

BRENNAN

CENTER

FOR JUSTICE

DOMESTIC INTELLIGENCE:
NEW POWERS, NEW RISKS

Emily Berman

ABOUT THE BRENNAN CENTER FOR JUSTICE

The Brennan Center for Justice at New York University School of Law is a non-partisan public policy and law institute that focuses on the fundamental issues of democracy and justice. Our work ranges from voting rights to campaign finance reform, from racial justice in criminal law to presidential power in the fight against terrorism. A singular institution – part think tank, part public interest law firm, part advocacy group – the Brennan Center combines scholarship, legislative and legal advocacy, and communications to win meaningful, measurable change in the public sector.

ABOUT THE BRENNAN CENTER'S LIBERTY AND NATIONAL SECURITY PROJECT

The Brennan Center initiated its Liberty and National Security Project as part of its Justice Program to foster better public understanding of the importance of accountability, transparency, and checks and balances in the formulation and implementation of national security policy. We have since been at the forefront of advocating for sound, rights-respecting policy based on broad public education, legislative advocacy, litigation, and scholarly activity.

ABOUT THE AUTHOR

Emily Berman is Counsel in the Liberty and National Security Project at the Brennan Center for Justice. She works through litigation, advocacy, and scholarship to promote rights-protecting and effective oversight of United States national security policy. Before joining the Brennan Center, Ms. Berman was at New York University School of Law pursuing her LL.M. in International Law. She clerked for Judge John M. Walker, Jr. of the Second Circuit Court of Appeals and graduated magna cum laude from New York University School of Law.

ACKNOWLEDGEMENTS

The author would like to thank Liza Goitein, David Udell, Faiza Patel, Aziz Huq, Ellen Fisher, R. Kyle Alagood, Susan Lehman, Jeanine Plant-Chirlin, and Michael Waldman for their invaluable comments and assistance. Thanks for research assistance go to Lorraine Leete, Patrick Wylie, Alice Clapman, and Alexander Stone-Tharpe. The author also greatly benefited from conversations with Zachary W. Carter, Sung-Hee Suh, Samuel Issacharoff, James E. Johnson, Steven Schulhofer, Mike German, Kate Martin, and members of the Muslim American Civil Liberties Coalition. The Brennan Center is grateful to The Atlantic Philanthropies, Open Society Foundations, The Herb Block Foundation, and The William C. Bullitt Foundation, Inc. for their generous support of our Liberty and National Security Project. The views expressed in this report are solely the responsibility of the Brennan Center.

© 2011. This paper is covered by the Creative Commons "Attribution-No Derivs-NonCommercial" license (see <http://creativecommons.org>). It may be reproduced in its entirety as long as the Brennan Center for Justice at NYU School of Law is credited, a link to the Center's web page is provided, and no charge is imposed. The paper may not be reproduced in part or in altered form, or if a fee is charged, without the Center's permission. Please let the Center know if you reprint.

TABLE OF CONTENTS

| | |
|---|-----------|
| Executive Summary | 1 |
| Introduction | 4 |
| I. Background on the Attorney General's Guidelines | 7 |
| A. The Role of the FBI | 7 |
| B. The Genesis and Development of the Attorney General's Guidelines | 8 |
| 1. The Pre-Guidelines Era: 1908-1976 | 8 |
| 2. The Levi Guidelines: 1976-1980 | 10 |
| 3. The Erosion of the Guidelines' Protections: 1980-2008 | 13 |
| C. The Mukasey Guidelines: 2008-Present | 21 |
| II. The New Changes Should Be Reconsidered | 26 |
| A. The Guidelines' Adverse Effects on Civil Liberties and Law Enforcement Effectiveness | 26 |
| 1. Threat of Privacy Invasions | 26 |
| 2. Chill to First-Amendment-Protected Activity | 28 |
| 3. Dangers of Profiling | 30 |
| 4. Risks of Excessive Collection | 36 |
| B. Operational Considerations Do Not Justify the 2008 Changes | 37 |
| Recommendations | 43 |
| Conclusion | 45 |

TABLE OF CHARTS

| | |
|---|----|
| Standards for Investigations | 16 |
| Permissible Investigative Methods | 18 |
| Time Limits & Supervisory Approval Requirements | 19 |

EXECUTIVE SUMMARY

Successful domestic counterterrorism policy is vital to keep the homeland safe. In this effort, policymakers must resist the oft-exhibited tendency to overreact to the threats we face. This overreaction, time and again,¹ takes a similar form: In the face of a perceived existential threat, we expand the scope of the government’s powers while simultaneously diminishing oversight of and accountability for the use of those powers. We fail to ensure that these powers will be employed in a manner consistent with our fundamental values. Civil liberties—such as privacy and freedom of expression, association, and religion—are often curtailed. In the wake of 9/11, government action exhibited this tendency across a wide range of counterterrorism policies.

To his credit, President Obama acknowledged this overreaction in several areas, implementing much-needed modifications to inherited policies, which improved procedural protections, guarded against civil liberties violations, and increased transparency. But in many respects, the Obama Administration’s counterterror efforts resemble those of the Bush Administration’s second term. This is especially true in the context of countering domestic terrorism threats.

One key example: The Obama Administration’s choice to rely upon rules drafted by its predecessor to increase the FBI’s authority for domestic investigations, including probes into terrorist threats. We believe these rules, known as the Attorney General’s Guidelines for Domestic FBI Operations (“Attorney General’s Guidelines” or “Guidelines”), tip the scales too far in favor of relatively unchecked government power, allowing the FBI to sweep too much information about too many innocent people into the government’s view. In so doing, they pose significant threats to Americans’ civil liberties and risk undermining the very counterterrorism efforts they are meant to further.

And while some may doubt the severity of these threats, nobody can argue that such broad powers in the hands of government officials should not be monitored regularly to ensure that they are not being abused.

The Guidelines, implemented by Attorney General Michael Mukasey in December 2008, are considerably more permissive than earlier versions implemented by previous Attorneys General. This permissiveness raises two concerns. First, the Guidelines expand the FBI’s discretion to investigate individuals and groups while simultaneously limiting oversight requirements and thereby risk opening the door to invasions of privacy and the use of profiling on the basis of race, ethnicity, religion, national origin, or political ideology. In so doing they also risk chilling constitutionally protected activities. Second, the Guidelines could render the FBI’s counterterrorism efforts less effective. Some perceive investigations under these Guidelines to impact disproportionately the freedom of expression and association of law-abiding members of certain groups. This perception risks undermining any otherwise beneficial aspects of the Guidelines by alienating the very communities whose cooperation is most essential. Moreover, the sheer volume of information collected raises the concern that it will elude meaningful analysis.

The Mukasey Guidelines significantly loosen the restrictions on the FBI's investigative powers that had been in place for decades—restrictions that remained even in the Guidelines implemented by Attorney General John Ashcroft in the wake of 9/11—in the following ways:

1. They authorize “non-predicated” investigations—substantive investigative activity in circumstances in which there is no “information or . . . allegation indicating” wrongdoing or a threat to national security.²
2. They permit intrusive investigative techniques—such as using informants, conducting interviews under false pretenses, and engaging in unlimited physical surveillance—during non-predicated investigations.
3. They encourage the government to collect, retain, and disseminate vast amounts of information about law-abiding individuals.
4. They weaken procedural safeguards—eliminating or reducing many of the requirements for supervisory approval of particular investigative techniques and temporal limits on investigative activity—that have been integral to the Guidelines’ regime since it was first implemented in 1976.

These changes are not merely cosmetic. They grant the FBI license to employ intrusive techniques to investigate Americans when there is no indication that any wrongdoing has taken place. This means that FBI agents can collect and retain vast amounts of information, much of it about the innocent activities of law-abiding Americans. And it can then retain that information indefinitely and share it with other government agencies. It is thus crucial to ensure that sufficient limits, as well as meaningful internal and external checks, are imposed on this power.

We cannot know how much of this information-collection occurs, or how frequently it leads to the identification and neutralization of threats. But what we do know is that the Guidelines grant government officials significant discretion in making investigative decisions. In the absence of meaningful limitations on the FBI's authority, agents or informants may attend religious services or political gatherings to ascertain what is being preached and who is attending. They may focus their attention on particular religious or ethnic communities. They may gather and store in their databases information about where individuals pray, what they read, and who they associate with. All with no reason to suspect criminal activity or a threat to national security. And then they may keep that information in their databases, regardless of whether it indicated any wrongdoing.

We also know that without sufficient limits and oversight, well-meaning efforts to keep the homeland safe—efforts which rely heavily on the collection and analysis of significant amounts of information about Americans—can adversely impact civil liberties. Indeed, history teaches that insufficiently checked domestic investigative powers frequently have been abused and that the burdens of this abuse most often fall upon disfavored communities and those with unpopular political views. Investigations triggered by race, ethnicity, religious belief, or political ideology may seem calibrated to address the threat we face, but instead they

routinely target innocent people and groups. Beyond the harm done to individuals, such investigations invade privacy, chill religious belief, radicalize communities and, ultimately, build resistance to cooperation with law enforcement.

Given the risks posed by placing such power in officials' hands, it is particularly important to ensure that the FBI's domestic authorities are designed and implemented in ways to ensure both that they minimize these adverse effects and that the cost of any drawbacks that do persist is outweighed by what is gained. In other words, unless the Guidelines effectively enable law enforcement to counter the terrorist threat, the risks they pose to civil liberties are too high. It is therefore also critical to know how the Guidelines are being administered and whether they are effective.

