 billion to $10 billion. *In our illustrative calculations in later sections of this chapter, we therefore have chosen to examine a range of four orders of magnitude for average annual losses of $100 million to $100 billion.* For a given expected level of annual loses, the maximum CT benefit of a particular intelligence effort would be to reduce that expected loss to zero.[11]

In our listing of possible benefits, we also included the potential that intelligence might produce other tangible and intangible benefits outside CT. Because of the diversity of possible benefits that could be relevant, we have chosen not to make any estimates of the possible size of those benefits and use only the range we have defined for potential CT benefits in our illustrative calculations. Instead, we subsequently discuss how the presence (or absence) of collateral benefits would affect a break-even analysis of CT intelligence efforts.

[11] Corresponding, for our range of terrorism losses, to a potential benefit range of $100 million to $100 billion per year, depending on the assumed level of terrorism risk the country faces.

How Can the Costs of Domestic Counterterrorism Intelligence Activities Be Estimated?

In our description of the types of costs that might be associated with domestic CT intelligence, we discussed a wide range of possible costs, from the very tangible (budget outlays) to the very abstract (costs from reduction in privacy). How estimates of dollar values for some of those costs might be made is far from obvious or intuitive. Putting numbers to some of these costs is controversial. Many view such things as personal privacy and the exercise of individual freedoms as priceless and attempts to place dollar values on them misguided. However, given the use of balance sheets and cost-benefit–type analyses in examining policy choices, not even trying to put some numbers to these important costs risks treating them not as priceless but as valueless. In considering these disparate costs, we therefore explored a range of approaches, including comparisons with the costs of current government activities and analogies to other measurable costs. The goal in doing so was not precision in estimation but to define reasonable ranges and orders of magnitude to support our subsequent comparisons.

Direct and Transition Costs

The direct costs associated with an intelligence activity are, in principle, knowable from what the government spends to put that activity in place. Although much intelligence budget information is classified for security reasons, some information is available to calibrate a cost assessment for individual intelligence efforts or to make broader arguments about what it might cost to make changes to intelligence policy, such as founding a new domestic CT intelligence organization.

For example, documents describing the budget of the Federal Bureau of Investigation (FBI) provide some unclassified data that can be used to explore what different types of domestic intelligence efforts might cost. As a benchmark, in its fiscal year (FY) 2008 request to Congress, the total FBI budget was $6.4 billion. The portion of the budget called out as resources aimed at the strategic goal of preventing terrorism and promoting the nation's security, which includes the FBI's CT and counterintelligence (CI) activities, was $3.8 billion (FBI,

2008, p. 1-3). The FY 2008 budget request for the FBI's Intelligence Decision Unit, "comprised of the Directorate of Intelligence (DI), intelligence functions within Counterterrorism, Cyber, and Criminal Divisions, Special Technologies and Applications Office, source funding, infrastructure and technology, and intelligence training" (FBI, 2008, p. 4-1) was $1.2 billion. In some cases, more-detailed, unclassified information is available describing specific activities—for example, the total request for the FBI's data intercept and access program (which does not include activities under the Foreign Intelligence Surveillance Act, or FISA) is approximately $56 million. These values can be compared with the FBI's roughly $3.1 billion *total* budget before the September 11, 2001, terrorist attacks (Cumming and Masse, 2004).

The costs involved in founding a new domestic intelligence agency would depend on what is meant by "founding a new agency." Elsewhere in this volume, we present a number of illustrative models that could define what is meant by creating a new agency. The costs associated with those models would vary a great deal, with the highest costs likely associated with creating an additional, entirely new organization on top of current domestic intelligence efforts (i.e., leaving the activities of other organizations in place) and much lower costs being associated with more-modest options. These costs would arise through the new agency's need for new infrastructure (e.g., buildings, technology), new personnel, and so on. The more a new agency was built from existing parts (e.g., transfer of the FBI's National Security Branch, or NSB), the less it could cost, though past experience with government reorganization and consolidation suggests that savings could be less than expected.

Though some reorganizations of current activities could save money (i.e., if some efforts are eliminated in a consolidation), for our illustrative analysis, we have assumed that costs would increase. Because of the variety of models and the many options associated with each one that would have cost implications, we have not made point estimates for the costs of specific policy options, or even chosen to define likely ranges. Instead, we have simply chosen three values: *low* for an agency costing $250 million more annually than what is spent now on domestic intelligence activities, *medium* for one costing an

additional $1 billion annually, and *high* for one costing an additional $5 billion annually. For the high estimate, this would correspond to creating another FBI-scale agency; the low estimate might correspond to a modest organization and other investments to improve key functions, such as information-sharing.

These values are intended to capture both direct and any transition costs associated with creating a new agency[12] but do not address the fact that transition costs might fall over time (i.e., even if a new agency cost $5 billion in its first year because of high transition costs, its annual costs in later years could be considerably smaller). We illustrate the effects of these transition costs in a specific example in the next section.

Indirect or Intangible Costs

Intangible costs are more difficult to address. It is hard to put a value on things like privacy or how citizens of other nations view the United States. As a result, any attempt to consider values for these costs must explore either indirect ways of assessing them or, more frequently, how assigning different values to each might affect the results of the analysis. However, thinking through such costs and wrestling with ways to assess their magnitudes is a useful part of examining these types of policy changes, whether or not exact values could ever be derived. The following sections illustrate the variety of challenges involved in assessing the effect of intelligence on personal privacy, measures of civil liberties costs, and the potential effect on travel to the United States by international visitors.

Privacy Reduction. Placing a monetary value on personal privacy is difficult. The concept of privacy has a range of meanings and means different things to different people. In response to broad concern about both the collection and use of personal information for commercial purposes and criminal activity, such as identity theft, researchers have sought to determine the values that individuals place on privacy in a number of ways.

---

[12] Interviewees for the study suggested that transition costs of creating a new agency, including the effect on current CT efforts, could be considerable.

Privacy has proven to be a difficult value to characterize, since individuals often express that privacy is very important to them but act in ways that compromise their privacy for comparatively small rewards (e.g., supermarket loyalty programs or the provision of personal information to Internet sites to get personalized purchasing recommendations) (see, e.g., Acquisti and Grossklags, 2005, pp. 24–30). By designing different behavioral experiments, researchers have measured the value that groups of individuals place on keeping particular pieces of information hidden. Because of the focus in the private sector on privacy concerns, many studies have been focused on individuals' views on privacy in business transactions or on the Internet.[13] The rel-

[13] Examples of studies from the literature that have estimated monetary values associated with certain types of privacy preferences include the following:

Hann et al. (2003) studied individuals' willingness to disclose personal information on Web sites depending on the presence of particular incentives to do so (e.g., monetary benefits) and used those preferences to assess the willingness to pay to avoid certain privacy risks (e.g., errors being introduced into their data that affected them later, improper access to the data, and secondary use of their personal information by others). The amount they were willing to pay to avoid those risks was between $30 and $45.

Huberman, Adar, and Fine (2005) designed an auction technique to measure the value individuals placed on keeping their weight or age secret from a group. The average price demanded for revealing their age was $58, while it was $74 for weight. There were differences in the price demanded based on how much individuals believed they deviated from the norm of the group (i.e., individuals who thought they were overweight demanded a higher price).

Png (2007), based on economic analyses of demand for state-level do-not-call registries estimated the value of privacy from unsolicited calls at between $3 and $8 per household per year.

Grossklags and Acquisti (2007) report on an experiment that also focused on subjects' willingness to pay to protect a piece of personal information (e.g., their weight) and the price they would accept to reveal it. For a range of pieces of data, there was a substantial gap between what people would accept to reveal information and the much lower amount they would be willing to pay to protect it. For example, for their weights, the average price people demanded to reveal their weight was approx $32, but they were willing to pay less than $1 to protect it.

Cvrcek et al. (2006) assessed the compensation that individuals would demand if data on their physical locations extracted from their mobile-phone records were used commercially. Compensation demands varied across the European countries in the study: For one year of location data, the demands varied from approximately €100 ($140) to more than €2,000 ($2,800).

evance of individual values for specific pieces of information in specific contexts to broader questions of valuing privacy writ large is unclear, though they do provide at least a starting point for considering how to think about valuing intangible and abstract goods, such as privacy.

The perceived privacy costs associated with founding a new intelligence organization would depend on how the activities of that organization are viewed as different from what law enforcement and intelligence organizations do today. For example, it is appears to be the case (e.g., given the reaction to the Total, subsequently Terrorism, Information Awareness, or TIA, program) that at least some elements of the public are leery of government programs that seek to centralize, in single data sets, large amounts of information about citizens. As a result, if such information centralization was part of forming a new intelligence agency, it would likely be viewed has having significant privacy costs. On the other hand, if formation of a new intelligence organization was viewed as actually reducing information-gathering from its current level and potentially better controlling access to and use of personal data, the privacy "cost" associated with its formation could actually be negative (i.e., it would actually be a benefit when compared with the status quo).

It is difficult to estimate what a reasonable dollar value might be for the perceived cost that individuals would associate with the activities of a new intelligence agency. Most studies to assess people's perceived value of personal information or willingness to pay to protect it focus on individual pieces of data, rather than the broader data collection and the variety of collection means likely to be associated with domestic intelligence operations. Those numbers would be more akin to assessments of individuals' willingness to pay to be not included in specific government databases or watch lists (GAO, 2006a). *As a result, for the purposes of this discussion, we use an estimate of the range of potential privacy costs associated with forming a new intelligence organization that is between $1 and $100 per person per year.* This range includes many of the values found in literature studies examining the value that individuals place on protecting specific types of personal data and, if anything, assigns a conservatively low value. It should be emphasized that these values are averages—e.g., even when an estimate of $1 is

used, the range of privacy preferences that exist in the population would mean that some people would assign a much larger and some a much lower (or even no) cost. The population for which this is assessed could be the adult (approximately 225 million people) or the total population of the United States (approximately 300 million people).[14]

Civil Rights and Civil Liberties. In considering the potential effects of intelligence activities on civil rights and civil liberties, some mechanisms do exist to assign monetary values to the infringement of particular rights for some individuals. Civil litigation by individuals or organizations that contend that the government infringed their rights and the awarding of damages in successful suits are a societal mechanism to place values on some of the potential effects of additional intelligence activities. A review of media accounts and analyses of awards and settlements can provide data to characterize the range of values assigned to particular civil rights and civil liberties effects.

Since September 11, 2001, there have been a few cases of individuals awarded compensation as a result of their arrest, detention, or other treatment resulting from their suspected involvement in terrorism. The awards have varied significantly in their total amounts and have been in response to a range of allegedly improper or mistaken actions on the part of authorities. Examples include the following:

- A Southern California man was awarded $100,000 for being wrongly arrested by the FBI under suspicion that he was involved in an Earth Liberation Front attack on sport utility–vehicle dealers (Piasecki, 2005).
- An Iraqi immigrant was awarded $250,000 as a result of being detained for six days by Border Patrol agents in Montana (Bowermaster, 2007; MacFarquhar, 2007a).
- A lawyer from Oregon who was arrested based on misidentified fingerprint evidence linking him to the Madrid train attacks settled his suit against the government for a reported $2 million ("U.S. to Pay $2M for False Terror Arrest," 2006).

[14] Rounded 2006 estimates from the U.S. Census Bureau (2008).

- A Canadian citizen who was arrested and deported to Syria, where he was reportedly tortured, was given $10.5 million in compensation by the Canadian government ("Harper's Apology," 2007).

Apart from terrorism-specific claims, there is a larger body of data on claims against law enforcement organizations for other civil rights–related violations. A number of studies have documented judgments against police departments or legal settlements by police organizations and have identified costs ranging from amounts in the low hundreds of dollars up to multiple millions, with averages falling between $50,000 to $200,000 per case (e.g., Kappeler, Kappeler, and del Carmen, 1993; Vaughn, Cooper, and del Carmen, 2001; D. Ross and Bodapati, 2006). Not unexpectedly, judgments and settlements vary considerably with the intensity of the rights infringement, with wrongful death or excessive force ranking highest (averaging nearly $300,000, according to one source, nearly $190,000, according to another), false arrest or imprisonment less (approximately $14,000 according to one source, $90,000 according to another), and such actions as malicious prosecution, denial of due process, and illegal search and seizure ranking in the thousands to tens of thousands of dollars (Kappeler, Kappeler, and del Carmen, 1993; D. Ross and Bodapati, 2006).

Available data suggest a reasonable range for the per-incident costs of civil liberties and civil rights infringements from $100,000 (from the range of judgments against law enforcement organizations) to $2 million (based on the case in Oregon). This range is intentionally set conservatively low (e.g., discounting the instance in which compensation was $10 million).

However, to estimate a cost related to civil rights and civil liberties infringements, simply defining a reasonable range of cost values for different civil rights infringements is only part of the picture. Assessing the total annual cost to the country requires knowing how founding a new agency would affect the number of such infringements occurring each year.[15] Any intelligence system will make some mistakes and mis-

[15] This type of analysis has been applied to the costs imposed on individuals misidentified on terrorist watch lists; see the section "Although Likely a Small Percentage of All People

identify some innocent individuals. Inappropriate or illegal behavior by individuals or organizations within the intelligence system could also lead to the intentional targeting of individuals who are not involved in terrorism. Assessing a significant change in intelligence activities, such as founding a new agency, requires making a judgment about whether those mistakes will be more or less likely to occur than under the current system. For example, if one assumes a modest increase in false positives of one per 1,000,000 citizens[16] resulting in civil liberties infringements and an adult U.S. population of 225 million people,[17] this would correspond to an additional 225 cases per year. This false-positive rate and the range of costs defined earlier would correspond to a cost range of $22.5 million to $450 million per year. A higher assumed error rate would move that cost range upward, while a lower one would decrease it.[18]

Screened, the Thousands of Persons Misidentified to the Terrorist Watch List Can Experience Additional Questioning, Delays, and Other Effects" in GAO (2006a).

Much higher false-positive values have been cited for database-driven profiling systems explored for such tasks as screening travelers. For example, in describing systems proposed in 2002, the Markle Foundation Task Force (2002, pp. 30–31) suggests,

> 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. . . . [W]e 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. [Emphasis added]

[16] Such an increase in errors could occur even if the error rate of the new agency's activities is the same as current activities but can simply examine more people.

[17] Unlike privacy reductions, in which the costs could reasonably be viewed as affecting the entire population, the *adult* population is viewed as a more reasonable basis for making estimates about potential civil liberties costs of mistaken arrest or detention of terrorist suspects.

[18] Note that we have made an estimate of these costs as an overall total for the nation as a whole and have not examined whether they might fall disproportionately on some segments of the population. If these costs are not equitably distributed across the total population, an

If it is assumed that founding a new intelligence agency—e.g., by centralizing oversight and strengthening the performance of the intelligence system—would actually reduce the number of individuals mistakenly (or otherwise) arrested, detained, or affected by CT intelligence activities, this cost could be converted to a benefit of making such a change.

Although some impacts on individuals' civil rights and civil liberties can be measured in an approximate way based on how the legal process compensates them, other civil rights and civil liberties concerns are even more abstract and difficult to value in this sort of cost-benefit comparison. A major concern about increasing intelligence activities domestically is that proliferation of government surveillance and the government's recording of data on people and their activities will have a chilling effect on the individuals' exercise of many rights that are fundamental to the U.S. way of life, including speech, dissent, and free association. The argument for such chilling effects is based on the concept that individuals act differently when they know they are being observed and that people cannot feel free to, for example, attend a meeting of a controversial organization if they know that the government will record their attendance and that it might provide the basis for taking action against them later.[19] Although this is an important cost of domestic intelligence efforts, since we could not develop a basis for estimating its value, we have neglected it.

Effect on the United States' Reputation Abroad. Because the effects of foreign perceptions on the full variety of activity that occurs in the international economy would be difficult to estimate and is far beyond the scope of this effort, for the purpose of this discussion, we have chosen to focus on only one possible source of costs from changes in behavior by individuals from other nations: the costs that would result if new domestic intelligence activities led to foreign travelers being less eager to travel to the United States for business or leisure.

---

argument could be made that they should be weighted more heavily than their absolute value might otherwise suggest.

[19] See Siegal (1989) for a discussion of chilling injuries and their treatment in the legal system.

Since the September 11, 2001, terrorist attacks, substantial changes have been made in U.S. security policy with respect to foreign travelers entering the country. For example, initiation of the United States Visitor and Immigrant Status Indicator Technology (US VISIT) program requiring fingerprinting of foreign nationals entering the United States has produced a substantial change in international travelers' experience when coming into the country. Representatives of the travel industry have expressed concern that these changes are affecting the United States' relative position as a destination for travelers, with the U.S. share of international travel dropping since September 11, 2001.[20] Estimates of the contribution of international travelers to the U.S. economy are significant. For 2006, the Travel Industry Association of America estimated that travel expenditures for international travelers (including passenger fares) were approximately $108 billion (Travel Industry Association, 2008). As a result, if the founding of a new domestic intelligence organization caused a 1-percent decline in travel from current levels, this would correspond to an annual cost of more than $1 billion. A 1-percent drop would be relatively modest and compares to estimates that, in the past five years, overseas travel to the United States dropped by 17 percent, reportedly due in part to international travelers' experiences with U.S. security measures (Meserve and Ahlers, 2007).

Summary of Intangible Costs. Developing reasonable estimates of indirect or intangible costs of changes in intelligence policy is much more difficult than for more tangible costs. In some cases, approaches to ballpark figures are available—e.g., given a total value for the contribution of foreign travelers to the U.S. economy, thinking about the effect of small percentage changes in that contribution is straightforward. Similarly, the assignment of values to civil liberties concerns in the legal system is a process intended to do just what is necessary: assign monetary values to important but intangible things. For other variables, assigning values has to be done by analogy, as is the case with privacy. And, in some cases, there are limited approaches avail-

[20] See survey results and discussion of travel volume and balance numbers presented in Travel Industry Association (undated) and Meserve and Ahlers (2007).

able to estimate values at all. For example, lacking a clear path to even assign an order-of-magnitude estimate to the indirect governmental costs of policy changes like agency reorganization, we remain silent on that factor. In such cases, the knowledge that such costs exist must be addressed by putting a wider error bar around conclusions and focusing on making assessments of their potential magnitude for individual policy changes.