In designing Guidelines that allow the FBI to combat the threat of terrorism while protecting our values, it is important to note one additional fact: the United States is not at war with Islam. Indeed, to the contrary. Presidents Obama and George W. Bush both took great pains to disavow any implication that the U.S. struggle was against Islam as such.³ Policymakers past and present,⁴ scholars,⁵ national security experts,⁶ and terrorists⁷ themselves all recognize that any appearance that the U.S. views Islam as the enemy actually provides Al Qaeda and its allies propaganda that aids recruitment and creates additional risk for our armed forces.⁸ While a tiny minority of Muslims adopt a perverse version of their faith that encourages violence, the vast majority of American Muslims are law-abiding, patriotic, productive members of society. Any investigative scheme that singles out groups or individuals for government scrutiny based on the assumption that all Muslims in the U.S. are potential terrorists fosters an environment of suspicion and distrust and is likely counterproductive as well.

Again, we do not know exactly how these powers are being used or whether they are being abused. Nor do we know what measures, if any, the Justice Department has taken to protect against such abuse. What we do know is this: the Guidelines, on their face, raise new and troubling concerns about possible violations of civil liberties on a wide scale. Ensuring that such abuses do not, in fact, take place requires two types of remedies. First, some of the powers extended to the FBI should be curtailed. In addition to any substantive changes, however, we must ensure that there are meaningful checks on the FBI's remaining powers—internal checks, such as supervisory approval requirements and regular reviews, as well as external checks, from both Congress and the public.

The current Guidelines can be modified relatively easily. A few changes will limit agents' discretion and increase oversight and accountability mechanisms. This report recommends two types of changes to the existing guidelines. First, procedural mechanisms should be put in place to ensure sufficient oversight of how the Guidelines are used, and whether they are effective. Such mechanisms must exist both within the Justice Department and outside it. For example, Congress should undertake regular reviews of the Guidelines, the ways in which they are being implemented, and their level of effectiveness. Second, some of the most dramatic expansions of FBI power should be scaled back, both to ensure that intrusive investigative methods are used only when there are facts indicating a need for further investigation and to guard against improper consideration of race, religion, ethnicity, national origin, or political ideology in investigative decisions.

INTRODUCTION

Each of the following examples of law enforcement investigative activity shares two characteristics. First, each provides an example of problems posed when law enforcement agents conduct their operations in the absence of clear—sufficiently regulated and enforced—limits on investigative activity. Second, none yielded any evidence of terrorist activity or threats to America’s security. Consider the following:

- From 2003 to 2007, in violation of law and FBI policy, the FBI misused so-called “exigent letters”—informal requests for information that may be used in lieu of formal subpoenas in limited, emergency situations—and other forms of informal information requests to obtain thousands of phone records that were not connected with terrorism emergencies.⁹ According to the Justice Department’s Inspector General, the unlawful practices, which included the acquisition of the phone records of reporters,¹⁰ were widespread, systemic, and the result of significant management failures.¹¹ The result was what the Inspector General called an “egregious breakdown” of the FBI’s responsibility to comply with privacy laws and internal policies.¹²
- In 2009, the North Central Texas Fusion System,¹³ a joint enterprise by FBI and local law enforcement, made public a “Prevention Awareness Bulletin.” The Bulletin informed recipients that it was “imperative for law enforcement offices to report” the activities of lobbying groups, Muslim civil rights organizations, and anti-war groups in their areas.¹⁴
- In 2007, in Orange County, California, the Council on American-Islamic Relations reported a suspected terrorist to the FBI. The “suspect” had been barred from a mosque for promoting terrorist plots and attempting to recruit others. It later emerged that the agitator was an FBI informant paid to infiltrate area mosques—despite the fact that the FBI had assured Muslim community leaders that it was not monitoring their places of worship.¹⁵
- Documents disclosed through Freedom of Information Act (FOIA) requests and confirmed by an Inspector General report indicate that the members and activities of several religious and political organizations—including Greenpeace, the Global Network Against Weapons and Nuclear Power in Space, and the Catholic Workers’ Union—have been subjects of FBI surveillance.¹⁶ These same documents show that the FBI has collected information regarding the Thomas Merton Center, an organization committed to “nonviolent struggle to bring about a more peaceful world,” and its anti-war protests.¹⁷
- From 2001 to 2006, in the course of investigations into anti-war groups, environmental activists, and animal-rights activists, the FBI conducted investigations with insufficient factual predicate, failed to document properly the basis for investigations, improperly extended the duration of investigations, and considered as “domestic terrorism cases” investigations into potential crimes—such as trespassing and vandalism—that are not commonly considered terrorism, raising “questions about whether the FBI has expanded the definition of domestic terrorism to people who engage in mainstream political activity, including nonviolent protest and civil disobedience.”¹⁸

When government officials operate with increased discretion, individual liberties, particularly privacy rights and First Amendment rights to speak and to gather, often suffer.

The concerns raised by these examples—risk of government overreaching to acquire information that may or may not be useful—are always present, but they are particularly stark when investigations lack concrete focus. When government officials operate with increased discretion, individual liberties, particularly privacy rights and First Amendment rights to speak and to gather, often suffer. At the same time, the risk increases that law enforcement agents will rely on inappropriate criteria—race, religion, national origin, ethnicity or political leanings—as the basis for investigation. In short, the greater the official discretion, the greater the potential for abuse.

American law enforcement agencies have three primary roles: 1) solving crimes committed in the past, 2) preventing crimes that are imminent, and 3) collecting intelligence to stop future crimes. The further law enforcement moves toward the intelligence-collection end of the spectrum, the more expansive, and the less dependent on concrete indicia of crime or threat the investigation is likely to be. Overreach on the part of law enforcement is therefore of particular concern when it involves intelligence-gathering.

Historically, the FBI has vacillated between a crime-solving and intelligence-gathering focus. Originally created to investigate specific federal crimes, the Bureau expanded into the notorious Hoover-era domestic intelligence agency, famous for excess and overreach. Revelations of Hoover-era abuses prompted the Bureau to refocus for a time on crime-solving, and a season of robust oversight and operational limitations on intelligence gathering followed. These limits were set forth in an internal set of rules, known since their creation, as the “Attorney General’s Guidelines.”

The first set of Guidelines, issued in 1976, was designed to authorize FBI domestic intelligence investigations and also to answer concerns about excessive intrusiveness on the part of the agency and its agents. The Guidelines sought to tether the FBI’s intelligence-gathering activities to crime detection and prevention. They demanded a higher level of evidence of possible criminal activity (past or future) in order to justify the use of more intrusive investigative techniques. Initially, the Guidelines cabined the FBI’s activities successfully. But the restrictions began to erode over time, and the agency again expanded its intelligence-collection activities.

The expansion was slow for many years but accelerated rapidly in the wake of the 9/11 attacks. And the Guidelines that Attorney General Ashcroft issued in 2002 dramatically loosened previous restrictions.

After the Ashcroft revisions went into effect, several independent and congressional commissions concluded that insufficient coordination between foreign intelligence-collection efforts and domestic law-enforcement efforts contributed to the government’s failure to detect—and prevent—the 9/11 plot. Attorney General Michael Mukasey responded by issuing further-revised Guidelines in December 2008. Like the changes implemented by Attorney General Ashcroft in the wake of 9/11, the Mukasey Guidelines stress the FBI’s mission of preventing

terrorist attacks. At the same time, they further liberalize the limits and oversight regime designed to check abuses of investigative power by extending time limits and eliminating supervisory approval requirements.

The current Guidelines' focus on terror prevention—rather than terror response—is commendable. Investigating imminent criminal activity or threats to the homeland is of obvious value. However, intelligence investigations pose unique risks. History teaches that as the government's discretionary intelligence-collection powers grow, so, too, do instances of profiling based on race, religion, national origin, or unpopular viewpoint.

These risks are perhaps more salient today than ever before. Gone are the file cabinets J. Edgar Hoover stuffed with information on political enemies. They have been replaced by massive (and growing) electronic databases of information about Americans who may pose no security threat. It is therefore critical that the FBI implements its domestic investigative activities in ways that avoid unnecessarily compromising the civil liberties of law-abiding Americans or the effectiveness of the FBI's terrorism prevention efforts. The current Guidelines fail to prescribe rules designed to prevent the excesses—and their consequences—that can flow from the expansive authority they confer. The predictable result will be to chill the free exercise of religion, association, and expression of the population as a whole and to alienate the very communities whose cooperation is most vital to successful national security efforts.¹⁹

This report proceeds as follows. Part I will briefly describe the FBI's history, why the Attorney General's Guidelines initially were created, how they have evolved over the years, and what the changes were wrought by the current Guidelines. Part II will then explore some of the negative effects likely to flow from those changes. It will then briefly conclude with some specific recommendations for adjustments to the Guidelines.

I. BACKGROUND ON THE ATTORNEY GENERAL'S GUIDELINES

A. The Role of the FBI

The most familiar type of FBI investigation is one aimed at traditional law enforcement, known today as a “general crimes investigation.” These usually begin after and in response to the commission of a particular criminal act. They are meant to determine “who committed that act and...secur[e] evidence to establish the elements of the particular offense.”²⁰ The object of the investigation is clearly defined. Its scope is limited. Its focus extends only to evidence relevant to elements of the particular crime. And the investigation ends when the crime is solved.

A second type of investigation is one that collects intelligence in order to deter the commission of future criminal acts. Intelligence investigations may consist of domestic investigations into criminal enterprises, such as organized crime syndicates or terrorist organizations, known as “criminal intelligence investigations.” Or they may aim to collect foreign intelligence, which is defined as “information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorists.”²¹ Criminal intelligence investigations are open-ended by nature and last longer than general crimes investigations. “[T]here may be no completed offense to provide a framework for the investigation. ...[T]he investigation is broader and less discriminate,”²² collecting information on the “size and composition of the group involved, its geographic dimensions, its past acts and intended criminal goals, and its capacity for harm.”²³ Foreign intelligence investigations share many of these characteristics as well.