An Illustrative Break-Even Analysis of Changes in Domestic Counterterrorism Intelligence

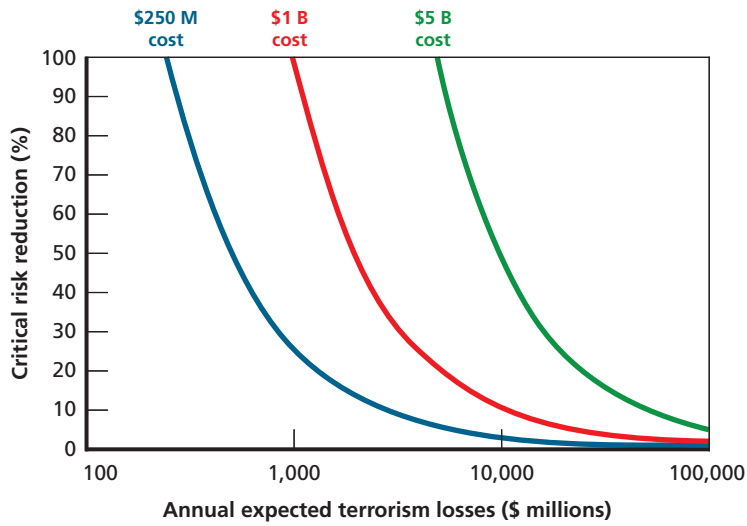
In spite of efforts to make reasonable or even intentionally conservative estimates of the potential benefit of intelligence activities and the value of intangible costs like privacy reduction, estimates of both sides of the cost-benefit balance for changes in intelligence policies have major and irreducible uncertainty associated with them. Furthermore, even if estimates of average expected annual losses from terrorism could be known with certainty, significant ambiguity would remain about how much specific changes in intelligence activities—in this case, the creation of a new domestic intelligence agency—would reduce that risk. In such situations, rather than using uncertain estimates to reach deceptively certain conclusions, break-even analysis can be used. Rather than asking whether the policy change *reduces risk enough* that its benefits justify its costs, a break-even calculation asks *how great the estimated benefit must be* to equal the estimated costs (see LaTourrette and Willis, 2007).

Based on the estimates described here, we performed this type of analysis to explore the levels of reduction in terrorism risk that would be required for new intelligence activities based on the range of estimates of the costs of the terrorism they would prevent (their benefits) and the costs, both tangible and intangible, of putting them in place. Given the multiple levels of uncertainty in the numerical estimates, the intent was not to provide an answer on a specific policy proposal but to demonstrate the utility of the thought process involved and how explicit consideration of different costs and benefits—even if only at the order-of-magnitude level—can provide a different way of framing

debate on new intelligence-policy options. For the purposes of presentation, we begin with a single set of costs—the three point values of the direct costs associated with a new agency of $250 million, $1 billion, and $5 billion and add each type of cost in a stepwise manner to illustrate their cumulative effects.

Figure 9.1 shows how we present the results of this analysis. Each of the cost levels for a domestic intelligence agency is shown as different colored lines on the graph (low cost in blue, medium in red, and high in green) against a logarithmic scale of terrorism risk from $100 million in losses annually at the low end to a very high level of $100 billion in annual losses. At each level of terrorism risk, the break-even level of effectiveness (the point of *critical risk reduction* at which the policy would break even) for an intelligence agency at each cost level is shown on the vertical axis. For example, looking at the red line for a $1 billion agency, the break-even level at $10 billion of annual terrorism risk is 10 percent. As the assumed level of terrorism risk drops,

Figure 9.1
Critical Risk-Reduction Levels for Three Agency Models at Different Levels of Terrorism Risk (tangible costs only)



RAND *MG804-9.1*

agencies at all cost levels have a "higher bar" in effectiveness before they break even. That same red line for an agency costing $1 billion annually hits the top of the graph at a level of $1 billion in terrorism risk—since, to break even at that level, it would have to completely eliminate the risk of terrorist attack.

Even though we have so far considered only tangible costs, we can already say that whether the creation of a new agency would be beneficial is very sensitive to the assumed level of terrorism risk. In Figure 9.1, the benefits of creating an agency exceed the costs in the areas above and to the right of each curve. In the areas below the curves, they do not. That is, organizational approaches that cost more than $1 billion per year are viable only if the expected annual losses from terrorism are more than $1 billion and must be very effective to be justified for risk levels at the lower end of that range. Less costly approaches are viable at lower risk levels but even then require the assumption that creating the agency would have a substantial effect on terrorism risk levels (Figure 9.1).

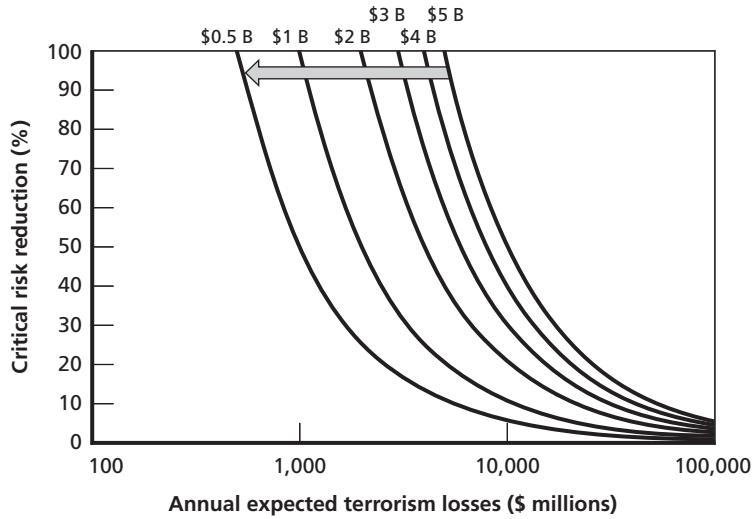
Considering Transition Costs

In the first break-even analysis, the cost of a new agency is viewed as static: Each of the high, medium, and low cost estimates assumed that the cost of the agency was the same every year from its establishment onward. Though such a level expenditure profile could occur for a new initiative that was added on top of current domestic intelligence efforts, it is not realistic for efforts that would require significant reorganization, such as creating either a stand-alone agency or an agency within an agency by combining parts of existing intelligence efforts. Those efforts would likely have significant transition costs associated with them that would be high initially but fall over time as the disruption associated with the changes dissipated. Some of these costs could be financial (e.g., from merging data systems or retraining staff). Others could be less tangible—for example, if the dislocation and disruption of reorganizing the government actually temporarily reduced the ability to prevent terrorist attacks relative to where it is now, the increased risk exposure would be an important transition cost.

The effect of transition costs on the risk reduction required for a new agency's benefits to justify its costs is illustrated in Figure 9.2. To show the broadest range of effect, we have used a notional agency whose costs in its first year start at the extreme upper end of our cost range (at $5 billion) and drop rapidly in its next five years. This drop (and corresponding reduction in the required level of effectiveness) is illustrated by the break-even curves moving from right to left in the direction of the arrow.

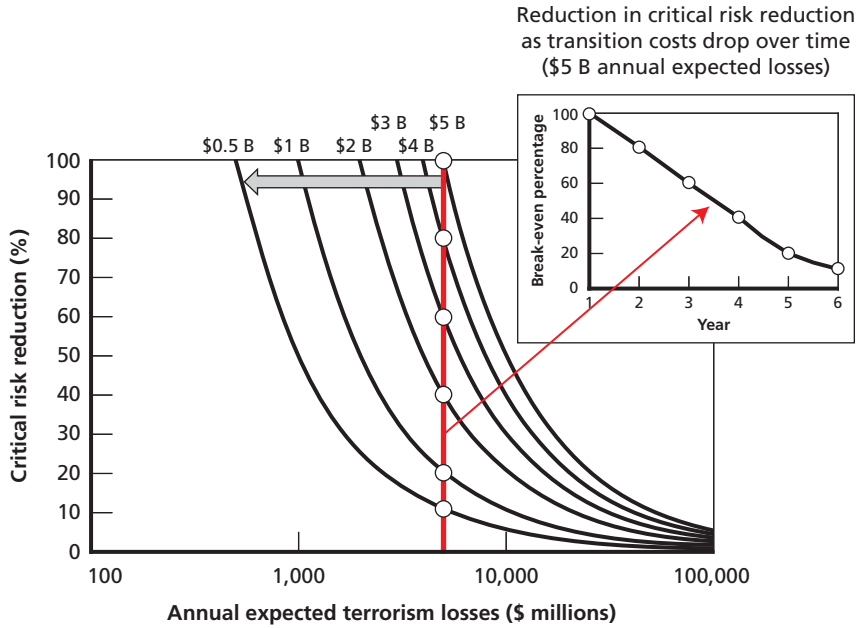
The effect of falling transition costs is most clear by taking a slice vertically through the set of curves shown in Figure 9.2 to illustrate the drop in required risk reduction at a given level of assumed terrorism risk. Figure 9.3 (in which the red line cutting across the break-even curves shows where the slice was taken) demonstrates the drop-off in required effectiveness for a level of terrorism risk of $5 billion in expected annual losses. As a result, depending on the scale of the

Figure 9.2
Drop in Critical Risk-Reduction Levels as Agency Costs Fall (from $5 billion to $0.5 billion annually) Due to Falling Transition Costs



RAND *MG804-9.2*

Figure 9.3
Drop in Critical Risk-Reduction Levels as Agency Costs Fall (from $5 billion to $0.5 billion annually) for a Single Level of Terrorism Risk



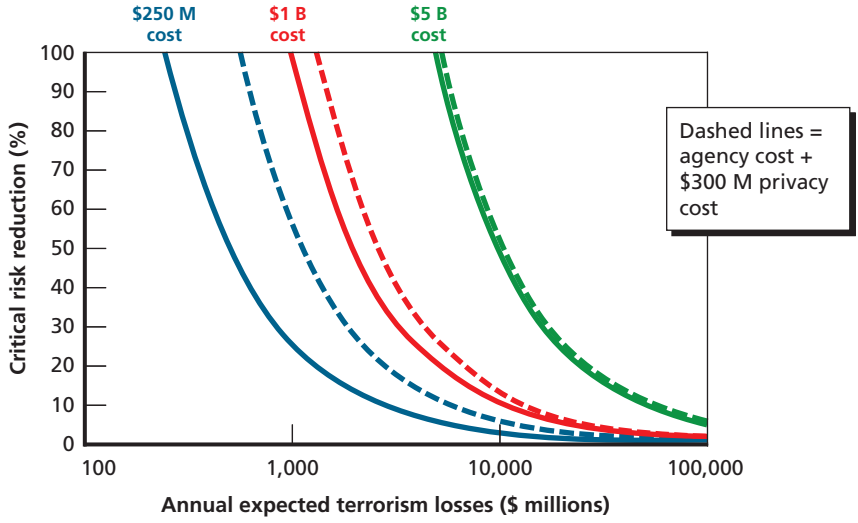
RAND *MG804-9.3*

transition costs involved in creating a particular model agency, a model that is initially nonviable (e.g., in our example, the agency would have to entirely eliminate the risk of terrorist attack in its first year to break even) could become viable as the transition costs are paid and annual costs fall in succeeding years. Its effectiveness in those later years would, however, have to exceed its break-even value to pay the "effectiveness debt" it accumulated when it was not breaking even.

Adding Estimated Privacy Costs

In considering estimates from of monetary values for personal privacy, we defined a range of costs between $1 per person per year and $100 per person per year. To present how adding this cost affects the analysis, Figure 9.4 presents each of the curves included in Figure 9.1, but with the lowest level of privacy costs added: $300 million annually,

Figure 9.4
Critical Risk-Reduction Levels for Three Agency Models at Different Levels of Terrorism Risk (tangible and low privacy cost)

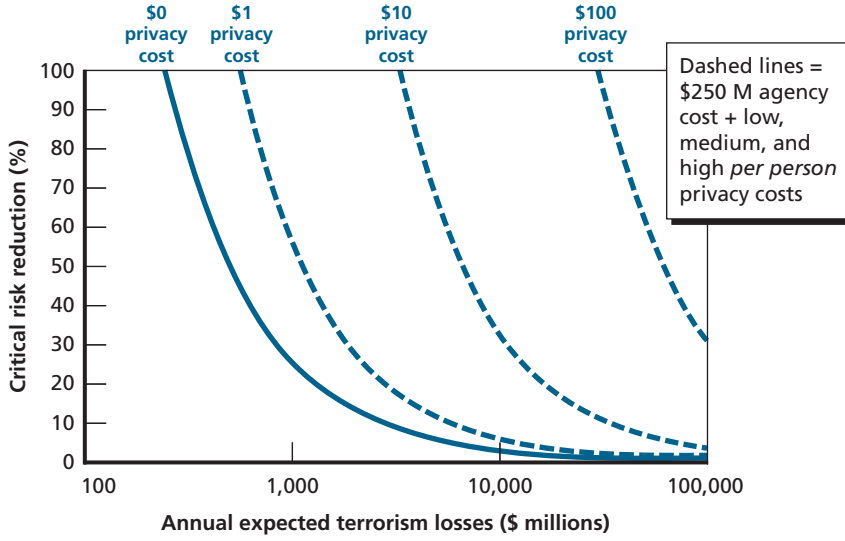


RAND *MG804-9.4*

corresponding to a privacy cost of $1 per member of the U.S. population. As shown by the dotted lines in the figure, the increase in the total cost from the perceived privacy impacts of creating a new agency shifts all the break-even curves to the right, raising how effective they would need to be at reducing terrorism risk before they would be viable. The effect is greatest for the lowest cost model, since the privacy cost represents a larger fraction of its total cost.

Raising the perceived cost of privacy reduction from our conservative $1 per adult per year or adding additional intangible costs shifts all the curves further to the right, raising the level of required effectiveness for each agency's benefits to equal its costs. Because each dollar increase in the perceived cost of privacy reduction adds $300 million to the total costs, using higher values shifts the curves dramatically. To illustrate this, Figure 9.5 shows the effect of valuing privacy at the low, medium, and high levels, *but only for the lowest-cost version of a domestic intelligence agency* (the $250 million case).

Figure 9.5
Critical Risk-Reduction Levels for an Agency Costing $250 Million at Different Levels of Terrorism Risk (tangible and low, medium, and high privacy costs)



RAND *MG804-9.5*

Adding Other Intangible Costs

Rather than iteratively add each intangible cost one-by-one to our analysis, having demonstrated how the break-even analysis changes as additional costs are added, we present a case including intermediate values for each of our intangible costs. In addition to each of the three cost levels for creation of an agency ($250 million, $1 billion, and $5 billion), this last case includes the following costs:

- the lowest value for privacy costs at $1 per U.S. citizen (total cost: $300 million)
- a value for civil liberties costs corresponding to settlements of $100,000 per settlement and 225 such cases nationwide per year (total cost: $22.5 million)
- a value for a modest 1-percent drop in expenditures by international travelers to the United States as a result of changes in public

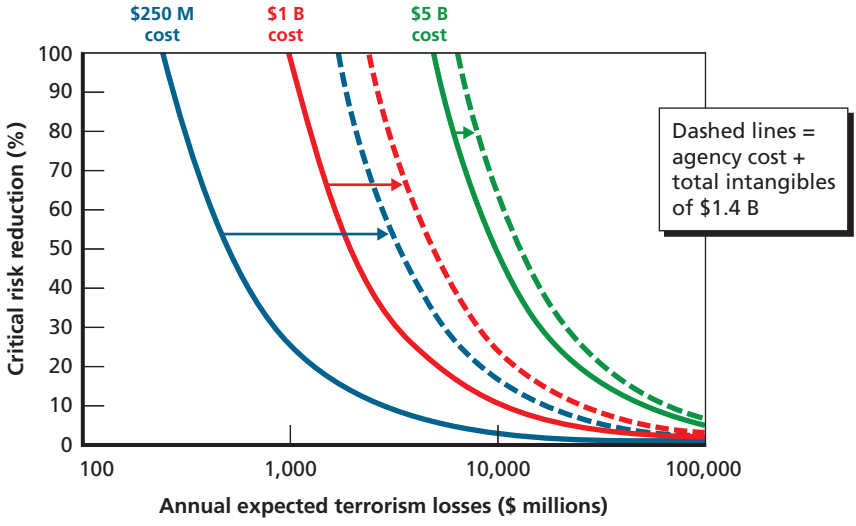
opinion about how welcoming the country is to foreign visitors (total cost: $1.1 billion).

Each of these cost values is at the low end of the ranges that we estimated for each type of cost. The net result of adding these intangible costs on the required break-even effectiveness of any new intelligence agency is shown in Figure 9.6. Given the total of all of these costs, the impact is greatest when considering a minimalist agency (since the $1.4 billion in intangible costs dwarfs the $250 million agency cost). For more-expensive approaches that require very large expected annual losses from terrorism to be viable, the corresponding shift in the break-even curve is much less dramatic.

Intangible Benefits of Creating a New Domestic Intelligence Agency

Though the break-even analysis has, to this point, considered only intangible *costs*, as we discussed previously, approaches to creating a

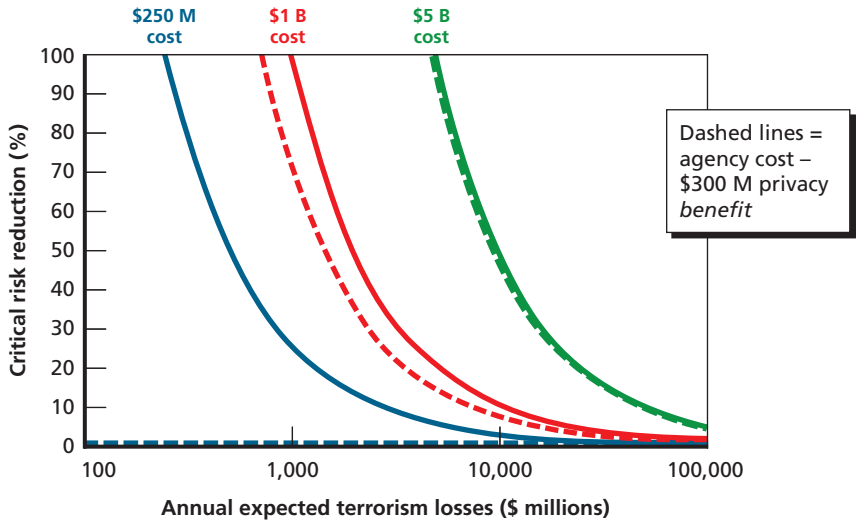
Figure 9.6
Critical Risk-Reduction Levels for Three Agency Models at Different Levels of Terrorism Risk (tangible and low estimate of total intangible costs)



RAND *MG804-9.6*

new domestic intelligence agency—by eliminating duplication in the current decentralized domestic intelligence enterprise or through stringent oversight—could have intangible benefits as well as (or instead of) costs. For example, such an organization might protect privacy *better* than the status quo arrangement does. If that proved to be the case, rather than being an intangible cost, the improved privacy protection would be counted as a benefit in this type of analysis. This case, using the same value for privacy benefits of $1 per member of the U.S. population that was used before, is shown in Figure 9.7. As was the case previously, the effect of the intangible benefit is strongest for the least costly implementation of a domestic intelligence agency, since the fixed privacy benefit offsets a greater fraction of the agency's cost. The difference for an agency with $250 million in annual costs (corresponding to the low end of our cost estimate for a modest agency-within-an-agency implementation) is most striking, reducing the required effectiveness of the agency to zero, since the perceived privacy benefit alone would compensate for the costs associated with the agency whether or not it

Figure 9.7
Critical Risk-Reduction Levels for Three Agency Models at Different Levels of Terrorism Risk (tangible costs and privacy benefit)



RAND *MG804-9.7*

prevented any terrorism. For more-expensive models of an agency, the privacy benefit does shift the break-even curves, though far less dramatically. As a result, they still require quite high levels of effectiveness for such agencies to break even unless terrorism risk levels are assumed to be very high.