As the Justice Department recognizes, the open-ended nature of intelligence investigations coupled with their attenuated connection to specific crimes poses particular risks. In the absence of clearly defined limits on an investigation and its scope, purpose, or duration, it is likely that agents will collect much information about law-abiding Americans. And an investigation of organizational activity “may present special problems particularly where it deals with politically motivated acts. ... [S]pecial care must be exercised in sorting out protected activities from those which may lead to violence or serious disruption of society.”²⁴ Thus, while the FBI has conducted investigations for both law enforcement and intelligence purposes throughout its history, it is the intelligence-collection activities that occasion the most frequent calls for reform.

Debate over the proper role of the FBI—whether it is primarily a crime-solving entity, a domestic-intelligence agency, or some mixture of the two—has not yet yielded a definitive answer. Indeed, the FBI’s statutory mandate remains remarkably vague. There is no legislative charter defining the FBI’s purpose or setting out the scope of its authority.²⁵ Congress’s hands-off approach to the Bureau’s role leaves the Department of Justice (“DOJ”), the Attorney General, the Director of National Intelligence, and the FBI Director with enormous discretion to determine the Bureau’s goals and how it will pursue them.

Some of the methods the FBI employs, such as seizing items from inside a suspect’s home and monitoring electronic communications, are subject to constitutional and statutory constraints.²⁶ But the FBI has a host of

investigative tools at its disposal that are effectively unregulated. At times the FBI has exploited this regulatory void, going so far as to attack anonymously the political beliefs of targets to induce their employers to fire them; to mail letters anonymously to spouses of intelligence targets in order to destroy their marriages; or to disseminate misinformation in order to disrupt demonstrations and encourage violence.²⁷

As discussed below, the use of many of these tactics led to the promulgation of the first set of Attorney General's Guidelines in 1976. Though some of the most troubling tactics are impermissible under the current Guidelines, many tactics authorized by the current Guidelines involve significant intrusion into the private lives of Americans. These include permitting FBI agents (or informants acting under FBI instructions) to spy on worship services or political gatherings; to question family, friends, neighbors, and coworkers of an investigative target without revealing that they are FBI agents; to engage in 24-hour physical surveillance of targets; and to monitor the addresses to which targets send letters and the phone numbers that they call. Given the significant intrusion these and other permissible techniques allow, it is vital to have rules in place to ensure that the uses to which these techniques are put are appropriate.

B. The Genesis and Development of the Attorney General's Guidelines

1. The Pre-Guidelines Era: 1908-1976

The FBI originated in the early 1900s as a small cadre of investigators—known as the Bureau of Investigation—that reported directly to the Attorney General and were responsible for investigating the few federal crimes that then existed.²⁸ The Bureau's first foray into domestic intelligence activities came with the United States' entry into World War I in 1917; then the Bureau's responsibilities expanded to include investigation of possible violations of the Espionage, Selective Service, and Sabotage Acts.²⁹ The result: the investigation of thousands of individuals for “un-American activities.”³⁰

In the 1920s, Attorney General Harlan Fiske Stone attempted to return the Bureau to its pre-war role, directing that its activities be “limited strictly to investigations of violations of the law.”³¹ But this limitation was short-lived. President Roosevelt instructed the FBI in the 1930s to collect domestic intelligence about “subversive activities,” especially on fascists and communists,³² as well as about possible crimes. In its effort to carry out these and similar directives from subsequent Presidents, Attorneys General, and other government officials through the 1970s, the FBI frequently scrutinized law-abiding domestic groups and individuals, and ultimately engaged in systematic abuse of its power and authority.³³

In the mid-1970s, the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, commonly known as the Church Committee for its chair Senator Frank Church (D-ID), exposed a number of covert—and often illegal—projects conducted by the intelligence community from the Eisenhower Administration onward.³⁴ Tellingly, the largest volume of the Committee's concluding report was the one addressing the activities of the FBI.

Congress and the public were outraged by the excesses of the U.S. intelligence community, especially programs like COINTELPRO (Counterintelligence Program)—a series of covert action programs initially directed against members of the Communist Party but ultimately expanded to target a broad range of domestic protest groups, including civil rights groups and others commonly known as the “New Left.” “In these programs,” the Church Committee found, “the Bureau went beyond the collection of intelligence to secret action designed to ‘disrupt’ and ‘neutralize’ target groups and individuals.”³⁵ The groups and individuals were targeted based not on their proclivity toward criminal activity, but instead on their political beliefs.³⁶ The purpose was to harass and discredit law-abiding—though often anti-war or pro-civil rights—groups and individuals,³⁷ employing the results of widespread surveillance using “wiretaps, bugs, break-ins, and mail opening targeting American citizens” to do so.³⁸ Not surprisingly, given this purpose, the FBI often failed to discontinue an investigation even when it had become clear that the targeted individual or organization was engaged in neither criminal nor subversive activities.³⁹

The Church Committee also identified specific abuses. These include attempts to provoke an Internal Revenue Service investigation to deter a protest leader from attending the Democratic National Convention; falsely labeling as government informants members of groups believed to be violent, in order to expose them to expulsion or physical attack; and attempting to provoke violent conflict between the leader of a Chicago street gang and the Black Panthers.⁴⁰ In attempting to incite violence among targeted groups, the FBI had turned its mission of solving and preventing crime on its head.

Perhaps most famously—driven by FBI Director J. Edgar Hoover’s distrust of and animosity towards the civil rights movement—the FBI engaged in intensive efforts to discredit Dr. Martin Luther King, Jr. and render him ineffective as a civil rights leader. Using techniques similar to those used against Soviet agents, the FBI subjected King to surveillance and wiretaps; waged a misinformation campaign to undermine his reputation; attempted to cause his marriage to fail; and even apparently endeavored to induce King’s suicide.⁴¹

Pressure grew for FBI reform. The Church Committee recommended that Congress pass a statutory charter governing the FBI’s activities,⁴² which would contain a “[f]oundational statement of the basic duties and responsibilities of the FBI” as well as limitations on its investigative powers.⁴³ Over the course of several years, Congress held hearings in an effort to develop such a charter.⁴⁴

The Attorney General's Guidelines

The Attorney General has issued guidelines governing the FBI's conduct in a number of areas. Examples include the Attorney General's Guidelines:

- Regarding the Use of Confidential Informants
- On FBI Undercover Operations
- On Foreign Intelligence Collection and Foreign Counterintelligence Investigation
- On Seized and Forfeited Property
- For Victim And Witness Assistance

As used in this report, the term "Guidelines" refers to the guidelines governing the FBI's domestic investigative powers, which have gone by several names:

- Levi Guidelines, 1976: *Domestic Security Investigation Guidelines*
- Civiletti Guidelines, 1982: *Guidelines on Criminal Investigations of Individuals and Organizations*
- Smith Guidelines, 1983: *Guidelines on Domestic Security/Terrorism Investigations*
- Thornburgh Guidelines, 1989: *Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations*
- Ashcroft Guidelines, 2002: *Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations*

The current version of the guidelines governing the FBI's domestic investigative powers, issued by Michael Mukasey in December 2008, are called the *Guidelines for Domestic FBI Operations*. They consolidate several sets of guidelines into one document:

- *Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations*
- *Supplemental Guidelines for Collection, Retention, and Dissemination of Foreign Intelligence*
- *Guidelines for Reporting and Use of Information Concerning Violation of Law and Authorization for Participating in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence, or International Terrorism Intelligence Investigations*
- *Guidelines for Reporting on Civil Disorders and Demonstrations Involving a Federal Interest*

2. The Levi Guidelines: 1976-1980

In an effort to stave off statutory reform, President Ford's Attorney General, Edward Levi, issued the first set of Attorney General's Guidelines, known as the Levi Guidelines, to govern the FBI's domestic intelligence activities.⁴⁵ The Guidelines were implemented at the height of the Cold War, but they were not merely an empty gesture designed to dilute proposed legislation. Attorney General Levi's reforms included substantive and important limits on the FBI's intelligence gathering, many derived from the Church Committee's recommendations. Therefore, though they were implemented unilaterally by the executive branch, their contents reflected meaningful congressional involvement.

The Levi Guidelines embodied the idea that “government monitoring of individuals or groups because they hold unpopular or controversial political views is intolerable in our society.”⁴⁶ Consequently, the Guidelines aimed to prevent such monitoring. To do so, they required “progressively higher standards and higher levels of review for more intrusive investigative techniques.” They also demanded “that domestic security investigations [were] tied closely with the detection of crime.” Finally, they implemented “safeguards against investigations of activities that are merely troublesome or unpopular.”⁴⁷

The 1976 Levi Guidelines resulted in a dramatic reduction in the number of “domestic security investigations”—the forerunner to today’s criminal intelligence investigations—conducted by the FBI. When these guidelines were issued in 1976, the FBI had 4,868 pending cases, a number that had dropped to just a few dozen by 1982.⁴⁸

The Levi Guidelines⁴⁹ set forth the permissible purpose for domestic security investigations and envisioned three increasingly robust investigative phases: preliminary, limited, and full investigations. For each successive investigative phase, a higher threshold of suspicion was necessary to proceed; the investigative tools agents were permitted to use were more intrusive; and procedural safeguards, such as supervisory approval before using certain techniques, were more stringent. This basic structure—increasingly intrusive levels of investigation, accompanied by higher suspicion thresholds and greater procedural constraints—has been retained in all subsequent versions of the Guidelines.

Required Nexus to Criminal Activity. The Levi Guidelines required a close tie between domestic security investigations and the prevention of criminal activity. They limited investigations to ascertaining “information on the activities of individuals, or the activities of groups, which involve or will involve the use of force or violence and which involve or will involve the violation of federal law.”⁵⁰

The Levi Guidelines embodied the idea that government monitoring of individuals or groups because they hold unpopular or controversial political views is intolerable in our society.

Standards. The 1976 Levi Guidelines allowed preliminary investigations based on “allegations or other information that an individual or group may be engaged in activities which involve or will involve the use of force or violence and which involve or will involve the violation of federal law.”⁵¹ When a preliminary investigation proved inadequate to determine whether a full investigation was warranted, the Guidelines authorized a limited investigation to follow up.⁵² And the FBI could initiate a full investigation only on the basis of “specific and articulable facts giving reason to believe that an individual or group is or may be engaged in activities which involve the use of force or violence and which involve or will involve the violation of federal law.”⁵³

Investigative Authorities. Agents conducting a preliminary investigation could examine public sources of information, as well as federal, state, and local government records.⁵⁴ They could question existing informants, and they could conduct physical surveillance and interview others for the sole purpose of identifying the subject of the investigation.⁵⁵ The Guidelines prohibited, however, the use of “mail covers” (collecting the information on the outside of a piece of mail), the recruitment and tasking of informants, and electronic surveillance at the preliminary investigation stage.⁵⁶ Agents conducting limited investigations could employ the same techniques, as well as physical surveillance and interviews for purposes other than to identify the subject.⁵⁷ Agents conducting full investigations could employ all lawful techniques.

Procedural Safeguards. Under the Levi Guidelines, field offices could initiate preliminary investigations; agents were required to finish them within 90 days unless FBI headquarters authorized an extension.⁵⁸ A limited investigation had to be approved by either a Special Agent in Charge (SAC) or FBI headquarters,⁵⁹ and only headquarters could authorize a full investigation.⁶⁰ Further, the Guidelines required the FBI to notify the Justice Department of full investigations within a week of their initiation and to provide progress reports every 90 days.⁶¹ With respect to the more intrusive investigative techniques available at the later stages of an investigation, FBI headquarters had to approve the use of informants, the Attorney General had to approve the use of mail covers, and electronic surveillance had to comply with statutory restrictions.⁶²

Each of the above requirements served a crucial purpose. The differentiated levels of investigatory activity, and the higher threshold required to initiate each level, ensured that the FBI had sufficient evidence before bringing intrusive techniques to bear against a given target. Limiting the duration of investigations ensured that, once the FBI determined that a target was not involved in criminal activity, all investigative activity would cease. Supervisory authorization requirements provided a check on rogue agents who might disregard the Guidelines’ limits; they also created a procedural hurdle to help ensure that agents only sought to use intrusive techniques where truly necessary. Finally, reporting requirements ensured that the FBI’s activities were documented, which in turn served to deter unauthorized activity and to create an audit trail should there be allegations or indications of abuse.⁶³

Finally, the Levi Guidelines strove to ensure that the scope of investigations and the tactics they employed were constrained so as to avoid becoming any more intrusive than necessary. Investigations were required to be “designed and conducted so as not to limit the full exercise of rights protected by the Constitution and laws of the United States.”⁶⁴ Preliminary investigations were limited to gathering information pertinent to a decision to conduct or forego a full investigation,⁶⁵ and a decision to initiate a full investigation required consideration of the danger to privacy and free expression posed by the investigation.⁶⁶

Attorney General Levi also issued guidelines to govern foreign counterintelligence investigations (FCI),⁶⁷ which are investigations into “espionage and other intelligence activities, sabotage, and assassination conducted by, for, or on behalf of foreign powers, organizations, or persons.”⁶⁸

3. The Erosion of the Guidelines' Protections: 1980-2008

Since their inception, the Guidelines have functioned as the primary constraint on the FBI's operations, and they remain a justification for the lack of a statutory charter governing the FBI's activities.⁶⁹ Initially implemented in response to the perceived abuses by the FBI in the context of domestic intelligence collection, they represented an effort to reject the pre-guidelines practice of broad intelligence-collection activities unrelated to crimes or threats and instead to treat domestic threats as a facet of criminal law enforcement.⁷⁰ The purpose of the original Guidelines was thus to constrain the FBI's intelligence-collection role within acceptable bounds, to prevent it from interfering unduly in the lives of law-abiding groups or individuals, and to tether the FBI's activities to the detection and prevention of crime.

Attorney General Civiletti in 1980 issued new Guidelines, which incorporated the 1976 Levi Guidelines and added to them rules for investigating general crimes and racketeering enterprises.⁷¹

In 1983, Attorney General William French Smith again altered the structure of the Guidelines,⁷² expanding the concept of domestic security investigations—labeling them “criminal intelligence investigations”—to include both terrorism investigations and racketeering enterprise investigations.⁷³

The 1983 Smith Guidelines thus governed on the one hand “general crimes investigations” and on the other “criminal intelligence investigations,” which included both racketeering and domestic security/terrorism. And the FCI Guidelines, known by this time as the Foreign Intelligence Collection and Foreign Counterintelligence Investigation (FI/FCI) Guidelines, governed the FBI's collection of foreign intelligence and counterintelligence operations. So the full spectrum of the FBI's domestic activities was subject to the limits of various guidelines.⁷⁴

These limits on FBI authority did not preclude all possibility of misplaced domestic intelligence efforts. For example, a 1980s investigation into the Committee in Solidarity with the People of El Salvador (CISPES), an activist organization that opposed Reagan-era policies toward El Salvador, became an exercise in mapping the activities of a community engaged in lawful dissent.⁷⁵ The result was a broad investigation into the activity and membership of groups opposed to U.S. policy in El Salvador that produced “no reliable information of planned violence or other illegal activity.”⁷⁶ And the Cold-War-era Library Awareness Program included regular FBI visits to public libraries seeking information regarding individuals who read scientific and technical journals, sometimes asking “librarians to be wary of ‘foreigners’ or persons with ‘East European or Russian-sounding names.’”⁷⁷ These examples illustrate that even under a guidelines regime, meaningful limits, procedural safeguards, and effective oversight remain necessary to keep investigations from wandering too far afield and interfering with the activities of law-abiding individuals and groups.

But over time, and especially in the wake of perceived domestic intelligence and crime prevention failures, the lessons of history seem to have faded. Successive sets of guidelines, while expanding the breadth of

their coverage, have loosened restrictions on FBI operations. The commendable desire to prevent domestic threats, rather than merely to respond to them, has led to the expansion of the FBI's domestic-intelligence-collection and analysis role—a development that calls for increased vigilance against abuse, not the opposite. At the same time, the standard that must be met before the FBI can engage in investigative activity has become less and less stringent; both obligatory and discretionary limits on the intrusiveness of investigative techniques have been rolled back; and oversight and approval requirements have been relaxed.

Diminished Requirement of Nexus to Criminal Activity

Over time, the changes in the Guidelines have expanded the scope of information the FBI is permitted to pursue, allowing collection of information far removed from any suspicion of wrongdoing. The original Guidelines limited investigations to information regarding the use of force or violations of federal law.⁷⁸ The 1983 Smith Guidelines, however, envisioned investigations into matters of “legitimate law enforcement interest” rather than merely the “detection, prevention and prosecution of crimes.”⁷⁹ And they also introduced the concept of “criminal enterprises,” which granted the FBI the new power to take steps to discover the composition, size, scope, and goals of particular groups.⁸⁰ (The types of groups that could be subject to these broader investigations themselves broadened in 2002.⁸¹) Attorney General Reno’s 1995 reinterpretation of the Guidelines—prompted by the Oklahoma City bombing—further expanded the permissible scope of investigative activity by specifying that violations of law need not be imminent to justify investigation of domestic groups that advocate violence, so long as those groups had the ability to carry out violent acts in violation of federal law.⁸²

While these developments loosened the connection between completed or impending criminal acts and FBI authority to collect information, the Ashcroft Guidelines, prompted by the attacks of 9/11, nearly severed the tie altogether. In the post-9/11 era, crime prevention—always a part of the FBI’s work—shifted to the fore and dominated the FBI’s resources, focus, and conception of its core mission.⁸³ Indeed, its stated “central mission” became “preventing the commission of terrorist acts against the United States and its people.”⁸⁴ The Ashcroft Guidelines represented and enabled this sea change in the Bureau’s understanding of its role. It is impossible to overemphasize the degree to which this shift affected the Bureau’s investigative priorities and decisions. To effectuate the FBI’s new mission, the Ashcroft Guidelines “affirmatively authorize[d] agents to ‘scour public sources for information on future terrorist threats’ even in the absence of ‘specific investigative predicates.’”⁸⁵

Over time, the changes in the Guidelines have expanded the scope of information the FBI is permitted to pursue, allowing collection of information far removed from any suspicion of wrongdoing.

Attorney General Ashcroft also issued guidelines for FBI National Security Investigations (NSI Guidelines) in 2003 to replace the existing Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintel-

ligence Investigation (FI/FCI Guidelines). A full discussion of these 2003 guidelines and their evolution is impossible because portions of them are classified. But certain things are clear. The FI/FCI guidelines governed “all foreign intelligence, foreign counterintelligence ... and intelligence investigations of international terrorism conducted by the FBI.”⁸⁶ The NSI guidelines, by contrast, authorized “investigation by the FBI of threats to the national security of the United States; investigative assistance by the FBI to state, local, and foreign governments...; the collection of foreign intelligence by the FBI; the production of strategic analysis by the FBI; and the retention and dissemination of information resulting from the foregoing activities.”⁸⁷ The NSI Guidelines are thus broader in scope than their predecessors.

Relaxation of the Investigation Standard

The 1976 Levi Guidelines began by requiring “specific and articulable facts giving reason to believe that an individual or a group is or may be engaged in activities which involve the use of force or violence and which involve or will involve the violation of federal law”⁸⁸ in order to open a full investigation. Twenty-five years later, under the 2002 Ashcroft Guidelines, that same domestic intelligence investigation could be initiated based on merely a “reasonable indication” that a group is engaged in a terrorism or racketeering enterprise.⁸⁹ Preliminary inquiries, originally permitted only when information or allegations indicated the possibility of the use of force or violence,⁹⁰ and then limited to the general crimes context, could be carried out with an even lesser showing.