Conclusions

Given the uncertainty associated with the potential CT benefits of creating a new domestic intelligence agency and the costs associated with doing so, evaluating this potential policy change requires applying techniques that make it possible to look at the attractiveness of different policies across ranges of possible costs and benefits. To provide a structured way to think through the different costs and benefits identified in our analysis, we used break-even analysis to examine how effective a new CT agency would need to be at particular levels of terrorism risk based on assumed levels of costs involved in its creation and operation. Based on estimates of the costs associated with creating an agency, this analysis suggests that the advisability of creating such an organization depends most heavily on how great the level of terrorism risk is assumed to be currently, a topic on which experts and policymakers differ considerably.

Even without considering the intangible costs that might be associated with forming a new domestic intelligence agency, it is clear that the new organization would have to be quite effective for its costs to be justified if we assume a $10 billion annualized loss level of risk (calibrated by the 9/11 attacks). Expensive models of a new agency (e.g., our $5 billion case) would have to reduce terrorism risk by 50 percent to be justified, which would be a very high bar for performance. Lower costs and higher assumed levels of terrorism risk lower the bar for critical risk reduction. Adding intangible costs for reductions in privacy, civil liberties, and other indirect economic effects, such as effects on international travel, raises the bar even higher.

This examination is clearly an approximate one, relying on estimates of costs for things like privacy and civil liberties for which no

exact data are available. In making estimates, we sought to base the ranges we examined on available data on how individuals (or society, in the case of civil rights and civil liberties) have assigned values to these intangibles.[21] Based on that data, we also were intentionally conservative, anchoring our ranges as low as $1 per adult U.S. citizen for some elements and assuming very modest changes in the rate of errors that might result in infringement of individuals' liberties or rights. Though we believe we have made appropriate analogies and intentionally chose conservatively low values to include in our illustrative examples, individual readers will almost certainly disagree about the numbers that were chosen. Some may view even the upper end of our scale as unreasonably low, while others may view the numbers we used as too high. It is also the case that we have omitted a variety of intangible and other costs in the interest of simplifying this discussion. Concern about whether intelligence will chill individuals' exercise of their rights and participation in political debate and dissent is real, but since we could not put a value to that chilling effect, we did not address it.

In fact, our analysis also relies on estimates of many things about which reasonable people will differ. The perceived threat of terrorism is a strong driver of whether creating a new domestic intelligence agency appears attractive. For those who believe that the threat of terrorism is very high, even substantial costs will be justified if the new agency modestly reduces the risk of terrorist attacks. In contrast, lower levels of assumed risk raise the bar for a new agency's effectiveness sufficiently that it does not appear to be a wise policy choice. Across all the cases, the critical risk reduction needed for founding a new agency to be justified is much lower for the highest risk levels. If a level of expected annual losses from terrorism of $100 billion per year is assumed, even a

[21] An analogy to another policy area is illustrative: The intangible costs of privacy reduction or potential effects on civil liberties from a change in intelligence activities are somewhat akin to environmental pollution or other externalities associated with physical manufacturing processes. Though the product (in the case of intelligence, subsequently improved security) may be valuable in its own right, if the external costs associated with producing it are high enough, it may be difficult to do so sustainably. On the other hand, if technologies or other measures can be put in place to abate the pollution, the economics of production could become much more favorable.

modestly effective agency can be justified even at relatively high absolute cost. However, getting to such a high level of terrorism risk would involve frequent attacks of the scale of 9/11 or much larger incidents, such as nuclear attacks. While perceptions about the risk of terrorism at that level differ, it may also be the case that more cost-effective means could exist to address those threats than creation of a new intelligence organization.

In our examination, we consciously adopted an approach that began from a general baseline of current activities and asked about changes from what is being done today. As a result, the critical risk reductions required for a new agency's costs to be justified are risk reductions from an assumed level of risk today, given all the efforts that are already in place and their current level of effectiveness at addressing the threat. As a result, our examination of the intangible costs associated with forming a new agency were also based on where they are today, illustrated by the example that, if a new agency could be formed that was viewed as preserving privacy and protecting civil liberties better than do current intelligence efforts, that intangible cost could actually become a benefit.

Given the clear uncertainties, we view the results presented here as a guide for policy debate as opposed to an answer to a specific policy question. In spite of its limitations, an approach relying on break-even analysis like that presented here requires addressing the full range of costs and benefits of a policy choice in a common way. If participants in a debate over intelligence policy and the advisability of creating a new domestic intelligence agency disagree, such a common framework provides a systematic way to identify *why* they disagree. Is it because they differ on what they believe the terrorist threat is, or do they diverge on the likely effectiveness of a reorganized domestic intelligence effort? Though disagreement about such factors would not be surprising, nor would identifying the source of the disagreement necessarily lead to consensus and agreement, a policy debate that recognizes and addresses the sources of difference has the potential to be far more productive than simply a fight over differences in final conclusions.

CHAPTER TEN

Conclusion

From its inception, the research effort that produced the chapters of this volume was not intended to produce a recommendation on whether the United States should create any of the types of organizations that have been put forward in policy debate as potential domestic counterterrorism (CT) intelligence agencies. Even if that had been the intent of the effort, providing an objective and final answer would be impossible, given the large number of factors that shape the decision, the strong effect of threat perception, and the influence of a range of personal and other preferences on the relative importance of the costs and benefits of doing so. Instead, the goal of the effort was to start from the policy proposal that such an agency be created—which has recurred in policy debate since the September 11, 2001, terrorist attacks—and examine it from a variety of perspectives to inform future policy decisionmaking.

In thinking about the creation of such an agency, decisionmakers would have to consider the factors that would affect its capability (how well the national domestic intelligence enterprise would address the risk of terrorism compared to how well current efforts do so) and its acceptability (whether the American public would support its creation). In search of insights into both of these issues, our research examined the U.S. domestic context for intelligence issues from a variety of different perspectives and approaches.

Since policy consideration of intelligence—particularly domestic intelligence—is complicated by the many competing values and divergent preferences on intangibles, such as personal privacy, we also

explored ways of thinking through the different balances and trade-offs. These ranged from relatively common approaches, such as comparison of different possible intelligence-agency structures based on insights from organizational theory, to the more nontraditional, such as our exploration of performance metrics and cost-effectiveness analysis of domestic intelligence activities.

In thinking about this issue, it is easier to say what we would want from creating a new intelligence agency than to make compelling arguments about what we would actually get from doing so. Lessons from history and public opinion clearly demonstrate intense sensitivities about domestic intelligence activities, but the importance of those sensitivities vary over time. Looking at current domestic intelligence efforts shows a clearly complex structure, but much less information is available to characterize the functioning of ongoing efforts and support arguments about why different models would be superior. Our various qualitative approaches for thinking through and weighing different trade-offs are instructive and useful as systematic analytical processes, but the uncertainties in the numbers on which they are based mean that their results should not be overinterpreted.

Reflecting the limits in the data available and the significant uncertainty associated with this policy area, if there is a unifying message across the study, it is one of caution and deliberation. In an area in which direct assessment and analysis are limited, there is a need to carefully consider the implications and potential outcomes of significant policy changes, such as the creation of new organizations or the reorganization of ongoing efforts across a web of agencies at many levels inside and outside government. In doing so, examination from different perspectives and through different approaches—to ideally capture a sufficient picture of the complexity to see not just the benefits we hope to gain from policy change but the layers of effects and interactions that could either help or hurt the chances of those benefits appearing—is a critical ingredient of policy deliberation and design.

Bibliography

9/11 Commission Report—*see* National Commission on Terrorist Attacks upon the United States.

ABC News, poll, September 5–7, 2006a. Retrieved from iPOLL Databank, Roper Center for Public Opinion Research, University of Connecticut, November 2, 2008.

———, poll conducted by ABC News and based on telephone interviews conducted by TNS Intersearch of a national sample of 1,003 adults, September 5–7, 2006b. Retrieved from iPOLL Databank, Roper Center for Public Opinion Research, University of Connecticut, November 2, 2008.

ABC News/Washington Post poll, N = 1,000 adults nationwide; margin of error ± 3 (for all adults), March 2–5, 2006a.

———, 9/11 anniversary poll, September 5–7, 2006b.

———, N = 502; margin of error ± 4.5, January 10, 2007. As of October 16, 2008:
http://www.washingtonpost.com/wp-srv/politics/polls/postpoll_011107.htm

Accenture, "Public Service," undated Web page. As of October 15, 2008:
http://www.accenture.com/Global/Services/By_Industry/Government_and_Public_Service/

Acquisti, Alessandro, and Jens Grossklags, "Privacy and Rationality in Individual Decision Making," *IEEE Security and Privacy*, Vol. 3, No. 1, January–February 2005, pp. 26–33.

"Advanced Passenger Information System (APIS)," *GlobalSecurity.org*, last modified March 9, 2007. As of August 15, 2006:
http://www.globalsecurity.org/security/systems/apis.htm

Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *Implementing the National Strategy: Fourth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction*, Washington, D.C., 2002. As of October 10, 2008: http://purl.access.gpo.gov/GPO/LPS25391

———, *Forging America's New Normalcy: Securing Our Homeland, Protecting Our Liberty—Fifth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction*, Washington, D.C., 2003. As of October 16, 2008: http://purl.access.gpo.gov/GPO/LPS41265

Allison, Graham T., *Essence of Decision: Explaining the Cuban Missile Crisis*, Boston, Mass.: Little, Brown, 1971.

American Civil Liberties Union, "ACLU Says Bush Administration Should Not Allow Operation TIPS to Become an End Run Around Constitution," press release, Washington, D.C., July 15, 2002. As of October 15, 2008: http://www.aclu.org/natsec/emergpowers/14432prs20020715.html

Andrews, Edmund L., "Threats and Responses: Liberty and Security: New Scale for Toting Up Lost Freedom vs. Security Would Measure in Dollars," *New York Times*, March 11, 2003, p. 13. As of October 20, 2008: http://query.nytimes.com/gst/fullpage.html?res=9404E1D9173EF932A25750C0A9659C8B63

Arnone, Michael, "InfoZen Wins $148M TSA Contract," *FCW.com*, April 19, 2006. As of October 15, 2008: http://www.fcw.com/online/news/94121-1.html

Arquilla, John, and David Ronfeldt, eds., *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Santa Monica, Calif.: RAND Corporation, MR-1382-OSD, 2001. As of October 15, 2008: http://www.rand.org/pubs/monograph_reports/MR1382/

Bamford, James, "Big Brother Is Listening," *Atlantic*, April 2006. As of October 16, 2008: http://www.theatlantic.com/doc/200604/nsa-surveillance

Bartoldus, Charles, director, National Targeting Center Office of Field Operations, Customs and Border Protection, "Progress in Consolidating Terrorist Watchlists: The Terrorist Screening Center (TSC)," statement before the U.S. House of Representatives Select Committee on Homeland Security Subcommittee on Intelligence and Counterterrorism and Committee on the Judiciary Subcommittee on Crime, Terrorism, and Homeland Security, March 25, 2004. As of October 15, 2008: http://www.iwar.org.uk/homesec/resources/tsc-mar-25-04/Bartoldus.pdf

Batvinis, Raymond J., *The Origins of FBI Counterintelligence*, Lawrence, Kan.: University Press of Kansas, 2007.

Behrman, Robert, "Structure and Effectiveness of Intelligence Organizations," Pittsburgh, Pa.: Carnegie Mellon University, undated.

Bergman, Lowell, Eric Lichtblau, Scott Shane, and Don Van Natta Jr., "Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends," *New York Times*, January 17, 2006. As of October 15, 2008: http://www.nytimes.com/2006/01/17/politics/17spy.html

Berrick, Cathleen A., *Aviation Security: Federal Coordination for Responding to In-Flight Security Threats Has Matured, but Procedures Can Be Strengthened*, Washington, D.C.: U.S. Government Accountability Office, GAO-07-891R, July 31, 2007a. As of October 15, 2008: http://purl.access.gpo.gov/GPO/LPS86188

———, *Transportation Security: Efforts to Strengthen Aviation and Surface Transportation Security Are Under Way, but Challenges Remain*, Washington, D.C.: U.S. Government Accountability Office, GAO-08-140T, October 16, 2007b.

Best, Richard A., *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.*, Washington, D.C.: Congressional Research Service, Library of Congress, December 3, 2001.

Best, Richard A., and Alfred Cumming, *Director of National Intelligence Statutory Authorities: Status and Proposals*, Washington, D.C.: Congressional Research Service, Library of Congress, RL34231, April 17, 2008. As of October 16, 2008: http://www.fas.org/sgp/crs/intel/RL34231.pdf

Best, Samuel J., and Monika L. McDermott, "Measuring Opinions vs. Non-Opinions: The Case of the USA PATRIOT Act," *Forum*, Vol. 5, No. 2, 2007, pp. 1–27.

Betts, Richard K., "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," *World Politics*, Vol. 31, No. 1, October 1978, pp. 61–89.

Birrer, Frans A. J., "Data Mining to Combat Terrorism and the Roots of Privacy Concerns," *Ethics and Information Technology*, Vol. 7, No. 4, December 2005, pp. 211–220.

BJA—*see* Bureau of Justice Assistance.

Blind, Peri K., *Building Trust in Government in the Twenty-First Century: Review of Literature and Emerging Issues*, Vienna, Austria: 7th Global Forum on Reinventing Government Building Trust in Government, June 26–29, 2007, written November 2006. As of October 16, 2008: http://unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN025062.pdf

Block, Robert, "U.S. to Expand Domestic Use of Spy Satellites," *Wall Street Journal*, August 15, 2007. As of October 20, 2008: http://online.wsj.com/public/article/SB118714764716998275.html

Block, Robert, and Jay Solomon, "Neighborhood Watch: Pentagon Steps Up Intelligence Efforts Inside U.S. Borders," *Wall Street Journal*, April 27, 2006.

Bonner, Robert C., commissioner, U.S. Customs and Border Protection Committee on Government Reform Subcommittee on Criminal Justice, Drug Policy, and Human Resources, statement to the U.S. House of Representatives Select Committee on Homeland Security Subcommittee on Infrastructure and Border Security, July 22, 2004. As of October 16, 2008: http://www.cbp.gov/xp/cgov/newsroom/commissioner/speeches_statements/archives/2004/072204_reform.xml

Booth, Richard T., "Air and Marine Operations Center (AMOC) Role in Securing the Border," Technologies for Critical Incident Preparedness Conference and Exposition, September 7, 2006.

Booz Allen Hamilton, "Case Studies: ADNET—Using Technology in the War on Drugs," undated Web page. As of October 15, 2008: http://www.boozallen.com/about/article/657786

Bowermaster, David, "Feds Apologize for Iraqi Refugee's Detention," *Seattle Times*, August 24, 2007. As of October 20, 2008: http://seattletimes.nwsource.com/html/localnews/2003851019_aclu24m.html

Brackett, Robert, director, Food and Drug Administration Center for Food Safety and Applied Nutrition, "Bio-Security and Agro-Terrorism," testimony before the U.S. Senate Committee on Agriculture, Nutrition, and Forestry, July 20, 2005. As of October 16, 2008: http://agriculture.senate.gov/Hearings/hearings.cfm?hearingid=1572&witnessId=4470

Bruce, James B., "How Leaks of Classified Intelligence Help U.S. Adversaries: Implications for Laws and Secrecy," in Roger Z. George and Robert D. Kline, eds., *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, Washington, D.C.: National Defense University Press, 2004, pp. 399–414.

Bureau of Alcohol, Tobacco, Firearms, and Explosives, "About ATF," undated Web page. As of October 15, 2008: http://www.atf.treas.gov/about/mission.htm

———, *ATF 2005 Annual Report*, 1000.4, March 2006a. As of October 16, 2008: http://www.atf.gov/pub/gen_pub/2005annual_report.pdf

———, *Privacy Impact Assessment for the GangNet*, Washington, D.C., May 31, 2006b. As of November 6, 2008: http://www.atf.gov/about/foia/pia/053106privacy_impact_assessmentt-gangnet.pdf

———, *Privacy Impact Assessment: National Field Office Case Information System (NFOCIS)*, Washington, D.C., May 31, 2006c. As of November 6, 2008: http://www.atf.gov/about/foia/pia/privacy_impact_assessment-nfocis-pia-final.pdf

Bureau of Justice Assistance, *New Realities: Law Enforcement in the Post-9/11 Era*, Washington, D.C.: U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, 2005.

Burns, William J., *Risk Perception: A Review*, Los Angeles, Calif.: Center for Risk and Economic Analysis of Terrorism Events, University of Southern California, May 22, 2007. As of October 16, 2008:
http://www.usc.edu/dept/create/assets/003/54570.pdf

Byman, Daniel, "US Counter-Terrorism Options: A Taxonomy," *Survival*, Vol. 49, No. 3, 2007, pp. 121–150.

Carey, Thomas, special agent in charge, Washington Division, Federal Bureau of Investigation, "Communication with the Law Enforcement Community," testimony before the U.S. Senate Committee on the Judiciary, November 13, 2001. As of October 15, 2008:
http://www.fbi.gov/congress/congress01/carey111301.htm

CBO—*see* Congressional Budget Office.

Centers for Disease Control and Prevention, "Detailed Definition of PHIN," undated Web page. As of October 15, 2008:
http://www.cdc.gov/phin/about.html

———, "Health Alert Network," last reviewed January 18, 2002. As of October 15, 2008:
http://www2a.cdc.gov/han/

———, "Vision, Mission, Core Values, and Pledge," last updated September 29, 2008. As of October 15, 2008:
http://www.cdc.gov/about/organization/mission.htm

Chalk, Peter, and William Rosenau, *Confronting "the Enemy Within": Security Intelligence, the Police, and Counterterrorism in Four Democracies*, Santa Monica, Calif.: RAND Corporation, MG-100-RC, 2004. As of October 10, 2008:
http://www.rand.org/pubs/monographs/MG100/

Chanley, Virginia A., "Trust in Government in the Aftermath of 9/11: Determinants and Consequences," *Political Psychology*, Vol. 23, No. 3, December 2002, pp. 469–483.

Chester, Jesse L. Jr., special agent, chief, Arson and Explosives Repository, Office of Strategic Intelligence and Information, Bureau of Alcohol, Tobacco, Firearms, and Explosives, "Bombs and Arson Tracking System (B.A.T.S.) Status Report," briefing, May 13, 2004. As of October 15, 2008:
http://www.iacptechnology.org/LEIM/2004Presentations/BATS%20IACP.pdf

Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc., 467 U.S. 837, June 25, 1984.

Chief Executive Office, Los Angeles County, "Information on Terrorism," undated Web page. As of October 15, 2008:
http://lacoa.org/terror.htm

Church Committee Report—*see* U.S. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities.

Churchill, Ward, and Jim Vander Wall, *The COINTELPRO Papers: Documents from the FBI's Secret Wars Against Dissent in the United States*, 2nd ed., Cambridge, Mass.: South End Press, 2002.

CIFA—*see* U.S. Department of Defense Counterintelligence Field Activity.

Cinquegrana, Americo R., "The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978," *University of Pennsylvania Law Review*, Vol. 137, No. 3, January 1989, pp. 793–828.

Clayton, Mark, "US Suspends Vast ADVISE Data-Sifting System," *Christian Science Monitor*, August 28, 2007. As of October 14, 2008:
http://www.csmonitor.com/2007/0828/p01s02-usju.html

CNN, survey by Cable News Network, conducted by Opinion Research Corporation, based on telephone interviews with a national sample of 1,022 adults, May 16–17, 2006.

Cohen, Dara K., Mariano-Florentino Cuellar, and Barry R. Weingast, "Crisis Bureaucracy: Homeland Security and the Political Design of Legal Mandates," *Stanford Law Review*, Vol. 59, No. 3, 2006, pp. 673–760.

Colby, William E., "After Investigating U.S. Intelligence," *New York Times*, February 26, 1976, p. 11.

Cole, David, professor, Georgetown University Law Center, "Chasing the Sleeper Cell," *Frontline*, interview, September 12, 2003. As of October 16, 2008:
http://www.pbs.org/wgbh/pages/frontline/shows/sleeper/interviews/cole.html

Collins, ADM Thomas, Commandant of the U.S. Coast Guard, U.S. Department of Homeland Security, statement on transportation security before the U.S. Senate Committee on Commerce, Science, and Transportation, September 9, 2003. As of October 15, 2008:
http://commerce.senate.gov/pdf/collins090903.pdf

Comer, John S., assistant special agent in charge, Phoenix Field Division, Drug Enforcement Administration, "Pushing the Border Back: The Role Intelligence Plays in Protecting the Border," testimony before the U.S. House of Representatives Select Committee on Intelligence, Sierra Vista, Ariz., August 17, 2006. As of November 6, 2008:
http://www.usdoj.gov/dea/pubs/cngrtest/ct081706.html

Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States*, official government edition, Washington, D.C., March 31, 2005.

Congressional Budget Office, *Immigration Policy in the United States*, Washington, D.C., February 2006. As of October 20, 2008: http://purl.access.gpo.gov/GPO/LPS72417

"Counterintelligence Field Activity," *SourceWatch*, last modified April 1, 2008. As of July 26, 2007: http://www.sourcewatch.org/index.php?title=Counterintelligence_Field_Activity

Crenshaw, Martha, "The Psychology of Political Terrorism," in Margaret G. Hermann, ed., *Political Psychology*, 1st ed., San Francisco, Calif.: Jossey-Bass Publishers, 1986, pp. 379–413.

Cumming, Alfred, and Todd Masse, *FBI Intelligence Reform Since September 11, 2001: Issues and Options for Congress*, Washington, D.C.: Congressional Research Service, Library of Congress, RL32336, April 6, 2004.

Cvrcek, Dan, Vashek Matyas, Marek Kumpost, and George Danezis, *A Study on the Value of Location Privacy*, presented at Fifth Association for Computing Machinery Workshop on Privacy in Electronic Society, Alexandria, Va., October 30, 2006. As of October 20, 2008: http://www.cosic.esat.kuleuven.be/publications/article-845.pdf

Davidson, Roger H., and Walter J. Oleszek, *Congress and Its Members*, 9th ed., Washington, D.C.: CQ Press, 2004.

Davis, Darren W., and Brian D. Silver, *Continuity and Change in Support for Civil Liberties After the 9/11 Terrorist Attacks: Results of a Panel Study*, presented at the Annual Meeting of the American Political Science Association, Philadelphia, Pa., August 27–31, 2003.

———, "Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America," *American Journal of Political Science*, Vol. 48, No. 1, January 2004a, pp. 28–46.

———, *The Threat of Terrorism, Presidential Approval, and the 2004 Election*, prepared for the Annual Meeting of the American Political Science Association, Chicago, Ill., September 2–5, 2004b. As of October 16, 2008: https://www.msu.edu/~bsilver/APSA2004Election82.pdf

DeBree, Jordan, and Lee Wang, "Defending the Home Front: The Military's New Role," *Frontline*, October 10, 2006. As of October 15, 2008: http://www.pbs.org/wgbh/pages/frontline/enemywithin/reality/military.html

Defense Advanced Research Projects Agency, *Defense Advanced Research Projects Agency Strategic Plan*, February 2007. As of October 15, 2008: http://handle.dtic.mil/100.2/ADA468784

Defense Advanced Research Projects Agency Information Processing Techniques Office, "Predictive Analysis for Naval Deployment Activities (PANDA)," undated Web page. As of July 30, 2007:
http://www.darpa.mil/ipto/programs/panda/panda.asp

Defense Information Systems Agency, "Mission, Vision and Values," undated Web page. As of October 15, 2008:
http://www.disa.mil/about/missionvision.html

Defense Intelligence Agency, "Introduction to DIA," undated Web page. As of July 30, 2007:
http://www.dia.mil/thisisdia/intro/

Dempsey, James X., executive director, Center for Democracy and Technology, *Overview of Current Criminal Justice Information Systems*, Center for Democracy and Technology, February 9, 2000. As of October 15, 2008:
http://www.cdt.org/publications/overviewofcjis.pdf

———, "Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Governmental Use," testimony before the U.S. Senate Committee on the Judiciary, April 13, 2005. As of October 20, 2008:
http://www.cdt.org/testimony/20050413dempsey.pdf

Dempsey, James X., and Lara M. Flint, "Commercial Data and National Security," *George Washington Law Review*, Vol. 72, No. 6, August 2004, pp. 1459–1502.

DeRosa, Mary, *Data Mining and Data Analysis for Counterterrorism*, Washington, D.C.: CSIS Press, 2004.

DeYoung, Karen, "A Fight Against Terrorism—and Disorganization," *Washington Post*, August 9, 2006, p. A01. As of October 15, 2008:
http://www.washingtonpost.com/wp-dyn/content/article/2006/08/08/AR2006080800964.html

DHS—*see* U.S. Department of Homeland Security.

DHS OIG—*see* U.S. Department of Homeland Security Office of the Inspector General.

Dixon, Robert G. Jr., "The Griswold Penumbra: Constitutional Charter for an Expanded Law of Privacy?" *Michigan Law Review*, Vol. 64, No. 2, December 1965, pp. 197–218.

"Documents Show Errors in TSA's 'No Fly' and 'Selectee' Watch Lists," Electronic Privacy Information Center, last updated March 23, 2006. As of October 14, 2008:
http://epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html

DOJ and DHS—*see* U.S. Department of Justice Global Justice Information Sharing Initiative and U.S. Department of Homeland Security Homeland Security Advisory Council.

DOJ OIG—*see* U.S. Department of Justice Office of the Inspector General.

Dorschner, Jim, "Inside-Intelligence: Reforming the US Intelligence Community," *Jane's Intelligence Review*, October 1, 2007.

Duke, Lynne, "The Picture of Conformity: In a Watched Society, More Security Comes with Tempered Actions," *Washington Post*, November 16, 2007, p. C01.

Eggen, Dan, "Under Fire, Justice Shrinks TIPS Program," *Washington Post*, August 10, 2002, p. A01.

Electronic Privacy Information Center, "~~Total~~ 'Terrorism' Information Awareness (TIA)," last updated March 21, 2005. As of October 15, 2008: http://epic.org/privacy/profiling/tia/

———, comments on *Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*, c. 2007. As of January 2008: http://epic.org/privacy/id-cards/epic_realid_comments.pdf

English, Larry P., "Information Quality: Critical Ingredient for National Security," *Journal of Database Management*, Vol. 16, No. 1, January–March 2005, pp. 18–32.

EO—*see* Executive Order.

EPIC—*see* Electronic Privacy Information Center.

Executive Order 9835, Prescribing Procedures for the Administration of an Employees Loyalty Program in the Executive Branch of the Government, March 21, 1947.

Executive Order 12036, United States Foreign Intelligence Activities, January 24, 1976.

Executive Order 13354, National Counterterrorism Center, August 27, 2004.

Farhi, Paul, "Calling on Hollywood's Terrorism 'Experts': Homeland Security Chief Compares Reality and '24,'" *Washington Post*, June 24, 2006, p. C01. As of October 16, 2008: http://www.washingtonpost.com/wp-dyn/content/article/2006/06/23/AR2006062301804.html

FBI—*see* Federal Bureau of Investigation.

Federal Aviation Administration, *Security and Hazardous Materials: Federal Aviation Administration, Fiscal Year 2007 Business Plan*, Washington, D.C., c. 2006. As of October 15, 2008: http://www.faa.gov/about/plans_reports/business_plan2007/media/ASH%20FY2007%20Business%20Plan%20for%20Publication.pdf

Federal Bureau of Investigation, "FBI Tips and Public Leads," undated(a) Web page. As of October 14, 2008: https://tips.fbi.gov/

———, "Investigative Programs Critical Incident Response Group: Mission Statement," undated(b) Web page. As of October 15, 2008:
http://www.fbi.gov/hq/isd/cirg/mission.htm

———, "Investigative Programs Critical Incident Response Group: National Center for the Analysis of Violent Crime," undated(c) Web page. As of October 15, 2008:
http://www.fbi.gov/hq/isd/cirg/ncavc.htm

———, "National Security Branch," undated(d) Web page. As of October 15, 2008:
http://www.fbi.gov/hq/nsb/nsb.htm

———, "Protecting America from Terrorist Attack: Meet the National Joint Terrorism Task Force," July 2, 2004a. As of October 15, 2008:
http://www.fbi.gov/page2/july04/njttf070204.htm

———, "Protecting America Against Terrorist Attack: A Closer Look at the FBI's Joint Terrorism Task Forces," December 1, 2004b. As of October 15, 2008:
http://www.fbi.gov/page2/dec04/jttf120114.htm

———, "Frequently Asked Questions," last updated July 31, 2006a. As of October 17, 2008:
http://www.fbi.gov/hq/nsb/nsb_faq.htm

———, *National Security Branch Overview*, September 2006b.

———, *Privacy Impact Assessment for the Law Enforcement National Data Exchange (N-DEx)*, Section V: *Privacy Questions*, Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Division, January 2007. As of October 15, 2008:
http://foia.fbi.gov/piandex040607.htm

———, "FY 2008 Authorization and Budget Request to Congress," c. 2007.

Fessler, Pam, "Intelligence Officials to Discuss Terrorism," *NPR*, July 12, 2007. As of October 16, 2008:
http://www.npr.org/templates/story/story.php?storyId=11903737

Fidler, Stephen, "MI5 Ends Role in Probing Organised Crime to Fight Terrorism," *Financial Times*, May 12, 2006, p. 3.

Financial Crimes Enforcement Network, U.S. Department of the Treasury, undated (a) home page. As of October 15, 2008:
http://www.fincen.gov/

———, "HIFCA," undated (b) Web page. As of October 15, 2008:
http://www.fincen.gov/law_enforcement/hifca/

Finnegan, John Patrick, *Military Intelligence*, Washington, D.C.: Center of Military History, U.S. Army, 1998. As of October 13, 2008:
http://purl.access.gpo.gov/GPO/LPS100326

Fischhoff, Baruch, Roxana M. Gonzalez, Deborah A. Small, and Jennifer S. Lerner, "Judged Terror Risk and Proximity to the World Trade Center," *Journal of Risk and Uncertainty*, Vol. 26, No. 2–3, March 2003, pp. 137–151.

Fisher, Louis, and Ronald C. Moe, "Presidential Reorganization Authority: Is It Worth the Cost?" *Political Science Quarterly*, Vol. 95, No. 2, Summer 1981, pp. 301–318.

Flynn, Mark, director, Protective Security Division, U.S. Department of Homeland Security, "Protective Security Division (PSD) Programs and Operations," briefing, Regulatory Information Conference Session B2: Safeguards/ Security, March 8, 2005. As of October 15, 2008: http://www.nrc.gov/public-involve/conference-symposia/ric/past/2005/slides/ 03-b2-flynn.pdf

Food Safety and Inspection Service, U.S. Department of Agriculture, "About FSIS," last modified July 15, 2008. As of October 15, 2008: http://www.fsis.usda.gov/About_FSIS/OFDER/

Forman, Marcy M., deputy assistant director, Financial Investigations, U.S. Immigration and Customs Enforcement, U.S. Department of Homeland Security, "Terrorist Financing and Money Laundering Investigations: Who Investigates and How Effective Are They?" statement before the U.S. House of Representatives Committee on Government Reform Subcommittee on Criminal Justice, Drug Policy, and Human Resources, May 11, 2004. As of October 15, 2008: http://www.ice.gov/doclib/pi/news/testimonies/Forman_051104.pdf

FOXNews/Opinion Dynamics, poll conducted by Opinion Dynamics Corporation by telephone for FOXNews, N = 900 registered voters nationwide; margin of error ± 3, April 21–22, 2004a.

———, poll conducted by telephone, N = 900 registered voters nationwide; margin of error ± 3, December 14–15, 2004b.

Frederickson, H. George, and Todd R. LaPorte, "Airport Security, High Reliability, and the Problem of Rationality," *Public Administration Review*, Vol. 62, special issue, September 2002, pp. 34–44.

GAO—*see* U.S. Government Accountability Office.

Garcia, Michael J., assistant secretary, U.S. Immigration and Customs Enforcement, U.S. Department of Homeland Security, "Drugs and Security in a Post-9/11 World: Coordinating the Counternarcotics Mission at DHS," statement before the U.S. House of Representatives Committee on Government Reform Subcommittee on Criminal Justice, Drug Policy, and Human Resources and Select Committee on Homeland Security Subcommittee on Infrastructure and Border Security, July 22, 2004. As of October 15, 2008: http://www.ice.gov/doclib/pi/news/testimonies/072204garcia.pdf

Garrett, Elizabeth, "The Purposes of Framework Legislation," *Journal of Contemporary Legal Issues*, Vol. 14, No. 2, 2005, pp. 717–766.

Gellman, Barton, Dafna Linzer, and Carol A. Leonnig, "Surveillance Net Yields Few Suspects," *Washington Post*, February 5, 2006, p. A01. As of October 20, 2008:
http://www.washingtonpost.com/wp-dyn/content/article/2006/02/04/AR2006020401373.html

Georgia Emergency Management Agency, "GISAC," undated Web page. As of October 15, 2008:
http://www.gema.state.ga.us/ohsgemaweb.nsf/9C891F3A609DCA46852570C8005A2D64/2B51986BAAECD7528525711600698E79?OpenDocument

Gill, Peter, *Democratic and Parliamentary Accountability of Intelligence Services After September 11*, presented at Workshop on Democratic and Parliamentary Oversight of Intelligence Services, Geneva, October 3–5, 2002.

Gilmore Commission—*see* Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction.

Golle, Philippe, "Revisiting the Uniqueness of Simple Demographics in the US Population," *Workshop on Privacy in the Electronic Society: Proceedings of the 5th ACM Workshop on Privacy in Electronic Society*, Alexandria, Va.: Association for Computing Machinery, 2006, pp. 77–80.

Goodwin, Charles L., special agent in charge, Honolulu Division, Federal Bureau of Investigation, statement before the U.S. House of Representatives Committee on Government Reform Subcommittee on Criminal Justice, Drug Policy, and Human Resources, August 2, 2004. As of October 15, 2008:
http://www.fbi.gov/congress/congress04/goodwin080204.htm

Greene, Kate, "Blindfolding Big Brother, Sort of," *Technology Review*, January 30, 2006. As of October 20, 2008:
http://www.technologyreview.com/web/16209/?a=f

Grimmett, Richard F., *9/11 Commission Recommendations: Implementation Status*, Washington, D.C.: Congressional Research Service, Library of Congress, RL33742, December 4, 2006. As of October 16, 2008:
http://fpc.state.gov/documents/organization/77700.pdf

Grossklags, Jens, and Alessandro Acquisti, *When 25 Cents Is Too Much: An Experiment on Willingness-to-Sell and Willingness-to-Protect Personal Information*, presented at the 2007 Workshop on the Economics of Information Security, Pittsburgh, Pa., June 7–8, 2007. As of October 20, 2008:
http://weis2007.econinfosec.org/papers/66.pdf

Guevara, Rogelio E., chief of operations, Drug Enforcement Administration, statement before U.S. House of Representatives Committee on the Judiciary Subcommittee on Crime, Terrorism, and Homeland Security, May 6, 2003. As of October 15, 2008:
http://www.usdoj.gov/dea/pubs/cngrtest/ct050603.htm

Hall, Mimi, and Barbara DeLollis, "Plan to Collect Flier Data Canceled," *USA Today*, July 15, 2004. As of October 15, 2008:
http://www.usatoday.com/news/washington/2004-07-14-fly-plan_x.htm

Hamilton County (Ohio) Regional Terrorism Early Warning Group, undated home page. As of October 15, 2008:
https://www.hamiltoncountyohio-tewg.org/

Hammond, Thomas H., "Why Is the Intelligence Community So Difficult to Redesign? Smart Practices, Conflicting Goals, and the Creation of Purpose-Based Organizations," *Governance*, Vol. 20, No. 3, July 2007, pp. 401–422.