The Ashcroft Guidelines also designated “the prompt and extremely limited checking out of initial leads”—which was permitted “whenever information is received of such a nature that some follow-up as to the possibility of criminal activity is warranted”—as a new level of investigative activity before the preliminary inquiry.⁹¹

Standards for Investigations

| | Levi | Civiletti | Smith, Thornburgh, & Reno | Ashcroft |
|---|--|--|---|--|
| General Crimes | | | | |
| Checking of Leads | N/A | N/A | N/A | Information is received of such a nature that some follow-up as to the possibility of criminal activity is warranted |
| Preliminary Inquiries | N/A | Allegations or information indicating the possibility of criminal activity | No change | No change |
| Full Investigations | N/A | Facts or circumstances that reasonably indicate a federal crime has been, is being, or will be committed | No change | No change |
| Racketeering Enterprise Investigations | | | | |
| Checking of Leads | N/A | N/A | N/A | Same as general crimes |
| Preliminary Inquiries | N/A | N/A | N/A | Same as general crimes |
| Full Investigations | N/A | Facts or circumstances that reasonably indicate the existence of a racketeering enterprise whose activities include violence, extortion, or systematic public corruption | Facts or circumstances that reasonably indicate two or more persons are engaged in a continuing course of conduct for the purpose of obtaining monetary or commercial gains or profits wholly or in part through racketeering activity that includes violence, extortion, or systematic public corruption | Facts or circumstances that reasonably indicate two or more persons are engaged in a pattern of racketeering activity as defined in the RICO statute |
| Domestic Security Investigations | | | Domestic Security / Domestic Terrorism Investigations | Terrorism Investigations |
| Checking of Leads | N/A | No change | N/A | Same as general crimes |
| Preliminary Inquiries | Allegations or information indicating activities that involve the use of force or violence and that involve or will involve violation of federal law for the purpose of overthrowing or interfering with the activities or policies of a government or depriving persons of their civil rights | No change | N/A | Same as general crimes |
| Limited Investigations | When a preliminary inquiry is inadequate to determine if there is a factual basis for a full investigation | N/A | N/A | N/A |
| Full Investigations | Specific and articulable facts giving reason to believe that an individual or group is or may be engaged in activities which involve the use of force or violence and which involve or will involve violation of federal law for the purpose of overthrowing or interfering with the activities or policies of a government or depriving persons of their civil rights | No change | Facts or circumstances that reasonably indicate two or more persons are engaged in an enterprise for the purpose of furthering political or social goals wholly or in part through violence and a violation of federal criminal law | Facts or circumstances that reasonably indicate two or more persons are engaged in an enterprise for (a) furthering political or social goals wholly or in part through activities that involve force or violence and a violation of federal criminal law; (b) engaging in international or domestic terrorism that involves a violation of federal criminal law; or (c) committing any federal crime of terrorism |

Increase in the Intrusiveness of Investigative Authorities

Even as the standard for initiating investigations was relaxed, the intrusiveness of investigations increased. The first several sets of Guidelines contained what was essentially a “least intrusive method” rule. Agents were required to consider whether information available through use of an intrusive technique could be obtained in a timely and effective way by less intrusive means.⁹² Supervisors could approve highly intrusive techniques, but only under compelling circumstances and when other means were likely to be unavailing.

The “least intrusive means” standard was later undermined by the Ashcroft Guidelines, which paid lip service to the standard but added the caveat that agents should not “hesitate to use any lawful techniques consistent with these Guidelines, even if intrusive.”⁹³ Moreover, while the most intrusive methods remained subject to supervisory approval during preliminary investigations (though not necessarily during full investigations), the requirement of compelling circumstances was eliminated.⁹⁴ Such a caveat can have only one effect—to increase the intrusiveness of the tools that agents choose to employ.

More concretely, the Guidelines have evolved over time to permit the use of more intrusive methods at earlier stages of investigations where the nexus to criminal activity is often attenuated. The tasking of informants was originally allowed only in full investigations; the 1983 Smith Guidelines, however, allowed that method to be used in preliminary inquiries.⁹⁵ Similarly, the Smith Guidelines for the first time allowed the collection of publicly available information even before the requirements for a preliminary inquiry were satisfied.⁹⁵

The 2002 Ashcroft Guidelines continued this trend. They permitted the use of preliminary inquiries in the criminal intelligence investigation context,⁹⁷ thus opening up a wide range of investigative tools for use before the FBI had a reasonable indication that a group was engaged in wrongdoing. Moreover, in those preliminary inquiries, a technique that previously had been reserved for full investigations was added to the menu of available tactics—mail covers.⁹⁸ While collecting publicly available information absent any fact-based reason for suspicion had been permitted to a certain degree by the Smith Guidelines, the Ashcroft Guidelines expanded both the authority for and the focus on this practice.⁹⁹

Two groundbreaking aspects of the Ashcroft era bear emphasis. First, for the first time since the Guidelines’ inception, they permitted the FBI to attend First-Amendment-protected gatherings—such as religious services or political events—without any fact-based reason to suspect wrongdoing.¹⁰⁰ And second, the Ashcroft-issued 2003 NSI Guidelines permitted for the first time the use of National Security Letters during preliminary inquiries into threats to national security.¹⁰¹

It is important also to note that statutory changes have increased the intrusiveness of techniques approved by the Guidelines in ways that are not immediately apparent when looking at the Guidelines in isolation. The most illustrative example comes in the area of electronic surveillance. That technique—one of the most intrusive available to federal officials—always has been reserved for use only in full investigations. And the use of that technique always has been subject to statutory restrictions. But when those statutory restrictions loosen, the FBI’s authority to employ surveillance

expands. So while the Foreign Intelligence Surveillance Act used to require federal officials to show probable cause that a target was an agent of a foreign power before surveillance could be approved, statutory alterations enacted in 2008 permit surveillance of international communications so long as officials certify that their surveillance procedures are “reasonably designed” to limit the “targets” of the surveillance to “persons reasonably believed to be located outside the United States.”¹⁰² So while the Attorney General’s Guidelines themselves did not explicitly modify the permissible use of electronic surveillance, the surveillance power available to the FBI nonetheless expanded.

Similar statutory changes in the requirements for physical searches, the collection of financial, communications, and other types of records, many of them contained in the USA PATRIOT Act of 2001,¹⁰³ also permit increased FBI access to information.

| Permissible Investigative Methods | | | |
|--|--|--|---|
| | Levi | Civiletti, Smith, Thornburgh, & Reno | Ashcroft |
| Checking of leads | | | |
| | | | Authorized methods not specified |
| Preliminary Inquiries | | | |
| | Limited to the following methods: <ul style="list-style-type: none"> • Examination of FBI indices and files • Examination of public records or other public sources of information • Examination of federal, state, and local records • Use of previously established informants and sources of information • Physical surveillance and interviews for the purpose of identifying the subject of an investigation | The following methods were permitted with no supervisory approval: <ul style="list-style-type: none"> • Examination of FBI indices and files • Examination of public records or other public sources of information • Examination of federal, state, and local records • Interviews with the complainant, previously established informants, and confidential sources • Interviews of the potential subject • Interviews of persons who should readily be able to corroborate or deny the truth of the allegation EXCEPT pretext interview or interview of the potential subject’s employer or co-workers • Physical or photographic surveillance of any person All other methods not expressly barred are permitted with supervisory approval and subject to policy and statutory limitations. | No change *Note that while the methods available in preliminary inquiries did not change, the Ashcroft guidelines made preliminary inquiries available in racketeering and terrorism investigations. |
| Limited Investigations | | | |
| | Additional techniques: <ul style="list-style-type: none"> • Physical surveillance for other purposes • Interviews of persons not mentioned above for purposes other than identifying the subject of the investigation, if the interview is authorized by a Special Agent in Charge | | |
| Techniques Permitted Only in Full Investigations | | | |
| | <ul style="list-style-type: none"> • Mail covers (upon approval by the Attorney General) • Electronic surveillance • Recruitment of or placement of informants in groups (upon approval by FBI Headquarters and subject to review every 180 days) | <ul style="list-style-type: none"> • Mail covers • Mail openings • Nonconsensual electronic surveillance | <ul style="list-style-type: none"> • Mail covers • Nonconsensual electronic surveillance |

Relaxation of Procedural Safeguards

At the same time that the level of suspicion necessary to conduct investigations has fallen and the intrusiveness of investigations has risen, the procedural safeguards designed to ensure that the authorities conferred on FBI agents are not abused have eroded. Rules limiting the duration of investigations, or requiring supervisory authorization for use of particular investigative technique have become less stringent.