Hann, Il-Horn, Kai-Lung Hui, Tom S. Lee, and I. P. L. Png, "The Value of Online Information Privacy: Evidence from the USA and Singapore," Washington, D.C.: AEI-Brookings Joint Center for Regulatory Studies, 03-25, October 2003. As of October 20, 2008:
http://www.aei-brookings.org/admin/authorpdfs/redirect-safely.php?fname=../pdffiles/php2b.pdf

"Harper's Apology 'Means the World': Arar," CBC News, January 26, 2007. As of October 20, 2008:
http://www.cbc.ca/canada/story/2007/01/26/harper-apology.html

Harris, Shane, "TIA Lives On," *National Journal*, February 23, 2006a. As of October 20, 2008:
http://www.nationaljournal.com/about/njweekly/stories/2006/0223nj1.htm

———, "Agency Explores New Tool to Connect Intelligence Dots," *National Journal*, October 20, 2006b.

———, "Terrorist Profiling: Version 2.0," *National Journal*, October 20, 2006c. As of October 15, 2008:
http://www.nationaljournal.com/about/njweekly/stories/2006/1020nj3.htm

Harris Poll, "Support for Government Surveillance Programs Increases Among U.S. Adults, but Many Still Worry About Civil Liberty Safeguards," February 24, 2006. As of October 15, 2008:
http://www.harrisinteractive.com/harris_poll/index.asp?PID=643

Heritage Foundation, "'24' and America's Image in Fighting Terrorism: Fact, Fiction, or Does It Matter?" event, June 23, 2006. As of October 16, 2008:
http://www.heritage.org/Press/Events/ev062306.cfm

Herman, Michael, "Counter-Terrorism, Information Technology and Intelligence Change," *Intelligence and National Security*, Vol. 18, No. 4, Winter 2003, pp. 40–58.

Herron, Kerry G., and Hank C. Jenkins-Smith, *Critical Masses and Critical Choices: Evolving Public Opinion on Nuclear Weapons, Terrorism, and Security*, Pittsburgh, Pa.: University of Pittsburgh Press, 2006.

Highway Watch, "Program Overview," Web page. Accessed July 30, 2007; no longer available.

Homeland Security Council, and President George W. Bush, *National Strategy for Homeland Security*, Washington, D.C.: White House, October 2007. As of October 10, 2008:
http://purl.access.gpo.gov/GPO/LPS88800

HSC and Bush—*see* Homeland Security Council and President George W. Bush.

Hsu, Spencer S., and Robert O'Harrow Jr., "DHS to Replace 'Duplicative' Anti-Terrorism Data Network," *Washington Post*, January 18, 2008, p. A03. As of October 14, 2008:
http://www.washingtonpost.com/wp-dyn/content/article/2008/01/17/AR2008011703279.html

Huberman, Bernardo A., Eytan Adar, and Leslie R. Fine, "Valuating Privacy," *IEEE Security and Privacy*, Vol. 3, No. 5, October 2005, pp. 22–25.

Huddy, Leonie, Stanley Feldman, Theresa Capelos, and Colin Provost, "The Consequences of Terrorism: Disentangling the Effects of Personal and National Threat," *Political Psychology*, Vol. 23, No. 3, 2002, pp. 485–509. As of October 16, 2008:
http://ispp.org/publications/journal/back/v23no3Terrorism.pdf

Huddy, Leonie, Stanley Feldman, Charles Taber, and Gallya Lahav, "Threat, Anxiety, and Support of Antiterrorism Policies," *American Journal of Political Science*, Vol. 49, No. 3, July 2005, pp. 593–608.

Hulnick, Arthur S., "Openness: Being Public About Secret Intelligence," *International Journal of Intelligence and CounterIntelligence*, Vol. 12, No. 4, December 1999, pp. 463–483.

———, "Intelligence Reform 2007: Fix or Fizzle?" *International Journal of Intelligence and CounterIntelligence*, Vol. 20, No. 4, December 2007, pp. 567–582.

Information Sharing and Analysis Centers Council, "About the Council," undated Web page. As of October 15, 2008:
http://www.isaccouncil.org/about/

———, *Reach of the Major ISACs*, white paper, January 31, 2004. As of October 14, 2008:
http://www.isaccouncil.org/pub/Reach_of_the_Major_ISACs_013104.pdf

Information Sharing Environment, "Purpose and Vision of the Information Sharing Environment," undated Web page. No longer available.

———, *Information Sharing Environment Implementation Plan*, November 2006. As of October 15, 2008:
http://www.ise.gov/docs/ISE-impplan-200611.pdf

———, *Annual Report to the Congress on the Information Sharing Environment*, Washington, D.C., September 2007. As of October 15, 2008: http://www.ise.gov/docs/reports/Annual_Report_To_Congress_20070913.pdf

InfraGard, "About InfraGard," undated Web page. As of October 15, 2008: http://www.infragard.net/about.php?mn=1&sm=1-0

"Intelink," *GlobalSecurity.org*, last modified April 26, 2005. As of October 15, 2008: http://www.globalsecurity.org/intell/systems/intelink.htm

Internal Revenue Service, U.S. Department of the Treasury, "Criminal Enforcement," undated Web page. No longer available.

———, "Information Available from TECS," Part 9: Criminal Investigation, Chapter 10: Administrative Databases and Software, Section 2: Treasury Enforcement and Communication System and International Fugitive Notices, *Internal Revenue Manual*, November 21, 2001. As of October 15, 2008: http://www.irs.gov/irm/part9/ch10s02.html#d0e65450

International Association of Chiefs of Police, *IACP: An Information Integration Planning Model*, April 2000. As of October 15, 2008: http://www.theiacp.org/documents/pdfs/Publications/cjinfosharing.pdf

IRTPA—*see* Public Law 108-458.

ISAC Council—*see* Information Sharing and Analysis Centers Council.

ISE—*see* Information Sharing Environment.

Jackson, Brian A., ed., *Considering the Creation of a Domestic Intelligence Agency in the United States: Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom*, Santa Monica, Calif.: RAND Corporation, MG-805-DHS, 2008. As of publication date: http://www.rand.org/pubs/monographs/MG805/

Jackson, Brian A., John C. Baker, Peter Chalk, Kim Cragin, John V. Parachini, and Horacio R. Trujillo, *Aptitude for Destruction*, Vol. 1: *Organizational Learning in Terrorist Groups and Its Implications for Combating Terrorism*, Santa Monica, Calif.: RAND Corporation, MG-331-NIJ, 2005a. As of October 20, 2008: http://www.rand.org/pubs/monographs/MG331/

———, *Aptitude for Destruction*, Vol. 2: *Case Studies of Organizational Learning in Five Terrorist Groups*, Santa Monica, Calif.: RAND Corporation, MG-332-NIJ, 2005b. As of October 20, 2008: http://www.rand.org/pubs/monographs/MG332/

Jackson, Brian A., Peter Chalk, Kim Cragin, Bruce Newsome, John V. Parachini, William Rosenau, Erin M. Simpson, Melanie Sisson, and Donald Temple, *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies*, Santa Monica, Calif.: RAND Corporation, MG-481-DHS, 2007. As of October 10, 2008:
http://www.rand.org/pubs/monographs/MG481/

Jackson, Brian A., Lloyd Dixon, and Victoria A. Greenfield, *Economically Targeted Terrorism: A Review of the Literature and a Framework for Considering Defensive Approaches*, Santa Monica, Calif.: RAND Corporation, TR-476-CTRMP, 2007. As of October 20, 2008:
http://www.rand.org/pubs/technical_reports/TR476/

Jeffreys-Jones, Rhodri, *The CIA and American Democracy*, 3rd ed., New Haven, Conn.: Yale University Press, 2003.

———, *The FBI: A History*, New Haven, Conn.: Yale University Press, 2007.

Jenkins, Brian Michael, *Unconquerable Nation: Knowing Our Enemy, Strengthening Ourselves*, Santa Monica, Calif.: RAND Corporation, MG-454-RC, 2006. As of October 16, 2008:
http://www.rand.org/pubs/monographs/MG454/

Jenkins-Smith, Hank C., and Kerry G. Herron, "United States Public Response to Terrorism: Fault Lines or Bedrock?" *Review of Policy Research*, Vol. 22, No. 5, September 2005, pp. 599–623.

Jensen, Richard Bach, "The United States, International Policing and the War Against Anarchist Terrorism," *Terrorism and Political Violence*, Vol. 13, No. 1, Spring 2001, pp. 15–46.

Jervis, Robert, "The Politics and Psychology of Intelligence and Intelligence Reform," *The Forum*, Vol. 4, No. 1, 2006, pp. 1–9. As of October 17, 2008:
http://www.columbia.edu/cu/siwps/publication_files/Intelligence%20reform_JERVIS.pdf

Johnson, Loch K., *A Season of Inquiry: Congress and Intelligence*, Chicago, Ill.: Dorsey Press, 1988.

———, "Covert Action and Accountability: Decision-Making for America's Secret Foreign Policy," *International Studies Quarterly*, Vol. 33, No. 1, March 1989, pp. 81–109.

———, "Congressional Supervision of America's Secret Agencies: The Experience and Legacy of the Church Committee," *Public Administration Review*, Vol. 64, No. 1, January–February 2004, pp. 3–14.

Johnson, Matthew M., "FBI's Intelligence Woes Restir Debate on an American MI5," *CQ Homeland Security*, October 23, 2007. As of November 5, 2008:
http://public.cq.com/docs/hs/hsnews110-000002611323.html

Joint Chiefs of Staff, "J2 Joint Staff Intelligence: Mission Statement," undated Web page. As of July 30, 2007:
http://www.jcs.mil/j2/

Joint Interagency Task Force (JIATF) South, "Welcome to Joint Interagency Task Force (JIATF) South," last modified August 29, 2008. As of October 15, 2008:
http://www.jiatfs.southcom.mil/

Joint Task Force North, "Joint Task Force North Mission," undated Web page. As of July 30, 2007:
http://www.jtfn.northcom.mil/subpages/mission.html

"Joint Worldwide Intelligence Communications System (JWICS)," Federation of American Scientists, last updated January 18, 1999. As of October 15, 2008:
http://www.fas.org/irp/program/disseminate/jwics.htm

Jonas, Jeff, and Jim Harper, *Effective Counterterrorism and the Limited Role of Predictive Data Mining*, Washington, D.C.: Cato Institute, December 11, 2006. As of October 20, 2008:
http://www.cato.org/pubs/pas/pa584.pdf

Joslyn, Mark R., and Donald P. Haider-Markel, "Sociotropic Concerns and Support for Counterterrorism Policies," *Social Science Quarterly*, Vol. 88, No. 2, June 2007, pp. 306–319.

Kansas City Regional Terrorism Early Warning Group Interagency Analysis Center, undated home page. As of October 15, 2008:
http://www.kctew.org/

Kaplan, Eben, "Backgrounder: Fusion Centers," Council on Foreign Relations, February 22, 2007. As of October 15, 2008:
http://www.cfr.org/publication/12689/

Kappeler, Victor E., Stephen F. Kappeler, and Rolando V. del Carmen, "A Content Analysis of Police Civil Liability Cases: Decisions of the Federal District Courts, 1978–1990," *Journal of Criminal Justice*, Vol. 21, No. 4, 1993, pp. 325–337.

Kelley, Matt, "Feds Sharpen Secret Tools for Data Mining," *USA Today*, July 20, 2006. As of October 15, 2008:
http://www.usatoday.com/tech/news/techpolicy/2006-07-19-data-mining_x.htm

Kimbell, Abigail, regional forester, Northern Region, U.S. Department of Agriculture Forest Service, "Effects of Illegal Border Activities on Federal Land Management Agencies," testimony before the U.S. House of Representatives Committee on Resources, August 28, 2006. As of October 15, 2008:
http://www.fs.fed.us/congress/109/house/oversight/kimball/082806.html

Kime, Patricia, "Maritime 'Fusion' Centers Expand Coast Guard Intelligence Capabilities," Navy League of the United States, May 2004. As of October 15, 2008:
http://www.navyleague.org/sea_power/may_04_16.php

Kimery, Anthony L., "Big Brother Wants to Look in Your Bank Account," *Wired*, Vol. 1.06, December 1993. As of October 15, 2008: http://www.wired.com/wired/archive/1.06/big.brother.html

Kind, Peter A., and J. Katharine Burton, *Information Sharing and Collaboration Business Plan*, Alexandria, Va.: Institute for Defense Analyses, D-3206, June 2005. As of October 15, 2008: http://www.fas.org/irp/agency/dhs/ida2005.pdf

Koontz, Linda D., *Homeland Security: Continuing Attention to Privacy Concerns Is Needed as Programs Are Developed—Testimony Before the Subcommittee on Homeland Security, Committee on Appropriations, House of Representatives*, Washington, D.C.: U.S. Government Accountability Office, GAO-07-630, March 21, 2007. As of October 15, 2008: http://purl.access.gpo.gov/GPO/LPS80428

Krakovec, Laura L., "Fourth Amendment: The Constitutionality of Warrantless Aerial Surveillance," *Journal of Criminal Law and Criminology*, Vol. 77, No. 3, Autumn 1986, pp. 602–631.

Krouse, William J., and Bart Elias, *Terrorist Watchlist Checks and Air Passenger Screening*, Washington, D.C.: Congressional Research Service, Library of Congress, RL33645, September 6, 2006. As of October 15, 2008: http://www.fas.org/sgp/crs/homesec/RL33645.pdf

Kuzma, Lynn M., "Trends: Terrorism in the United States," *Public Opinion Quarterly*, Vol. 64, No. 1, March 3, 2007, pp. 90–105.

Kyllo v. United States, 533 U.S. 27, June 11, 2001.

Landau, Martin, "Redundancy, Rationality, and the Problem of Duplication and Overlap," *Public Administration Review*, Vol. 29, No. 4, July–August 1969, pp. 346–358.

LaTourrette, Tom, and Henry H. Willis, *Using Probabilistic Terrorism Risk Modeling for Regulatory Benefit-Cost Analysis: Application to the Western Hemisphere Travel Initiative Implemented in the Land Environment*, Santa Monica, Calif.: RAND Corporation, WR-487-IEC, 2007. As of October 20, 2008: http://www.rand.org/pubs/working_papers/WR487/

Law Enforcement Intelligence Unit, "History, Purpose, and Operations," undated Web page. As of October 15, 2008: http://leiu-homepage.org/about/historyPurpose.php

Leavitt, Mike, secretary, U.S. Department of Health and Human Services, "HHS: What We Do," press release, March 2008. As of October 15, 2008: http://www.hhs.gov/about/whatwedo.html

Lessons Learned Information Sharing, *LLIS Intelligence and Information Sharing Initiative: Homeland Security Intelligence Requirements Process*, Washington, D.C.: U.S. Department of Homeland Security, December 2005. As of October 15, 2008: http://www.dhs.gov/xlibrary/assets/Final_LLIS_Intel_Reqs_Report_Dec05.pdf

Lewis, Carol W., "The Clash Between Security and Liberty in the U.S. Response to Terror," *Public Administration Review*, Vol. 65, No. 1, January–February 2005, pp. 18–30.

Lichtblau, Eric, and James Risen, "Spy Agency Mined Vast Data Trove, Officials Report," *New York Times*, December 24, 2005. As of October 20, 2008: http://www.nytimes.com/2005/12/24/politics/24spy.html

LLIS—*see* Lessons Learned Information Sharing.

Lormel, Dennis, chief, Federal Bureau of Investigation Financial Crimes Section, "Tools Against Terror: How the Administration Is Implementing New Laws in the Fight to Protect Our Homeland," testimony before the U.S. Senate Committee on the Judiciary Subcommittee on Terrorism, Technology, and Homeland Security, October 9, 2002.

Lum, Cynthia, *Tip Line Technologies: Intelligence Gathering and Analysis Systems*, Phase I: *Final Report and Executive Summary*, Washington, D.C.: National Institute of Justice, Office of Justice Programs, U.S. Department of Justice, July 1, 2005. As of October 14, 2008: http://www.ncjrs.gov/pdffiles1/nij/grants/211677.pdf

MacFarquhar, Neil, "Detention Was Wrong, and U.S. Apologizes," *New York Times*, August 24, 2007a. As of October 20, 2008: http://www.nytimes.com/2007/08/24/washington/24settle.html

———, "Protest Greets Police Plan to Map Muslim Angelenos," *New York Times*, November 9, 2007b. As of October 16, 2008: http://www.nytimes.com/2007/11/09/us/09muslim.html

MacGaffin, John, "Chasing the Sleeper Cell," *Frontline*, interview, June 12, 2003. As of October 17, 2008: http://www.pbs.org/wgbh/pages/frontline/shows/sleeper/interviews/macgaffin.html

Markle Foundation Task Force, *Protecting America's Freedom in the Information Age*, New York and Washington, D.C.: Markle Foundation, October 2002. As of October 10, 2008: http://www.markletaskforce.org/documents/Markle_Full_Report.pdf

———, *Creating a Trusted Information Network for Homeland Security: Second Report of the Markle Foundation Task Force*, New York: Markle Foundation, December 2003. As of October 17, 2008: http://www.markletaskforce.org/Report2_Full_Report.pdf

———, *Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment*, New York, 2006. As of November 5, 2008:
http://www.markle.org/downloadable_assets/2006_nstf_report3.pdf

Markoff, John, and Scott Shane, "Documents Show Link Between AT&T and Agency in Eavesdropping Case," *New York Times*, April 13, 2006. As of October 20, 2008:
http://www.nytimes.com/2006/04/13/us/nationalspecial3/13nsa.html

Marshall, C. Kevin, acting deputy assistant attorney general, Office of Legal Counsel, U.S. Department of Justice, "Status of the Director of Central Intelligence Under the National Security Intelligence Reform Act of 2004: Memorandum Opinion for the Deputy Counsel to the President," January 12, 2005. As of October 16, 2008:
http://www.usdoj.gov/olc/dcidciaappointment0112final.pdf

Martin, Kate, "Domestic Intelligence and Civil Liberties," *SAIS Review*, Vol. 24, No. 1, Winter–Spring 2004, pp. 7–21.