For example, the original Guidelines dictated that preliminary investigations could last just 90 days, and only FBI headquarters could authorize a full investigation.¹⁰⁴ Further, they required the FBI to notify the Justice Department of full investigations and provide periodic progress reports.¹⁰⁵ By the time of the Ashcroft Guidelines, preliminary inquiries could last 180 days—twice their original duration¹⁰⁶—and full criminal intelligence investigations were authorized and renewed for a period of one year, up from the original limit of 180 days.¹⁰⁷ Moreover, both preliminary and full investigations could be authorized or renewed by a SAC, rather than FBI headquarters,¹⁰⁸ and there is no mention of any requirement for Justice Department notification.

| Time Limits & Supervisory Approval Requirements | | | | |
|---|------|---|---|---|
| | Levi | Civiletti | Smith, Thornburgh, & Reno | Ashcroft |
| General Crimes | | | | |
| Checking of Leads | N/A | N/A | N/A | <ul style="list-style-type: none"> • Time Limit: unspecified, but performed “with eye towards promptly determining whether further investigation should be conducted” • Supervisory Approval: none |
| Preliminary Inquiries | N/A | <ul style="list-style-type: none"> • Time Limit: 60 days • Supervisory Approval: FBI Supervisor • Extensions: 30-day extensions may be granted by FBI Headquarters upon receipt of a written request and statement of reasons why further investigative steps are warranted when there is not “reasonable indication” of criminal activity | <ul style="list-style-type: none"> • Time Limit: 90 days • Supervisory Approval: FBI Supervisor • Extensions: 30-day extensions may be granted by FBI Headquarters upon receipt of a written request | <ul style="list-style-type: none"> • Time Limit: 180 days • Supervisory Approval: FBI Supervisor • Extensions: Up to two 90-day extensions may be granted by the Special Agent in Charge (SAC). Subsequent extensions may only be granted by FBI Headquarters upon a written request |
| Full Investigations | N/A | <ul style="list-style-type: none"> • Time Limit: 180 days • Supervisory Approval: FBI Director or a designated Assistant Director • Extensions: 180 days with authorization from the FBI Director or a designated Assistant Director | <ul style="list-style-type: none"> • Time Limit: unspecified • Supervisory Approval: FBI Supervisor | <ul style="list-style-type: none"> • Time Limit: unspecified • Supervisory Approval: FBI Supervisor |

Time Limits & Supervisory Approval Requirements continued

| | Levi | Civiletti | Smith, Thornburgh, & Reno | Ashcroft |
|--|--|---|--|--|
| Racketeering Enterprise Investigations | | | | |
| Full Investigations | N/A | <ul style="list-style-type: none"> • Time Limit: 180 days • Supervisory Approval: FBI Director or a designated Assistant Director • Extensions: 180 days with authorization from the FBI Director or a designated Assistant Director | <ul style="list-style-type: none"> • Time Limit: 180 days • Supervisory Approval: FBI Director or a designated Assistant Director (SAC under Reno) • Extensions: 180 days with authorization from the FBI Director or a designated Assistant Director <p><i>* Investigations of a racketeering enterprise not engaged in violence, narcotics, extortion, or systematic public corruption required written authorization by both the Attorney General and the FBI Director</i></p> | <ul style="list-style-type: none"> • Time Limit: 1 year • Supervisory Approval: SAC • Extensions: 1-year extensions available with the authorization of the SAC |
| Domestic Security Investigations | | | Domestic Security / Domestic Terrorism Investigations | Terrorism Investigations |
| Preliminary Inquiries | <ul style="list-style-type: none"> • Time Limit: 90 days from date upon which preliminary inquiry initiated • Supervisory Approval: none • Extensions: 90 days with FBI Headquarters' approval when facts or information obtained in the original period justify such an extension | No change | N/A | N/A |
| Limited Investigations | <ul style="list-style-type: none"> • Time Limit: Same as the Preliminary Inquiry upon which the investigation is based • Supervisory Approval: written authorization from a SAC or FBI Headquarters • Extensions: 90 days with FBI Headquarters' approval when facts or information obtained in the original period justify such an extension | No change | N/A | N/A |
| Full Investigations | <ul style="list-style-type: none"> • Time Limit: 1 year • Supervisory approval: FBI Headquarters • Extensions: 1 year with written authorization by the Department of Justice | No change | <ul style="list-style-type: none"> • Time Limit: 180 days • Supervisory Approval: FBI Director or a designated Assistant Director • Extensions: 180 days with authorization from the FBI Director or a designated Assistant Director | <ul style="list-style-type: none"> • Time Limit: 1 year • Supervisory Approval: SAC • Extensions: 1-year extensions available with the authorization of the SAC |

So this is the result of the evolution of the Guidelines from the time of their inception in 1976 to the time at which Attorney General Mukasey made his changes in 2008: They had made it easier and easier to open investigations, authorized more investigative techniques with less evidence of wrongdoing, and reduced the procedural safeguards meant to avoid a repetition of the abuses associated with unfettered FBI authority and discretion. As a consequence, even before the current Guidelines were implemented, the Bureau had returned nearly full-circle to an inadequately cabined intelligence-collection role similar to the one the pre-Guidelines Bureau played so problematically during the Cold War years.

C. The Mukasey Guidelines: 2008-Present

Attorney General Mukasey's Guidelines continue down the same path as the Ashcroft Guidelines. They expand the scope of the enormous changes initiated after the 9/11 attacks. These Guidelines, which remain in operation today, were hastily issued in the final months of the Bush Administration, despite congressional requests to delay the process to allow time for sufficient consideration, debate, and input.¹⁰⁹ They consolidate several types of guidelines, including the General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations Guidelines, and the National Security Investigations and Foreign Intelligence Collection Guidelines, into a single framework.¹¹⁰

1. The Mukasey Guidelines

The new Guidelines further expand the scope of information the Bureau may collect, magnifying the FBI's domestic-intelligence and prevention role. In the Guidelines' own words, "[t]he FBI is an intelligence agency as well as a law enforcement agency ... [whose] functions accordingly extend beyond limited investigations of discrete matters."¹¹¹ To this end, the Guidelines urge the Bureau to use its analytic authority to "identify and understand trends, causes, and potential indicia of criminal activity and other threats to the United States that would not be apparent from the investigation of discrete matters alone."¹¹²

Abandoning the idea that the FBI's primary role is to investigate crimes (past and imminent) that fall under its jurisdiction, the Guidelines envision that the FBI will assist and broadly share information with other federal agencies as well as state local, tribal, and foreign agencies.¹¹³ They also state that, because investigative activities "provide critical information needed for broader analytic and intelligence purposes to facilitate the solution and prevention of crime, protect the national security, and further foreign intelligence objectives," all information collected "at all stages of investigative activity is ... to be retained and disseminated for these purposes ... regardless of whether it furthers investigative objectives in a narrower or more immediate sense."¹¹⁴

In short, the Guidelines envision an FBI that vacuums up all the information made available to it by permissive investigative rules, disseminates the information to other government agencies, and retains it indefinitely—regardless of whether any unlawful or threatening conduct has been uncovered. While one might hope that self-restraint on the part of FBI agents would help shape and limit this amorphous authority, the Guidelines themselves discourage such a result. In an organization charged with terrorism prevention, anything less than a 100% success rate will be viewed as failure. This sort of expectation places enormous pressure on agents to use every shred of authority at their disposal—and more.¹¹⁵ That pressure must be counterbalanced by reasonable restrictions on and meaningful oversight of investigative authorities.

The Mukasey Guidelines, however, take just the opposite approach, further loosening investigative standards and procedural safeguards. With respect to the showing required to initiate preliminary and full investigations, the current Guidelines retain the standards from earlier Guidelines. Thus, preliminary investigations can be initiated

on the basis of any “information or an allegation indicating” possible criminal or national-security-threatening activity, and full investigations retain the “reasonable indication” standard.¹¹⁷

The primary innovation—and the primary problem—in the Mukasey Guidelines is their authorization of “assessments”—an investigative stage prior to a preliminary investigation—without “factual predicates.” More specifically, the Guidelines authorize highly intrusive investigative techniques at what the Guidelines call the “assessment” stage. Assessments, characterized as inquiries designed to determine whether further investigation is warranted, require only an “authorized purpose,” meaning that the FBI must merely determine that it is acting to protect against criminal or national-security threats, or to collect foreign intelligence.¹¹⁸ Thus these assessments permit intrusive investigations of people or organizations absent any facts indicating possible wrongdoing on the part of the investigation’s target—i.e., absent *any* “factual predicate.”

This is a sharp departure from past practice. Under the “checking out of leads” concept in the 2002 Ashcroft Guidelines, the FBI could engage only in “limited activity ... conducted with an eye toward promptly determining whether further investigation (either a preliminary inquiry or a full investigation) should be conducted.”¹¹⁹ And while the Guidelines did not specify methods approved for “checking of leads,” they could not rely on investigative tools reserved for use in investigations. But when conducting an “assessment” under the new Guidelines, the FBI may—in addition to combing through any and all publicly available information—use the following investigative techniques: (1) recruiting and tasking informants to attend meetings or events surreptitiously;¹²⁰ (2) questioning people or engaging them in conversation while misrepresenting the agent’s true identity (so-called “pretext” interviews);¹²¹ and (3) engaging in indefinite physical surveillance of homes, offices, and individuals.¹²² The existence of “assessments” thus increases significantly the intrusiveness of the FBI’s investigative authority.

Exacerbating the risks to privacy that assessments pose, the current Guidelines abandon many of the oversight provisions contained in prior iterations of the Guidelines. In fact, for assessments, the Guidelines require no supervisory approval, nor are there any reporting requirements.¹²³ The Guidelines do not require the FBI to monitor how often assessments are being undertaken, what their targets or purposes are, what techniques are used, or how frequently they reveal actual criminal activity. Nor do the Guidelines place any time limit on an assessment’s duration.

A lack of sufficient *ex ante* oversight is similarly evident in the provisions regarding preliminary and full investigations, referred to collectively in the new guidelines as “predicated investigations.”¹²⁴ The Guidelines require no initial authorization for predicated investigations unless they are foreign-intelligence-related, in which case a SAC or FBI Headquarters must authorize the investigation.¹²⁵ In fact, FBI Headquarters need not even be notified of a predicated investigation except under certain limited circumstances.¹²⁶ Preliminary investigations can last six months, and a SAC can extend that period for another six months; there is no durational limit on full investigations. The Guidelines rely instead on various post hoc audits to ensure compliance with the rules.¹²⁸ But as we have learned from the FBI’s misuse of National Security Letters (NSLs) and exigent letters (forms of administrative subpoena used to collect records about individuals or groups from third parties), even when post hoc audits successfully identify abuses, such audits alone do not provide sufficient deterrent value.¹²⁹

2. *The Domestic Investigative Operational Guidelines*

The Attorney General’s Guidelines are implemented by the “Domestic Investigative Operational Guidelines” (DIOG), promulgated by the FBI. After official requests by at least two organizations pursuant to the Freedom of Information Act,¹³⁰ the Justice Department publicly released—with significant redactions—the current DIOG. The DIOG purports to impose additional rules on FBI agents in their exercise of some of the authorities criticized above. To be sure, the Guidelines themselves do occasionally reference FBI policy as an additional limitation on FBI investigative authority,¹³¹ and the DIOG includes laudable hortatory language regarding the need to be solicitous of civil liberties; to refrain from infringing on First Amendment rights and from profiling on the basis of race, religion, ethnicity, or national origin; and to limit appropriately the scope and intrusiveness of FBI activity.¹³²

But the DIOG’s efforts to achieve these goals fall short in at least four respects. First, the DIOG makes only a half-hearted commitment to the requirement that agents use the least intrusive method that is likely to procure the needed information when conducting investigations.¹³³ Upon close inspection, the admonition to use the least intrusive method is less forceful than it appears.¹³⁴ When advising agents on how to determine which method is the “least intrusive method,” the DIOG institutes a balancing test. After determining the least intrusive method for a given situation, “reviewing and approving authorities should balance the level of intrusion against investigative requirements” to determine which technique actually to employ.¹³⁵

In other words, the least intrusive method should be employed *unless* the agent decides—despite having determined that a less intrusive method is likely to procure the needed information—that a more intrusive method should be used because of the seriousness of the crime or threat, the significance of the information to be gained, or other such factors. This balancing test renders the term “least intrusive method” a misnomer.