Masse, Todd, *Domestic Intelligence in the United Kingdom: Applicability of the MI-5 Model to the United States*, Washington, D.C: Congressional Research Service, Library of Congress, 03-RL-31920, May 19, 2003. As of October 10, 2008:
http://handle.dtic.mil/100.2/ADA455815

———, *The 9/11 Commission and a National Counterterrorism Center: Issues and Options for Congress*, Washington, D.C.: Congressional Research Service, Library of Congress, RL32558, September 3, 2004. As of October 17, 2008:
http://www.ndu.edu/library/docs/crs%209.03.04.pdf

———, *The National Counterterrorism Center: Implementation Challenges and Issues for Congress*, Washington, D.C.: Congressional Research Service, Library of Congress, RL32816, March 16, 2005.

———, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*, Washington, D.C: Congressional Research Service, Library of Congress, RL33616, August 18, 2006. As of October 10, 2008:
http://handle.dtic.mil/100.2/ADA454484

Masse, Todd, Siobhan O'Neil, and John Rollins, *Fusion Centers: Issues and Options for Congress*, Washington, D.C.: Congressional Research Service, Library of Congress, RL34070, 2007. As of October 15, 2008:
http://handle.dtic.mil/100.2/ADA470027

Mayer, Jane, "Whatever It Takes: The Politics of the Man Behind 24," *New Yorker*, Vol. 83, No. 1, February 19, 2007. As of October 16, 2008:
http://www.newyorker.com/reporting/2007/02/19/070219fa_fact_mayer

Mefford, Larry A., executive assistant director, Federal Bureau of Investigation, "FBI Infrastructure Awareness," testimony before the U.S. House of Representatives Select Committee on Homeland Security Subcommittee on Cybersecurity, Science, and Research and Development and Subcommittee on Infrastructure and Border Security, September 4, 2003. As of October 15, 2008: http://www.fbi.gov/congress/congress03/mefford090403.htm

Meserve, Jeanne, and Mike M. Ahlers, "Travel Industry: U.S. Losing Out on International Tourism," CNN, Washington, D.C., January 31, 2007. As of October 20, 2008: http://www.cnn.com/2007/TRAVEL/01/31/international.travel/

Miller, Brad, chair, and James Sensenbrenner Jr., ranking member, U.S. House of Representatives Committee on Science and Technology Subcommittee on Investigations and Oversight, letter to the Honorable David Walker, comptroller general of the United States, June 5, 2007. As of October 15, 2008: http://democrats.science.house.gov/Media/File/AdminLetters/miller_snsbrnner_walker_GAO_6.5.07.pdf

Miller, Greg, "Spies Resist Plan to Shift Power," *Los Angeles Times*, May 31, 2008, p. A24. As of October 16, 2008: http://articles.latimes.com/2008/may/31/nation/na-intel31

Milligan, Darric, Bernadette Clemente, and Michael Schader, *Intelligence-Led Policing Tool: Intelligence-Led Policing Technology for State and Local Law Enforcement Agencies*, Falls Church, Va.: Mitretek Systems and Yellow House Associates, MTR-2006-016, March 2006. As of October 10, 2008: http://www.noblis.org/BusinessAreas/CriminalJustice/ILPT_MTR-2006-016.pdf

Mintz, John, "DHS Considers Alternatives to Color-Coded Warnings," *Washington Post*, May 10, 2005, p. A06. As of October 16, 2008: http://www.washingtonpost.com/wp-dyn/content/article/2005/05/09/AR2005050901128.html

MITRE, "Stopping Traffic: Anti Drug Network (ADNET)," July 2001, last updated March 20, 2001. As of October 15, 2008: http://www.mitre.org/news/digest/archives/2001/adnet.html

Morgan, Richard E., *Domestic Intelligence: Monitoring Dissent in America*, Austin, Tex.: University of Texas Press, 1980.

Moynihan, Daniel Patrick, *Secrecy*, New Haven, Conn.: Yale University Press, 1998.

Mueller, Robert S. III, director, Federal Bureau of Investigation, "Global Threats to the U.S. and the FBI's Response," testimony before the U.S. Senate Committee on Intelligence, February 16, 2005. As of October 20, 2008: http://www.fbi.gov/congress/congress05/mueller021605.htm

Myers, Gen. Richard B., U.S. Air Force, chair, Joint Chiefs of Staff, posture statement before the U.S. Senate Committee on Armed Service, February 3, 2004. As of October 15, 2008:
http://www.au.af.mil/au/awc/awcgate/dod/posture_3feb04myers.pdf

Nakashima, Ellen, "FBI Plans Initiative to Profile Terrorists: Potential Targets Get Risk Rating," *Washington Post*, July 11, 2007a, p. A08. As of October 15, 2008:
http://www.washingtonpost.com/wp-dyn/content/article/2007/07/10/AR2007071001871.html

———, "Terror Suspect List Yields Few Arrests: 20,000 Detentions in '06 Rile Critics," *Washington Post*, August 25, 2007b, p. A01. As of October 15, 2008:
http://www.washingtonpost.com/wp-dyn/content/article/2007/08/24/AR2007082402256.html

National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*, New York: Norton, 2004.

National Counterterrorism Center, "What We Do," last updated December 21, 2005. As of October 15, 2008:
http://www.nctc.gov/about_us/what_we_do.html

———, *NCTC and Information Sharing: Five Years Since 9/11—A Progress Report*, McLean, Va., September 2006. As of October 15, 2008:
http://www.nctc.gov/docs/report%5Fcard%5Ffinal.pdf

———, "Key Partners," last updated May 18, 2007. As of October 15, 2008:
http://www.nctc.gov/about_us/key_partners.html

National Drug Intelligence Center, U.S. Department of Justice, undated home page. As of October 15, 2008:
http://www.usdoj.gov/ndic/

National Geospatial-Intelligence Agency, home page, last modified October 7, 2008. As of July 30, 2007:
http://www.nga.mil

National Research Council Committee on Freight Transportation Information Systems Security, *Cybersecurity of Freight Information Systems: A Scoping Study*, Washington, D.C.: Transportation Research Board, Computer Science and Telecommunications Board, 2003. As of October 15, 2008:
http://onlinepubs.trb.org/Onlinepubs/sr/sr274.pdf

National Research Council Committee on Policy Implications of International Graduate Students and Postdoctoral Scholars in the United States; Committee on Science, Engineering, and Public Policy; Board on Higher Education and Workforce; and National Academies Press, *Policy Implications of International Graduate Students and Postdoctoral Scholars in the United States*, Washington, D.C.: National Academies Press, 2005. As of October 20, 2008:
http://www.nap.edu/catalog/11289.html

National Response Center, "NRC Background," undated Web page. As of October 14, 2008:
http://www.nrc.uscg.mil/nrcback.html

National Security Agency, "Mission Statement," undated (a) Web page. As of July 30, 2007:
http://www.nsa.gov/about/about00003.cfm

———, "Signals Intelligence: Who Is Considered a U.S. Person?" undated (b) Web page. As of October 10, 2008:
http://www.nsa.gov/about/about00020.cfm#5

National Security Council, Exploitation of Soviet and Satellite Defectors Outside the United States, National Security Council Intelligence Directive 13, Washington, D.C., January 19, 1950. As of October 16, 2008:
http://www.state.gov/documents/organization/96784.pdf

———, Communications Intelligence, National Security Council Intelligence Directive 9 Revised, Washington, D.C., December 29, 1952. As of October 16, 2008:
http://www.state.gov/documents/organization/96784.pdf

National Security Presidential Directive 43/Homeland Security Presidential Directive 14, Domestic Nuclear Detection Office, April 15, 2005. As of October 15, 2008:
http://www.nspd.gov/rawmedia_repository/6fc04b35707798e5d5ae21a7302275e9.pdf

Naval Criminal Investigative Service, "Mission," undated Web page. As of October 15, 2008:
http://www.ncis.navy.mil/mission.asp

NCTC—*see* National Counterterrorism Center.

Newton, Elaine, Latanya Sweeney, and Bradley Malin, *Preserving Privacy by De-Identifying Facial Images*, Pittsburgh, Pa.: School of Computer Science, Carnegie Mellon University, March 2003.

Nlets, undated home page. As of October 15, 2008:
http://www.nlets.org/

Noblis, *Comprehensive Regional Information-Sharing Project*, Vol. 1: *Metrics for the Evaluation of Law Enforcement Information-Sharing Systems*, Falls Church, Va.: Center for Criminal Justice Technology, MTR-2006-035, January 2007. As of October 20, 2008:
http://www.noblis.org/BusinessAreas/CriminalJustice/Metrics_hi-res.pdf

NRC—*see* National Response Center.

O'Connell, Anne Joseph, "The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World," *California Law Review*, Vol. 94, No. 6, December 2006, pp. 1655–1744.

O'Connell, Cynthia, acting director, Office of Intelligence, U.S. Immigration and Customs Enforcement, statement before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, June 28, 2006. As of October 15, 2008: http://www.ice.gov/doclib/pi/news/testimonies/060628testimony.pdf

ODNI—*see* Office of the Director of National Intelligence.

Office of the Attorney General, State of California Department of Justice, "Anti-Terrorism Information Center," undated Web page. As of October 15, 2008: http://ag.ca.gov/antiterrorism/

Office of the Chief of Naval Operations, and U.S. Marine Corps, *Naval Intelligence*, Washington, D.C., Naval Doctrine publication 2, September 30, 1994.

Office of the Director of National Intelligence, "About the ODNI," undated (a) Web page. As of October 14, 2008: http://www.dni.gov/who.htm

———, "Office of the Director of National Intelligence Organization," undated (b) Web page. As of October 14, 2008: http://www.dni.gov/organization.htm

———, "ODNI Announces Establishment of Open Source Center," press release, ODNI News Release No. 6-05, November 8, 2005. As of October 15, 2008: http://www.dni.gov/press_releases/20051108_release.htm

Office of Homeland Security, *National Strategy for Homeland Security*, Washington, D.C., July 2002a. As of October 10, 2008: http://purl.access.gpo.gov/GPO/LPS20641

———, *State and Local Actions for Homeland Security*, July 2002b. As of October 15, 2008: http://www.whitehouse.gov/homeland/stateandlocal/State_and_Local_Actions_for_Homeland_Security.pdf

Office of Justice Programs, *The National Criminal Intelligence Sharing Plan: Solutions and Approaches for a Cohesive Plan to Improve Our Nation's Ability to Share Criminal Intelligence*, Washington, D.C.: Office of Justice Programs, U.S. Department of Justice, October 2003. As of October 16, 2008: http://it.ojp.gov/documents/National%5FCriminal%5FIntelligence%5FSharing%5FPlan.pdf

Office of Management and Budget, "Detailed Information on the Drug Enforcement Administration Assessment," last updated September 6, 2008. As of October 15, 2008: http://www.whitehouse.gov/omb/expectmore/detail/10000170.2003.html

Office of National Drug Control Policy, "About," undated Web page. As of October 15, 2008:
http://www.whitehousedrugpolicy.gov/about/

OHS—*see* Office of Homeland Security.

Open Source Center, undated home page. As of October 15, 2008:
https://www.opensource.gov

Oxford, Vayl, director, Domestic Nuclear Detection Office, U.S. Department of Homeland Security, "Countering the Nuclear Threat to the Homeland: Evaluating the Deployment of Radiation Detection Technologies," testimony before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, February 21, 2007. As of October 14, 2008:
http://homeland.house.gov/SiteDocuments/20070321152336-60301.pdf

"Passport Rule Helps Collect Child Support," (Associated Press) *New York Times*, August 14, 2007. As of October 20, 2008:
http://www.nytimes.com/2007/08/15/us/15passport.html?adxnnl=1&adxnnlx=1213297350-LI08jHQ6qBHL3mfqIE7LpA

Patrick, John J., Richard M. Pious, and Donald A. Ritchie, "U.S. Secret Service," *The Oxford Guide to the United States Government*, Oxford and New York: Oxford University Press, 2001.

Payne, Mike, "Coast Guard Intelligence and Criminal Investigations CG-2," briefing, Armed Forces Communications and Electronics Association, June 20, 2006.

"Pentagon to Close Disputed Database," (Associated Press) *New York Times*, August 22, 2007. As of October 14, 2008:
http://www.nytimes.com/2007/08/22/washington/22terror.html

Petrie, Michael, "The Use of EMS Personnel as Intelligence Sensors: Critical Issues and the Recommended Practices," *Homeland Security Affairs*, Vol. 3, No. 3, September 2007, pp. 1–18. As of October 20, 2008:
http://www.hsaj.org/pages/volume3/issue3/pdfs/3.3.6.pdf

Pew Research Center for the People and the Press, Pew News Interest Index/Believability Poll, conducted by Princeton Survey Research Associates International by telephone interviews with a national sample of 1,501 adults, June 14–19, 2006. Retrieved from the Roper Center for Public Opinion Research, University of Connecticut.

Piasecki, Joe, "The Wrong Man," *LA CityBeat*, November 17, 2005. As of October 20, 2008:
http://www.lacitybeat.com/cms/story/detail/?id=2878&IssueNum=128

Pillar, Paul R., *Terrorism and U.S. Foreign Policy*, Washington, D.C.: Brookings Institution Press, 2001.

Pincus, Walter, "Pentagon Expanding Its Domestic Surveillance Activity: Fears of Post-9/11 Terrorism Spur Proposals for New Powers," *Washington Post*, November 27, 2005, p. A06. As of October 15, 2008: http://www.washingtonpost.com/wp-dyn/content/article/2005/11/26/AR2005112600857.html

———, "Corralling Domestic Intelligence: Standards in the Works for Reports of Suspicious Activity," *Washington Post*, January 13, 2006, p. A05. As of October 15, 2008: http://www.washingtonpost.com/wp-dyn/content/article/2006/01/12/AR2006011201852.html

———, "Pentagon to End Talon Data-Gathering Program," *Washington Post*, April 25, 2007, p. A10. As of October 15, 2008: http://www.washingtonpost.com/wp-dyn/content/article/2007/04/24/AR2007042402540.html

Png, I. P. L., *On the Value of Privacy from Telemarketing: Evidence from the "Do Not Call" Registry*, working paper, September 2007. As of October 20, 2008: http://www.comp.nus.edu.sg/~ipng/research/DNC_value.pdf

Posner, Richard A., *Uncertain Shield: The U.S. Intelligence System in the Throes of Reform*, Lanham, Md.: Rowman and Littlefield, 2006.

Powner, David A., director, Information Technology Management Issues, U.S. Government Accountability Office, *Information Technology: Homeland Security Network Needs to Be Better Coordinated with Key State and Local Initiatives*, testimony before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Washington, D.C.: U.S. Government Accountability Office, GAO-07-822T, May 10, 2007. As of October 15, 2008: http://www.gao.gov/new.items/d07822t.pdf

Princeton Survey Research Associates and CBS News/New York Times poll, January and June 2002.

Public Law 235, National Security Act, July 26, 1947.

Public Law 104-191, Health Insurance Portability and Accountability Act, August 21, 1996.

Public Law 107-296, Homeland Security Act, November 25, 2002.

Public Law 108-458, Intelligence Reform and Terrorism Prevention Act, December 17, 2004.

Quinn, Thomas D., director, Federal Air Marshals Service, U.S. Transportation Security Administration, "Tactical Information Sharing System," *Police Chief*, Vol. 73, No. 2, February 2006. As of October 15, 2008: http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=810&issue_id=22006

Ratcliffe, J., "Intelligence-Led Policing and the Problems of Turning Rhetoric into Practice," *Policing and Society*, Vol. 12, No. 1, January 2002, pp. 53–66.

Regan, Tom, "Does '24' Encourage US Interrogators to 'Torture' Detainees?" *Christian Science Monitor*, February 12, 2007. As of October 16, 2008: http://www.csmonitor.com/2007/0212/p99s01-duts.html

Richelson, Jeffrey T., *The U.S. Intelligence Community*, 5th ed., Boulder, Colo.: Westview Press, 2008.

Riley, K. Jack, Gregory F. Treverton, Jeremy M. Wilson, and Lois M. Davis, *State and Local Intelligence in the War on Terrorism*, Santa Monica, Calif.: RAND Corporation, MG-394-RC, 2005. As of October 10, 2008: http://www.rand.org/pubs/monographs/MG394/

Risen, James, and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, December 16, 2005. As of October 15, 2008: http://www.nytimes.com/2005/12/16/politics/16program.html

Risk Analysis, Special Issue on Terrorism, Vol. 27, No. 3, June 2007, pp. 503–787.

Roberts, John, *The Modern Firm: Organizational Design for Performance and Growth*, Oxford and New York: Oxford University Press, 2004.

Rood, Justin, "Exclusive: FBI Data Mining Program Raises Eyebrows in Congress," *The Blotter* (ABC News), June 12, 2007. As of October 15, 2008: http://blogs.abcnews.com/theblotter/2007/06/exclusive_fbi_d.html

Rosen, Jeffrey, "A Watchful State," *New York Times*, October 7, 2001. As of October 20, 2008: http://query.nytimes.com/gst/fullpage.html?res=9505E4DE123DF934A35753C1A9679C8B63

Rosenau, William, "Al Qaeda Recruitment in the United States: A Preliminary Assessment," *The MIPT Terrorism Annual 2004*, Oklahoma City, Okla.: National Memorial Institute for the Prevention of Terrorism, 2005, pp. 23–31. As of October 20, 2008: http://www.terrorisminfo.mipt.org/pdf/2004-MIPT-Terrorism-Annual.pdf

Ross, Brian, and Rhonda Schwartz, "Official Who Criticized Homeland Security Is Out of a Job," ABC News, December 9, 2004. As of December 30, 2007: http://abcnews.go.com/WNT/Investigation/story?id=316582&page=1

Ross, Darrell L., and Madhava R. Bodapati, "A Risk Management Analysis of the Claims, Litigation, and Losses of Michigan Law Enforcement Agencies: 1985–1999," *Policing*, Vol. 29, No. 1, 2006, pp. 38–57.

Sagan, Scott D., "The Problem of Redundancy Problem: Why More Nuclear Security Forces May Produce Less Nuclear Security," *Risk Analysis*, Vol. 24, No. 4, 2004, pp. 935–946. As of October 17, 2008: http://iis-db.stanford.edu/pubs/20274/Redundancy_Risk_Analysis.pdf

Sales, Nathan Alexander, "Secrecy and National Security Investigations," *Alabama Law Review*, Vol. 58, No. 4, 2007, pp. 811–884.

Salyers, Rick, and Troy Lutrick, "Best Defense," *Fire Chief*, February 1, 2007. As of October 20, 2008:
http://firechief.com/preparedness/firefighting_best_defense/

Schildkraut, Deborah J., "The More Things Change . . . American Identity and Mass and Elite Responses to 9/11," *Political Psychology*, Vol. 23, No. 3, September 2002, pp. 511–535.

Schulhofer, Stephen J., *The Enemy Within: Intelligence Gathering, Law Enforcement, and Civil Liberties in the Wake of September 11*, New York: Century Foundation Press, 2002.

Scott, W. Richard, *Organizations: Rational, Natural, and Open System*, 5th ed., New York: Prentice Hall, 2002.

"Secret Internet Protocol Router Network (SIPRNET)," Federation of American Scientists, updated March 3, 2000. As of October 15, 2008:
http://www.fas.org/irp/program/disseminate/siprnet.htm

"Security," *Jane's Sentinel Security Assessment: North America*, July 7, 2008.

Seifert, Jeffrey W., *Data Mining and Homeland Security: An Overview*, Washington, D.C.: Congressional Research Service, Library of Congress, RL31798, January 27, 2006. As of October 15, 2008:
http://www.fas.org/sgp/crs/intel/RL31798.pdf

Shane, Scott, "C.I.A. to Release Documents on Decades-Old Misdeeds," *New York Times*, June 22, 2007. As of October 20, 2008:
http://www.nytimes.com/2007/06/22/washington/22cia.html?fta=y

Shelby, Senator Richard C., vice chair, U.S. Senate Select Committee on Intelligence, "September 11 and the Imperative of Reform in the U.S. Intelligence Community," December 10, 2002. As of October 14, 2008:
http://intelligence.senate.gov/shelby.pdf

Shukovsky, Paul, Tracy Johnson, and Daniel Lathrop, "The FBI's Terrorism Trade-Off," *Seattle Post-Intelligencer*, April 11, 2007. As of October 17, 2008:
http://seattlepi.nwsource.com/national/311046_fbiterror11.html

Siegal, Jonathan R., "Chilling Injuries as a Basis for Standing," *Yale Law Journal*, Vol. 98, No. 5, March 1989, pp. 905–924.

Simon, Steven, and Jonathan Stevenson, "Her Majesty's Secret Service," *National Interest*, Winter 2005–2006.

Sims, Jennifer E., and Burton L. Gerber, eds. *Transforming U.S. Intelligence*, Washington, D.C.: Georgetown University Press, 2005.

Skrzycki, Cindy, "Writing Rules and Pricing Rights at the OMB," *Washington Post*, September 30, 2003, p. E1.

Solove, Daniel J., "Privacy and Power: Computer Databases and Metaphors for Information Privacy," *Stanford Law Review*, Vol. 53, No. 6, July 2001, pp. 1393–1462.

———, "A Taxonomy of Privacy," *University of Pennsylvania Law Review*, Vol. 154, No. 3, January 2006, pp. 477–560.

Spiller, Suzel, "FBI's Field Intelligence Groups and Police: Joining Forces," *FBI Law Enforcement Bulletin*, Vol. 75, No. 5, May 2006, pp. 1–6. As of October 14, 2008:
http://www.fbi.gov/publications/leb/2006/may06leb.pdf

Stanhouse, Darren W., "Comment: Ambition and Abdication: Congress, the Presidency, and the Evolution of the Department of Homeland Security," *North Carolina Journal of International Law and Commercial Regulation*, Vol. 29, No. 4, 2004, pp. 691–712.

Studeman, Michael, "Strengthening the Shield: U.S. Homeland Security Intelligence," *International Journal of Intelligence and Counterintelligence*, Vol. 20, No. 2, June 2007, pp. 195–216.

Sullivan, John P., *Networked All-Source Fusion for Intelligence and Law Enforcement Counter-Terrorism Response*, paper presented at the Annual Meeting of the International Studies Association, Montreal, Quebec, Canada, March 17, 2004.

Sunstein, Cass R., "Terrorism and Probability Neglect," *Journal of Risk and Uncertainty*, Vol. 26, No. 2–3, March 2003, pp. 121–136.

Sweeney, Latanya, *Uniqueness of Simple Demographics in the U.S. Population*, Pittsburgh, Pa.: Carnegie Mellon University, Laboratory for International Data Privacy working paper 4, 2000.

———, *Privacy-Preserving Surveillance Using Selective Revelation*, Pittsburgh, Pa.: Carnegie Mellon University, Laboratory for International Data Privacy working paper 15, February 2005. As of October 20, 2008:
http://privacy.cs.cmu.edu/dataprivacy/projects/selectiverevelation/pps.pdf

Taipale, Kim A., "Technology, Security, and Privacy: The Fear of Frankenstein, the Mythology of Privacy, and the Lessons of King Ludd," *International Journal of Communications Law and Policy*, Vol. 9, Autumn 2004, pp. 4–98. As of October 20, 2008:
http://www.ijclp.net/files/ijclp_web-doc_8-cy-2004.pdf

Tandy, Honorable Karen P., administrator, Drug Enforcement Administration, statement before the U.S. House of Representatives Committee on Appropriations Subcommittee on Science; the Departments of State, Justice, and Commerce; and Related Agencies, April 6, 2006. As of October 15, 2008:
http://www.usdoj.gov/dea/pubs/cngrtest/ct040606.html

Tanner, Mark, Foreign Terrorist Tracking Task Force, Federal Bureau of Investigation, "Foreign Terrorist Tracking Task Force (FTTTF)," testimony before the U.S. House of Representatives Committee on the Judiciary Subcommittee on Immigration, Border Security, and Claims, October 16, 2003. As of November 5, 2008:
http://www.fbi.gov/congress/congress03/tanner101603.htm

TAPAC—*see* U.S. Department of Defense Technology and Privacy Advisory Committee.

Theoharis, Athan G., "Researching the Intelligence Agencies: The Problem of Covert Activities," *Public Historian*, Vol. 6, No. 2, Spring 1984, pp. 67–76.

———, *The FBI and American Democracy: A Brief Critical History*, Lawrence, Kan.: University Press of Kansas, 2004.

Thessin, Jonathan, "Recent Development: Department of Homeland Security," *Harvard Journal on Legislation*, Vol. 40, No. 2, Summer 2003, pp. 513–536.

Transportation Security Administration, "Our Mission: Law Enforcement," undated (a) Web page. As of October 15, 2008:
http://www.tsa.gov/lawenforcement/mission/

———, "Secure Flight Program," undated (b) Web page. As of October 15, 2008:
http://www.tsa.gov/what_we_do/layers/secureflight/

———, "Transportation Worker Identification Credential (TWIC™): Layers of Security," undated (c) Web page. As of July 20, 2007:
http://www.tsa.gov/what_we_do/layers/twic/

———, "What Is TSA?" undated (d) Web page. As of October 15, 2008:
http://www.tsa.gov/who_we_are/what_is_tsa.shtm

———, "TSA Teams Up with the American Trucking Associations to Prevent and Respond to Terrorism," press release, March 23, 2004. As of October 15, 2008:
http://www.tsa.gov/press/releases/2004/press_release_0405.shtm

———, notice of proposed rulemaking, Secure Flight program, August 8, 2007. As of October 20, 2008:
http://www.dhs.gov/xlibrary/assets/SecureFlightNPRM20070809.pdf

Travel Industry Association, "The Power of Travel," undated Web page. As of October 20, 2008:
http://poweroftravel.org

———, "The Power of Travel: Research and Publications," updated June 2008. As of October 20, 2008:
http://www.tia.org/researchpubs/economic_research_impact_tourism.html

Treverton, Gregory F., "Intelligence: Welcome to the American Government," in Thomas E. Mann, ed., *A Question of Balance: The President, the Congress, and Foreign Policy*, Washington, D.C.: Brookings Institution, 1990, pp. 70–108.

———, *Reshaping National Intelligence for an Age of Information*, Santa Monica, Calif.: RAND Corporation, CB-397, 2001. As of October 16, 2008: http://www.rand.org/pubs/commercial_books/CB397/

———, "Terrorism, Intelligence, and Law Enforcement: Learning the Right Lessons," *Intelligence and National Security*, Vol. 18, No. 4, December 2003, pp. 121–140.

———, *The Next Steps in Reshaping Intelligence*, Santa Monica, Calif.: RAND Corporation, OP-152-RC, 2005. As of October 17, 2008: http://www.rand.org/pubs/occasional_papers/OP152/

———, *Reorganizing U.S. Domestic Intelligence: Assessing the Options*, Santa Monica, Calif.: RAND Corporation, MG-767-DHS, 2008. As of November 5, 2008: http://www.rand.org/pubs/monographs/MG767/

TSA—*see* Transportation Security Administration.

Tsvetovat, Maksim, and Kathleen M. Carley, "On Effectiveness of Wiretap Programs in Mapping Social Networks," *Computational and Mathematical Organization Theory*, Vol. 13, No. 1, March 2007, pp. 63–87.

United States v. Truong Dinh Hung, 629 F. 2d 908, 4th Cir., July 17, 1980.

Unknown, Office of General Counsel, Federal Bureau of Investigation, "RE: Question . . .," email exchange among eight unknown addressees, Office of General Counsel, Federal Bureau of Investigation, August 19, 2005. Redacted version released under the Freedom of Information Act on June 16, 2007. As of October 15, 2008: http://www.eff.org/files/filenode/07656JDB/070507_nsl09.pdf

U.S. Air Force Office of Special Investigations, undated (a) home page. As of July 30, 2007: http://www.osi.andrews.af.mil/main/welcome.asp

———, "U.S. Air Force Eagle Eyes," undated (b) Web page. As of July 30, 2007: http://www.osi.andrews.af.mil/eagleeyes/

U.S. Army Criminal Investigation Command, "Mission in Depth," undated Web page. As of July 30, 2007: http://www.cid.army.mil/mission2.html

U.S. Census Bureau, "State and County QuickFacts: USA," last revised July 25, 2008. As of October 20, 2008: http://quickfacts.census.gov/qfd/states/00000.html

U.S. Citizenship and Immigration Services, "About Us," last updated April 24, 2008. No longer available.

U.S. Coast Guard, "Coast Guard Launches America's Waterway Watch to Encourage Reporting of Suspicious Activity," press release, Washington, D.C., March 3, 2005. As of October 14, 2008:
https://www.piersystem.com/go/doc/786/65244/

———, "Drug Interdiction," last modified March 19, 2008a. As of October 15, 2008:
http://www.uscg.mil/hq/cg5/cg531/drug_interdiction.asp

———, "USCG Headquarters Organization: HQ Directorates," last modified October 14, 2008b. As of October 15, 2008:
http://www.uscg.mil/top/units/org.asp

U.S. Coast Guard Investigative Service, home page. Accessed May 17, 2006; no longer available.

U.S. Coast Guard Operations Systems Center, *Notice of Arrival*, undated brochure.

U.S. Code, Title 5, Government Organization and Employees, Section 552a, Records Maintained on Individuals.

———, Title 5, Government Organization and Employees, Section 901, Purpose.

———, Title 5, Government Organization and Employees, Section 902, Definitions.

———, Title 5, Government Organization and Employees, Section 903, Reorganization Plans.

———, Title 5, Government Organization and Employees, Section 905, Limitation on Powers.

———, Title 5, Government Organization and Employees, Section 908, Rules of Senate and House of Representatives on Reorganization Plans.

———, Title 5, Government Organization and Employees, Section 909, Terms of Resolution.

———, Title 5, Government Organization and Employees, Section 910, Introduction and Reference of Resolution.

———, Title 5, Government Organization and Employees, Section 911, Discharge of Committee Considering Resolution.

———, Title 5, Government Organization and Employees, Section 912, Procedure After Report or Discharge of Committee; Debate; Vote on Final Passage.

———, Title 12, Banks and Banking, Section 3402, Access to Financial Records by Government Authorities Prohibited; Exceptions.

———, Title 18, Crimes and Criminal Procedure, Section 2709, Counterintelligence Access to Telephone Toll and Transactional Records.

———, Title 18, Crimes and Criminal Procedure, Section 2710, Wrongful Disclosure of Video Tape Rental or Sale Records.

———, Title 20, Education, Section 1232g, Family Educational and Privacy Rights.

———, Title 47, Telegraphs, Telephones, and Radiotelegraphs, Section 551, Protection of Subscriber Privacy.

U.S. Computer Emergency Readiness Team, "About Us," undated Web page. As of October 15, 2008:
http://www.us-cert.gov/aboutus.html

U.S. Congress, 5th Congress, 2nd Session, *An Act Supplementary to and to Amend the Act [E]ntitled 'An Act to Establish a Uniform Rule of Naturalization; and to Repeal the Act Heretofore Passed on That Subject*, June 18, 1798.

———, 109th Congress, 2nd Session, *Making Appropriations for the Department of Homeland Security for the Fiscal Year Ending September 30, 2007, and for Other Purposes: Conference Report (to Accompany H.R. 5441)*, September 28, 2006. As of October 10, 2008:
http://purl.access.gpo.gov/GPO/LPS75576

"US Congress Reassesses Surveillance Laws," *Jane's Intelligence Digest*, September 17, 2007.

U.S. Constitution, September 17, 1787. As of October 17, 2008:
http://www.loc.gov/rr/program/bib/ourdocs/Constitution.html

U.S. Customs and Border Protection, "For Travel Industry Personnel," undated Web page. As of November 6, 2008:
http://www.cbp.gov/xp/cgov/travel/inspections_carriers_facilities/

———, "Interagency Border Inspection System (IBIS) Fact Sheet," Web page. Accessed July 23, 2007; no longer available.

———, *Performance and Accountability Report: Fiscal Year 2006*, December 19, 2006. As of October 15, 2008:
http://nemo.cbp.gov/of/customs_report.pdf

U.S. Department of Commerce Bureau of Industry and Security, "BIS Program Offices," undated Web page. As of October 15, 2008:
http://www.bis.doc.gov/about/programoffices.htm

U.S. Department of Defense, Department of Defense Counterintelligence Field Activity (DoD CIFA), Department of Defense Directive 5105.67, February 19, 2002.

———, DoD Antiterrorism (AT) Program, Department of Defense Directive 2000.12, August 18, 2003, certified current as of December 13, 2007. As of October 15, 2008:
http://www.dtic.mil/whs/directives/corres/pdf/200012p.pdf

U.S. Department of Defense Counterintelligence Field Activity, "What's New at CIFA: Proposal to Realign CIFA into New Defense CI and HUMINT Center," last updated August 21, 2008. No longer available.

U.S. Department of Defense Office of the Inspector General, "Support to the Global War on Terror (GWOT): Defense Criminal Investigative Service," last updated September 25, 2008. As of January 18, 2007:
http://www.dodig.mil/gwot_iraq/gwot.htm

U.S. Department of Defense Technology and Privacy Advisory Committee, *Safeguarding Privacy in the Fight Against Terrorism: Report of the Technology and Privacy Advisory Committee*, Washington, D.C., March 2004. As of October 15, 2008:
http://purl.access.gpo.gov/GPO/LPS52114

U.S. Department of Energy, "About DOE," undated Web page. As of October 15, 2008:
http://www.doe.gov/about/

U.S. Department of Homeland Security, *Privacy Impact Assessment for the Fraud Tracking System (FTS)*, June 24, 2005. As of October 15, 2008:
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscisfts.pdf

———, *DHS Intelligence Enterprise Strategic Plan*, Washington, D.C., January 2006a.