The DIOG includes laudable hortatory language regarding the need to be solicitous of civil liberties; to refrain from infringing on First Amendment rights and from profiling on the basis of race, religion, ethnicity, or national origin; and to limit appropriately the scope and intrusiveness of FBI activity. But the DIOG’s efforts to achieve these goals fall short.

Moreover, the final word on the FBI’s “least intrusive method” policy echoes the words of the Guidelines themselves: agents should use “any lawful method allowed, even if intrusive” when the agent determines such methods are warranted. This caveat sends an important message—minimal intrusiveness may be preferable, but is not actually required. Ultimately, as the Guidelines state and the DIOG echoes, “the choice of methods ... is a matter of judgment.”¹³⁶ Establishing such a loose and discretionary standard—and then presenting it as a “least intrusive method” requirement—provides an illusion of civil liberties protections with little substance behind it.

Second, the DIOG bars investigative activities “based solely on the exercise of First Amendment rights or on the race, ethnicity, national origin, or religion” of their subject.¹³⁷ The DIOG does not, however, preclude investigative activity based in part—or even primarily—on such factors. Notably, the Justice Department’s policy regarding the use of race by law enforcement officials prohibits employing “race or ethnicity *to any degree*” in making routine law enforcement decisions.¹³⁸ The DIOG thus appears to be in tension with existing DOJ policy on this point. Moreover, even the prohibition against basing investigations *solely* on protected characteristics is undermined by the DIOG’s instruction that such characteristics may permissibly be linked to terrorist or criminal behavior. For example,

if investigative experience and reliable intelligence reveal that members of a terrorist or criminal organization are known to commonly possess or exhibit a combination of religion-based characteristics or practices (e.g., group leaders state that acts of terrorism are based in religious doctrine), it is rational and lawful to consider such a combination in gathering intelligence about the group.¹³⁹

Similarly, the DIOG permits the collection of information regarding ethnic and racial behaviors “reasonably believed to be associated with a particular criminal or terrorist element of an ethnic community.”¹⁴⁰ The DIOG thus embraces the logical fallacy that if all members of a particular terrorist group share a certain characteristic (such as the Muslim faith), then anyone who shares that characteristic is a fair target of suspicion. On its face, this could mean collection of information on Muslim men who grow their beards or observe their religion in a particular fashion. No generic admonition to respect privacy and civil liberties can combat these permissive standards.

Also troubling is the DIOG’s embrace of community mapping—which involves collecting and storing information about particular communities. They “permit the FBI to identify locations of concentrated ethnic communities” as well as to collect “the locations of ethnic-oriented businesses and other facilities” (likely including religious facilities such as mosques) because “members of certain terrorist organizations live and operate primarily within a certain concentrated community of the same ethnicity.”¹⁴¹ This very same principle was proposed by local law enforcement authorities in Los Angeles but was ultimately scrapped when widespread and vocal protests from the Muslim and civil liberties communities equated the plan with racial profiling and noted that it was likely to alienate Muslim residents.¹⁴²

The DIOG seems to place great faith in the ability of the “authorized purpose” requirement¹⁴³ to keep investigative activities from wandering too far afield. But when the authorized purposes are as broad as they are—investigating violations of law or threats to national security, investigating the role of groups in violations of law or threats to national security, identifying potential targets of criminal activities or threats to national security, etc.—and when so much investigative activity may take place in the absence of any factual predicate, that requirement seems largely toothless.

Third, while the DIOG contains detailed rules regarding when, how, and under what circumstances the FBI may use each particular investigative method available to it,¹⁴⁵ the fact that these rules are set forth in the DIOG, rather than in the Attorney General’s Guidelines themselves, is problematic. The DIOG does usefully resurrect many of the procedural protections that had been stripped out of the Guidelines themselves. For example, they add supervisory approval requirements, both for particular investigative techniques and for certain types of investigations.¹⁴⁶ They place time limits on each investigative stage (except for full investigations). They require periodic file reviews for all assessments and investigations.¹⁴⁷ And they increase oversight for investigations into targets that raise “sensitive investigative matters,” which include investigations of politicians, political or religious organizations, or members of the news media.¹⁴⁸

Each of these provisions is a step in the right direction. But rather than forming part of the higher-profile, infrequently modified, and fully disclosed Guidelines themselves, they have been “downgraded” to the easier-to-change, less politically salient, and more secretive DIOG. If the DIOG reinstates so many of the procedural requirements that had been stripped out of the Guidelines, it begs the question why the location of these rules was moved. Moreover, while the DIOG seems to call for greater *internal* oversight than the Guidelines themselves require, neither set of rules provides for the *external* oversight—from Congress and from the public—necessary to ensure both that Americans’ civil liberties are safeguarded and that the Guidelines are effective.

Perhaps most troublingly, the rules regarding the most intrusive investigative techniques permitted in the absence of factual predicates for investigation—pretext interviews and undisclosed participation in religious and political gatherings—are redacted entirely (despite being labeled unclassified) from the publicly available DIOG. So whether the DIOG aims to mitigate any of the troubling aspects of these techniques is impossible to say. And if they do impose additional restrictions, the fact that they do so secretly limits their effectiveness as a constraint—if no one outside the Justice Department knows the rules to which agents are expected to adhere, enforcement of those rules becomes a matter of FBI grace.¹⁴⁹

II. THE NEW CHANGES SHOULD BE RECONSIDERED

The expansion of FBI powers contained in the 2008 Guidelines will have predictable consequences. Lessons of the FBI's history teach us that, in the absence of sufficient oversight and limitations on intelligence-collection activities, civil liberties will be trampled in our pursuit for security. This could happen in several areas. First, the ability to conduct "assessments" without any factual predicates is almost certain to lead to undue intrusions into the privacy of law-abiding Americans. Second, anecdotal evidence suggests that the Guidelines already have chilled First-Amendment-protected activity, and likely will continue to do so. Third, the burden of these civil liberties concerns likely will fall disproportionately on Muslims and persons of Arab or South Asian descent, as agents whose investigative decisions are unconstrained by objective factual criteria will be more likely to fall back on conscious or subconscious biases. This, in turn, will make the FBI less effective in countering the terrorist threat as targeted communities are alienated and rendered less willing to cooperate with law enforcement. Moreover, studies show that profiling is not an effective tool.

Finally, we cannot be sure that the FBI's newfound collection authority does, in fact, lead to increased security. As the *Washington Post's* recent series of reports on "Top Secret America" makes plain, the scope of America's surveillance-industrial complex is so massive, with so many agencies engaging in overlapping and redundant activities, it is impossible to determine the efficacy—from a security standpoint—of the billions of dollars we spend and the volumes of information the government collects.¹⁵⁰ Some even argue that this increased scope of collection will make us *less* safe, because the collection of vast amounts of information unrelated to factual indications of wrongdoing or threat could overwhelm the Bureau's ability to analyze effectively and employ the information it has collected.

In the face of these adverse effects, the executive branch has yet to articulate persuasively any countervailing operational considerations that would justify retaining the most recent changes to the Guidelines. Thus the powers they confer should be curtailed. In any event, the implementation of all investigative powers should be monitored closely and subjected to strict oversight for both compliance and effectiveness.

A. The Guidelines' Adverse Effects on Civil Liberties and Law Enforcement Effectiveness

On their face, and in light of the history of intelligence-collection in this country, the Mukasey Guidelines raise concerns that they might lead to significant imposition on Americans' civil liberties. In examining the varied ways in which this result might come to pass, the Guidelines' overbreadth becomes clear. Moreover, the need for vigilant, regular review of the FBI's authorities, as well as internal and external oversight mechanisms becomes all the more evident.

1. Threat of Privacy Invasions

The new Guidelines may pose significant threats to Americans' privacy. They permit the collection of vast amounts of information without any factual predicate and with no supervisory approval. Add to this expansive authority

the Guidelines' encouragement to agents to "take the initiative" and be proactive,¹⁵¹ and it seems likely that the FBI will be amassing substantial amounts of information on many Americans who have never been suspected of wrongdoing. The more the FBI sees itself as an intelligence-collection agency, the more robust these collection-without-suspicion activities are likely to be.