———, *Privacy Impact Assessment for the Automated Targeting System*, November 22, 2006b. As of October 15, 2008:
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats.pdf

———, *MATRIX Report: DHS Privacy Office Report to the Public Concerning the Multistate Anti-Terrorism Information Exchange (MATRIX) Pilot Project*, Washington, D.C., December 2006c. As of October 20, 2008:
http://www.dhs.gov/xlibrary/assets/privacy/privacy-matrix-122006.pdf

———, *Air Domain Surveillance and Intelligence Integration Plan: Supporting Plan to the National Strategy for Aviation Security*, March 26, 2007a. As of October 15, 2008:
http://www.dhs.gov/xlibrary/assets/hspd16_domsurvintelplan.pdf

———, *National Preparedness Guidelines*, Washington, D.C., September 2007b. As of October 20, 2008:
http://www.dhs.gov/xlibrary/assets/National%5FPreparedness%5FGuidelines.pdf

———, *Target Capabilities List: A Companion to the National Preparedness Guidelines*, September 2007c. As of October 20, 2008: https://www.llis.dhs.gov/displayContent?contentID=26724

———, "National Protection and Programs Directorate," last reviewed or modified September 11, 2008a. As of July 17, 2007: http://www.dhs.gov/xabout/structure/editorial_0794.shtm

———, "National Cybersecurity Division," last reviewed or modified October 3, 2008b. As of October 15, 2008: http://www.dhs.gov/xabout/structure/editorial_0839.shtm

———, "Directorate for Science and Technology," last reviewed or modified October 10, 2008c. As of October 15, 2008: http://www.dhs.gov/xabout/structure/editorial_0530.shtm

———, "Office of Operations Coordination," Web page, last reviewed or modified October 10, 2008d. As of October 14, 2008: http://www.dhs.gov/xabout/structure/editorial_0797.shtm

U.S. Department of Homeland Security Office of Security, Enforcement, and Investigations, "ICE: Consolidated Enforcement Environment (2008)," February 12, 2007. As of October 15, 2008: http://www.dhs.gov/xlibrary/assets/mgmt/e300-ice-consolidated2008.pdf

U.S. Department of Homeland Security Office of the Inspector General, *Improved Security Required for Transportation Security Administration Networks (Redacted)*, Washington, D.C.: Office of Information Technology, OIG-05-31, August 2005. As of October 15, 2008: http://www.dhs.gov/xoig/assets/mgmtrpts/OIGr_05-31_Aug05.pdf

———, *Survey of DHS Data Mining Activities*, Washington, D.C., OIG-06-56, August 2006. As of October 14, 2008: http://purl.access.gpo.gov/GPO/LPS84430

———, *Survey of DHS Intelligence Collection and Dissemination (Unclassified Summary)*, Washington, D.C., OIG-07-49, June 5, 2007a. As of October 13, 2008: http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_07-49_Jun07.pdf

———, *ADVISE Could Support Intelligence Analysis More Effectively*, Washington, D.C., OIG-07-56, July 2, 2007b. As of October 14, 2008: http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_07-56_Jun07.pdf

U.S. Department of Homeland Security Privacy Office, *Report to Congress on the Impact of Data Mining Technologies on Privacy and Civil Liberties*, Washington, D.C.: U.S. Department of Homeland Security, 108-774, July 6, 2006. As of October 15, 2008: http://purl.access.gpo.gov/GPO/LPS88776

U.S. Department of Justice, Federal Bureau of Investigation Regional Data Exchange, fiscal year 2008 justification, December 15, 2006. As of October 15, 2008:
http://www.usdoj.gov/jmd/2008justification/exhibit300/fbi_rdex.pdf

———, "Federal Bureau of Investigation," in *Organization, Mission, and Functions Manual*, September 12, 2007. As of October 15, 2008:
http://www.usdoj.gov/jmd/mps/manual/fbi.htm

U.S. Department of Justice Audit Division, *Follow-Up Audit of the Federal Bureau of Investigation's Efforts to Hire, Train, and Retain Intelligence Analysts*, Washington, D.C., audit report 07-30, April 2007. As of October 17, 2008:
http://www.usdoj.gov/oig/reports/FBI/a0730/final.pdf

U.S. Department of Justice Criminal Justice Information Services, "Integrated Automated Fingerprint Identification System or IAFIS," last updated March 13, 2008. As of October 15, 2008:
http://www.fbi.gov/hq/cjisd/iafis.htm

U.S. Department of Justice Dru Sjodin National Sex Offender Public Web Site, undated (a) home page. As of October 15, 2008:
http://www.nsopr.gov/

———, "Investigative Support," undated (b) Web page. As of October 15, 2008:
http://www.nw3c.org/isupport/overview.cfm

———, "Vision and Mission," undated (c) Web page. As of October 15, 2008:
http://www.nw3c.org/overview/mission.cfm

U.S. Department of Justice Global Justice Information Sharing Initiative and U.S. Department of Homeland Security Homeland Security Advisory Council, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era—Guidelines for Establishing and Operating Fusion Centers at the Local, State, and Federal Levels: Law Enforcement Intelligence, Public Safety, and the Private Sector*, Washington, D.C.: U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, August 2006. As of October 15, 2008:
http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf

U.S. Department of Justice National Crime Information Center, undated home page. As of October 15, 2008:
http://www.fbi.gov/hq/cjisd/ncic.htm

U.S. Department of Justice Office of the Inspector General, *The Department of Justice's Terrorism Task Forces: Evaluation and Inspections Report*, Washington, D.C., I-2005-007, June 2005a. As of October 14, 2008:
http://www.usdoj.gov/oig/reports/plus/e0507/

———, *Review of the Terrorist Screening Center's Efforts to Support the Secure Flight Program*, Washington, D.C., audit report 05-34, August 2005b. As of October 15, 2008:
http://www.usdoj.gov/oig/reports/FBI/a0534/final.pdf

———, *Review of United States Attorneys' Offices' Use of Intelligence Research Specialists*, I-2006-003, December 2005c. As of October 16, 2008: http://www.usdoj.gov/oig/reports/EOUSA/e0603/final.pdf

———, *A Review of the FBI's Handling of Intelligence Information Related to the September 11 Attacks*, Washington, D.C., June 2006a. As of October 13, 2008: http://www.usdoj.gov/oig/special/s0606/final.pdf

———, *Follow-Up Review of the Drug Enforcement Administration's Efforts to Control the Diversion of Controlled Pharmaceuticals: Evaluations and Inspections Report*, I-2006-004, July 2006b. As of October 15, 2008: http://www.usdoj.gov/oig/reports/DEA/e0604/

———, *Follow-Up Review of the FBI's Progress Toward Biometric Interoperability Between IAFIS and IDENT*, I-2006-007, July 2006c. As of October 15, 2008: http://www.usdoj.gov/oig/reports/FBI/e0607/final.pdf

———, *A Review of the Federal Bureau of Investigation's Use of National Security Letters*, Washington, D.C., March 2007. As of October 15, 2008: http://www.usdoj.gov/oig/special/s0703b/final.pdf

U.S. Department of State, "Bureau of Intelligence and Research," undated Web page. As of October 15, 2008: http://www.state.gov/s/inr/

U.S. Department of Transportation, undated organizational chart. As of October 15, 2008: http://www.dot.gov/chart.html

———, "Mission and History," last updated June 27, 2007. As of October 15, 2008: http://www.dot.gov/mission.htm

U.S. Department of the Treasury, Office of Terrorism and Financial Intelligence, undated organizational chart. As of October 15, 2008: http://www.ustreas.gov/offices/enforcement/pdf/org-chart.pdf

———, Office of Terrorism and Financial Intelligence, "The Office of Intelligence and Analysis (OIA)," last updated August 25, 2008a. As of October 15, 2008: http://www.ustreas.gov/offices/enforcement/oia/

———, Office of Terrorism and Financial Intelligence, "Mission," last updated October 2, 2008b. As of October 15, 2008: http://www.ustreas.gov/offices/enforcement/

U.S. Drug Enforcement Administration, "Aviation," undated (a) Web page. As of October 15, 2008: http://www.usdoj.gov/dea/programs/aviation.htm

———, "DEA Mission Statement," undated (b) Web page. As of October 15, 2008: http://www.usdoj.gov/dea/agency/mission.htm

———, "Diversion Control," undated (c) Web page. As of October 15, 2008: http://www.usdoj.gov/dea/programs/diversion.htm

———, "El Paso Intelligence Center," undated (d) Web page. As of October 15, 2008:
http://www.dea.gov/programs/epic.htm

———, "HIDTAs," undated (e) Web page. As of October 15, 2008: http://www.usdoj.gov/dea/programs/hidta.htm

———, "Mobile Enforcement Teams," undated (f) Web page. No longer available.

———, "National Drug Pointer Index," undated (g) Web page. As of October 15, 2008:
http://www.usdoj.gov/dea/programs/ndpix.htm

———, "Operations Pipeline and Convoy," undated (h) Web page. As of October 15, 2008:
http://www.usdoj.gov/dea/programs/pipecon.htm

———, "Organizational Chart," undated (i) Web page. As of October 15, 2008: http://www.usdoj.gov/dea/agency/orgchart.html

———, "Organized Crime Drug Enforcement Task Forces (OCDETF)," undated (j) Web page. As of October 15, 2008:
http://www.usdoj.gov/dea/programs/ocdetf.htm

———, "State and Local Task Forces," undated (k) Web page. As of October 15, 2008:
http://www.usdoj.gov/dea/programs/taskforces.htm

U.S. Environmental Protection Agency, *U.S. Environmental Protection Agency Strategic Plan for Homeland Security*, Washington, D.C., September 2002.

U.S. Government Accountability Office, *Identity Theft: Prevalence and Cost Appear to Be Growing*, Washington, D.C.: U.S. General Accounting Office, GAO-02-363, March 2002a. As of October 20, 2008:
http://purl.access.gpo.gov/GPO/LPS38410

———, *Information Technology: Justice Plans to Improve Oversight of Agency Projects*, Washington, D.C.: U.S. General Accounting Office, GAO-03-135, November 22, 2002b.

———, *Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, Washington, D.C.: U.S. General Accounting Office, GAO-04-385, February 2004a. As of October 15, 2008:
http://purl.access.gpo.gov/GPO/LPS45174

———, *Coast Guard: Relationship Between Resources Used and Results Achieved Needs to Be Clearer—Report to the Subcommittee on Oceans, Fisheries, and Coast Guard, Committee on Commerce, Science, and Transportation, U.S. Senate*, Washington, D.C.: U.S. General Accounting Office, GAO-04-432, March 2004b. As of October 15, 2008:
http://purl.access.gpo.gov/GPO/LPS51998

———, *Data Mining: Federal Efforts Cover a Wide Range of Uses*, Washington, D.C.: U.S. General Accounting Office, GAO-04-548, May 2004c. As of October 20, 2008:
http://purl.access.gpo.gov/GPO/LPS49947

———, *Data Mining: Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain—Report to the Ranking Minority Member, Subcommittee on Oversight of Government Management, Committee on Homeland Security and Governmental Affairs, U.S. Senate*, Washington, D.C.: U.S. Government Accountability Office, GAO-05-866, August 2005. As of October 14, 2008:
http://purl.access.gpo.gov/GPO/LPS64387

———, *Terrorist Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public*, Washington, D.C., GAO-06-1031, September 2006a. As of October 16, 2008:
http://purl.access.gpo.gov/GPO/LPS76494

———, *Homeland Security: Opportunities Exist to Enhance Collaboration at 24/7 Operations Centers Staffed by Multiple DHS Agencies*, Washington, D.C., GAO-07-89, October 2006b. As of October 15, 2008:
http://purl.access.gpo.gov/GPO/LPS76414

———, *Homeland Security: Progress Has Been Made to Address the Vulnerabilities Exposed by 9/11, but Continued Federal Action Is Needed to Further Mitigate Security Risks—Report to Congressional Requesters, House of Representatives*, Washington, D.C.: U.S. Government Accountability Office, GAO-07-375, January 2007a. As of October 15, 2008:
http://purl.access.gpo.gov/GPO/LPS78775

———, *Information Technology: Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information-Sharing Initiatives—Report to the Chairman, Committee on Homeland Security, House of Representatives*, Washington, D.C.: U.S. Government Accountability Office, GAO-07-455, April 2007b. As of October 16, 2008:
http://purl.access.gpo.gov/GPO/LPS82926

———, *Homeland Security: Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers*, Washington, D.C., GAO-08-35, October 2007c. As of October 15, 2008:
http://purl.access.gpo.gov/GPO/LPS90145

U.S. House of Representatives Committee on the Judiciary Subcommittee on Crime, Terrorism, and Homeland Security, "Law Enforcement Efforts Within the Department of Homeland Security," hearing, February 3, 2004. As of October 17, 2008:
http://commdocs.house.gov/committees/judiciary/hju91604.000/hju91604_0f.htm

U.S. Immigration and Customs Enforcement, "Fact Sheet: ICE Office of Investigations," July 7, 2004.

———, "About Us: Contact, Office of Intelligence," last modified March 22, 2006a. As of October 15, 2008:
http://www.ice.gov/about/intel/contact.htm

———, "Fact Sheet: ICE Office of Intelligence," last modified April 12, 2006b.

———, "National Fugitive Operations Program," last modified September 22, 2006c. As of October 15, 2008:
http://www.ice.gov/pi/dro/nfop.htm

———, "The Road to El Dorado," last modified November 24, 2006d. As of October 15, 2008:
http://www.ice.gov/partners/cornerstone/eldorado_taskforce.htm

———, "Topics of Interest: Trade-Based Money Laundering," last modified November 24, 2006e. As of October 15, 2008:
http://www.ice.gov/partners/financial/topics.htm

———, *ICE Fiscal Year 2006 Annual Report: Protecting National Security and Upholding Public Safety*, c. 2007a. As of October 15, 2008:
http://www.ice.gov/doclib/about/ice-06ar.pdf

———, "Operation Community Shield," last modified October 31, 2007b. As of October 15, 2008:
http://www.ice.gov/pi/investigations/comshield/

———, "About Us: ICE Operations," last modified October 2, 2008. As of October 15, 2008:
http://www.ice.gov/about/operations.htm

U.S. Intelligence Community, "Members of the Intelligence Community (IC)," undated Web page. As of July 24, 2007:
http://www.intelligence.gov/1-members.shtml

U.S. Marshals, "Criminal Information Branch," undated Web page. As of October 15, 2008:
http://www.usmarshals.gov/investigations/asu/asu.htm

———, "Fact Sheet: United States Marshals," Washington, D.C., 21-A, December 3, 2007. As of October 15, 2008:
http://www.usmarshals.gov/duties/factsheets/general.pdf

U.S. Northern Command, "About USNORTHCOM," undated Web page. No longer available.

U.S. Nuclear Regulatory Commission, "Threat Assessment," April 24, 2007. As of October 15, 2008:
http://www.nrc.gov/security/threat.html

———, "About NRC," September 26, 2008. As of October 15, 2008:
http://www.nrc.gov/about-nrc.html

U.S. Pacific Command, "U.S. Pacific Command Strategic Foundation," undated Web page. As of July 30, 2007:
http://www.pacom.mil/about/mvp-statements.shtml

———, "Joint Interagency Force West (JIATF-W)," last updated September 23, 2008.

U.S. Secret Service, "About the U.S. Secret Service Electronic Crimes Task Forces," undated (a) Web page. As of October 15, 2008:
http://www.secretservice.gov/ectf_about.shtml

———, "Criminal Investigations," undated (b) Web page. As of October 15, 2008:
http://www.secretservice.gov/criminal.shtml

———, "Electronic Crimes Task Forces and Working Groups," undated (c) Web page. As of October 15, 2008:
http://www.secretservice.gov/ectf.shtml

———, "Financial Crimes Division," undated (d) Web page. As of October 15, 2008:
http://www.secretservice.gov/financial_crimes.shtml

———, "Protective Mission," undated (e) Web page. As of October 15, 2008:
http://www.secretservice.gov/protection.shtml

U.S. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, *Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans*, Book III: *Final Report*, Washington, D.C., April 23, 1976.

U.S. Southern Command, "About Us," last updated April 15, 2008. As of October 15, 2008:
http://www.southcom.mil/AppsSC/pages/about.php

U.S. Special Operations Command, "United States Special Operations Command Mission," undated fact sheet. As of October 15, 2008:
http://www.socom.mil/Docs/Command_Mission_26112007.pdf

U.S. Statutes, Title 1, Section 566, An Act to Establish a Uniform Rule of Naturalization, June 18, 1798.

———, Title 1, Section 570, An Act Concerning Aliens, June 25, 1798.

———, Title 1, Section 577, An Act Respecting Alien Enemies, July 6, 1798.

———, Title 1, Section 5, An Act for the Punishment of Certain Crimes Against the United States, July 14, 1798.

———, Title 12, Section 755, Habeas Corpus Act, March 3, 1863.

———, Title 36, Section 825, United States White-Slave Traffic Act, June 25, 1910.

———, Title 39, Section 874, Immigration Act, February 5, 1917.

———, Title 40, Section 217, Espionage Act of 1917, May 16, 1918.

———, Title 40, Section 553, Sedition Act, May 16, 1918.

———, Title 40, Section 1012, Immigration Act of October 16, 1918, October 16, 1918.

———, Title 54, Section 670, Alien Registration Act, June 28, 1940.

"U.S. to Pay $2M for False Terror Arrest," CBS News, November 29, 2006. As of October 20, 2008:
http://www.cbsnews.com/stories/2006/11/29/national/main2216468.shtml

USA Freedom Corps, "Citizen Corps," undated Web page. As of October 15, 2008:
http://www.freedomcorps.gov/about_usafc/programs/citizencorps.asp

USCG—*see* U.S. Coast Guard.

USIC—*see* U.S. Intelligence Community.

Vaughn, Michael S., Tab W. Cooper, and Rolando V. del Carmen, "Assessing Legal Liabilities in Law Enforcement: Police Chiefs' Views," *Crime and Delinquency*, Vol. 47, No. 1, January 2001, pp. 3–27.

Warrick, Joby, "Intelligence-Gathering Program May Be Halted," *Washington Post*, April 2, 2008, p. A08. As of October 14, 2008:
http://www.washingtonpost.com/wp-dyn/content/article/2008/04/02/AR2008040200077.html

Washington-Baltimore High Intensity Drug Trafficking Area, "Investigative Support Center (ISC)," undated Web page. As of October 15, 2008:
http://www.hidta.org/isc/isc.asp

Weber, Max, *The Theory of Social and Economic Organization*, A. M. Henderson, trans., Talcott Parsons, ed., Glencoe, Ill.: Free Press, 1947.

Weisburd, David, and Anthony Allan Braga, eds., *Police Innovation: Contrasting Perspectives*, Cambridge and New York: Cambridge University Press, 2006.

Weldon, Honorable Curt, U.S. Representative, "Able Danger and Intelligence Information Sharing," testimony before the U.S. Senate Committee on the Judiciary, September 21, 2005.

Whitelaw, Kevin, "The Eye of the Storm," *U.S. News and World Report*, October 29, 2006. As of October 14, 2008: http://www.usnews.com/usnews/news/articles/061029/6center.htm

Wildhorn, Sorrel, Brian Michael Jenkins, and Marvin Lavin, *Intelligence Constraints of the 1970s and Domestic Terrorism*, Vol. I: *Effects on the Incidence, Investigation, and Prosecution of Terrorist Activity*, Santa Monica, Calif.: RAND Corporation, N-1901-DOJ, 1982. As of October 20, 2008: http://www.rand.org/pubs/notes/N1901/

Wilensky, Harold L., *Organizational Intelligence: Knowledge and Policy in Government and Industry*, New York, Basic Books, 1967.

Winton, Richard, Teresa Watanabe, and Greg Krikorian, "LAPD Defends Muslim Mapping Effort," *Los Angeles Times*, November 10, 2007. As of October 16, 2008: http://www.latimes.com/news/local/la-me-lapd10nov10,0,3960843.story

WMD Commission—*see* Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction.

Wohlstetter, Roberta, *Pearl Harbor: Warning and Decision*, Stanford, Calif.: Stanford University Press, 1962.

Youngstown Sheet and Tube Co. v. Sawyer, 343 U.S. 579, 72 S. Ct. 863, 96 L. Ed. 1153, June 2, 1952.

Zegart, Amy B., *Flawed by Design: The Evolution of the CIA, JCS, and NSC*, Stanford, Calif.: Stanford University Press, 1999.

———, *Spying Blind: The FBI, the CIA and the Origins of 9/11*, Princeton, N.J.: Princeton University Press, 2007.