Such collection seems to be at the heart of the government's counterterrorism efforts, both inside and outside the FBI. It is important to note that the FBI Guidelines are just one small part of a broader surveillance scheme.¹⁵² Each element of this scheme is engaged in aggressive information-collection and analysis. An illustration comes from the National Security Agency (NSA), the agency primarily responsible for the collection and analysis of various forms of communication. The NSA is building vast new facilities to increase its information-storage capacities.¹⁵³ One facility, in Utah, measures one million square feet; another, in San Antonio, is roughly the size of the Alamodome.¹⁵⁴ The amount of data expected to reside in these facilities has been estimated in the Yottabytes (as an indication of the size of a Yottabyte, numbers beyond Yottabytes have not yet been named).¹⁵⁵

The fact that the FBI will likely be gathering information on law-abiding Americans is particularly troubling in light of the methods it is now authorized to use. Going to political meetings or religious services to collect information about what takes place there and who attends; pretending to be an investigative target's new neighbor or business associate, or stationing agents outside the target's home or office—even having them followed—so that their movements are tracked day and night; accessing without a court order telephone and e-mail subscriber information. These are highly intrusive and invasive techniques, and Americans have a right to expect that they will not be subject to such government intrusion unless the government has some objective reason to suspect illegal activity or wrongdoing.

The collection and analysis of information from existing sources—another technique that FBI agents can employ in the absence of a factual predicate—seems less troublesome at first blush. After all, why shouldn't the FBI be permitted to access information already in the government's possession, or information available on the internet? In fact, however, the sophisticated collection and analysis of such information by FBI is significantly more revealing than a simple Google search that a private individual might conduct. Through public, commercial, and government databases, the FBI can readily collect vast amounts of employment information, residential information, financial information, information about shopping habits, and the like. This information can then be subjected to algorithmic data-mining, stored, or disseminated to other government databases and agencies.

The threat here is far from theoretical. Like the NSA, the FBI's National Security Branch has amassed vast amounts of information in its Analysis Center (NSAC), which houses multiple databases "[c]omposed of government information, commercial databases and records acquired in criminal and terrorism probes."¹⁵⁶ The stored information includes international travel records of citizens and aliens, financial forms, hotel and rental car records, a log of all calls made by federal prison inmates, and a reverse White Pages with 696 million names and addresses tied to U.S. phone numbers.¹⁵⁷ The FBI plans to expand the data set to include yet more travel records, as well as tax records from non-profit organizations and multiple databases whose de-

scriptions are redacted in a now-available (though formerly classified) document.¹⁵⁸ Most Americans would agree that the FBI should not be permitted to compile a dossier on every American. But the accumulation of these databases into one facility means that such a dossier is just one mouse-click away. Accordingly, all collection and use of information—even publicly available information—must be effectively policed.

The prospect of expansive collection of information leads to another concern. Even if information the FBI collects at the assessment stage provides no basis for further investigation—indeed, even if it wholly exonerates a group or individual from suspicion—that information will remain in government databases indefinitely for analysis and dissemination to other agencies. According to the Guidelines, since investigative “activities also provide critical information needed for broader analytic and intelligence purposes to facilitate the solution and prevention of crime, protect the national security, and further foreign intelligence objectives,” all information collected “at all stages of investigative activity is ... to be retained and disseminated for these purposes ... regardless of whether it furthers investigative objectives in a narrower or more immediate sense.”¹⁵⁹ To this end, the Guidelines include broad information-sharing provisions.¹⁶⁰ While it is indisputable that the FBI should be permitted to share appropriate information with other government agencies as well as local law enforcement for legitimate law enforcement purposes, the prospect of keeping and sharing large amounts of information about Americans under no suspicion of wrongdoing raises serious privacy concerns.

While it is indisputable that the FBI should be permitted to share appropriate information with other government agencies as well as local law enforcement for legitimate law enforcement purposes, the prospect of keeping and sharing large amounts of information about Americans under no suspicion of wrongdoing raises serious privacy concerns.

These possible invasions of privacy raise concerns not only because of their infringement on Americans’ fundamental rights. They also breed cynicism, resentment, and distrust towards law enforcement and government officials. Revelations of unwarranted invasions of privacy raise the specter of historic, Hoover-era FBI excesses. To be sure, today’s FBI bears little resemblance to that unregulated agency shrouded in secrecy. But federal law enforcement agencies possess the authority and the technology to engage in invasions of privacy far beyond those that took place in the Hoover era. And even if such excesses are the exception rather than the rule today, concern over systemic abuse arises with each isolated instance of overreaching.

2. Chill to First-Amendment-Protected Activity

The FBI’s broad authorities also risk causing significant chill of First-Amendment-protected religious and political activity. As First Amendment expert Floyd Abrams noted with respect to the pre-Guidelines FBI’s impact on free speech, “[t]he ‘chill’ on speech was real; Hoover intended just that and achieved just that.”¹⁶¹

Under the Guidelines, agents are permitted to attend all gatherings, events, political rallies, and religious services open to the public. How will they decide which ones to attend? If history provides any lessons, such decisions

will often be based on some form of religious or political profiling. Certainly the Hoover-era operations were targeted at minorities and political dissidents, aiming to harass and disrupt their operations.¹⁶² But even in the post-Guidelines era, innocent political and religious groups have been targeted and investigated. Recall the 1980s investigation into CISPES, the activist organization opposed to Reagan-era El Salvador policy. The investigation, and others like it from that same era, gathered a wealth of information on activist groups, with investigations of particular groups sometimes triggered solely on ideological similarity or association with other groups already under investigation.¹⁶³ Investigators monitored meetings, rallies, demonstrations, religious services, and other protected activity.¹⁶⁴ But the CISPES investigation produced “no reliable information of planned violence or other illegal activity.”¹⁶⁵ Another example is the Cold-War-era Library Awareness Program, which consisted of regular FBI visits to public and university libraries to seek information about the readers of unclassified scientific and technical journals, sometimes asking “librarians to be wary of ‘foreigners’ or persons with ‘East European or Russian-sounding names.’”¹⁶⁶

In the post-9/11 context, one study catalogs the experiences of dozens of law-abiding members of the Muslim, Arab, and South Asian (MASA) communities upon returning to the United States from abroad. They have been subjected to intrusive questioning by customs agents about their religious practices, political views, and charitable giving, as well as searches of their laptops, cell phones, and digital cameras, pursuant to a policy that permits such questioning and searches absent any individualized suspicion of wrongdoing.¹⁶⁷ And FBI Director Robert Mueller ordered all FBI branch offices to count the number of mosques within their jurisdiction as a starting point for proactive investigation of potential terrorists.¹⁶⁸

Imagine an FBI agent attending a religious service in which the priest, reverend, rabbi, or imam engaged in stark anti-government rhetoric, criticizing American foreign policy in the Middle East and sympathizing with the desire of residents of Middle Eastern countries to expel nonviolently U.S. military forces. Such expression is at the very core of First Amendment protections—political speech neither intended nor likely to incite actual violence, yet adamantly critical of U.S. actions. Americans are entitled to voice these sorts of opinions, and they should not necessarily trigger FBI intelligence-gathering activities that ultimately are likely to chill such expression. Yet such rhetoric, if observed in a mosque, likely would draw additional government attention.

In fact, there are a range of First-Amendment-protected activities that agents can take into account during the assessment stage to build a profile of traits that, taken together, are deemed suspicious. According to the FBI itself, potential indicators of terrorist activity include taking notes, drawing diagrams, espousing unpopular views,¹⁶⁹ or taking photographs,¹⁷⁰ and other law enforcement organizations have expressed the view that increased religiosity is suspicious as well.¹⁷¹

The FBI’s aggressive investigation and infiltration of mosques has already had a profound chilling effect on the exercise of fundamental rights, particularly religious freedoms. According to the *New York Times*, some Muslims have “canceled trips abroad to avoid arousing suspicion. People are wary of whom they speak to. Community groups say it is harder to find volunteers. Many Muslim charities are hobbled.”¹⁷² In the Southern California

Muslim community, reports the *Los Angeles Times*, “some people are avoiding mosques, preferring to pray at home. Others are reducing donations to avoid attracting government attention. . . . And some mosques have asked speakers to refrain from political messages in their sermons.”¹⁷³ And while empirical evidence of such claims is hard to come by, “Muslim leaders report a reduction in attendance at mosques, a change in the language used at worship services, a decrease in contributions to Muslim charities, and an erosion of the trust and good will that are essential to the vitality of a religious community.”¹⁷⁴

When the FBI sends investigators to question people about their political activities, when it sends agents to attend religious gatherings, when it monitors the calling records of members of the media, it can create a profoundly chilling effect on First Amendment activities. The FBI can hardly pretend ignorance of this effect, given that the agency has, at various points in its history, infiltrated political or religious groups *with the express purpose* of creating a chilling effect on unpopular or anti-government expression.¹⁷⁵ To engage in activities likely to have such an effect, the Bureau should have to show that such an infringement is justified by a particular level of suspicion.

Even the power to gather extensive information from public sources can contribute to the threat of First Amendment chill. The FBI can compile publicly available information on religious or political figures, government critics, or members of the media. If it does so based on a distrust of groups or individuals that represent dissenting perspectives, that is just as problematic from a privacy and constitutional standpoint as if those same motivations led to information gathering from non-public sources. Collection and use of information on people’s First-Amendment-protected activities, even where those activities are carried out in the public eye, is simply not appropriate absent a legitimate law enforcement justification. The Guidelines need to exhibit sufficient solicitude for constitutionally protected activity.

3. Dangers of Profiling

Permitting investigations without factual predicate and with limited supervisory involvement is overwhelmingly likely to lead to profiling¹⁷⁶ on the basis of race, religion, ethnicity, national origin, or political belief. In the absence of constraints imposed by a standard such as reasonable suspicion or probable cause, FBI agents are now free, in many situations, to rely on their own discretion. As we have seen time and again, individuals permitted such discretion in making law enforcement decisions are influenced by their conscious or subconscious biases.¹⁷⁷ And this reliance on bias can lead to profiling. Historically, when law enforcement officials have been able to collect intelligence on groups and individuals suspected—without any objective basis—of harboring ill will toward the U.S., the burden of that investigative activity has fallen on groups that espouse disfavored ideologies, minorities, or others who are perceived as threatening.¹⁷⁸

Justice Department officials have assured both Congress and the public that “department rules . . . forbid predicated an investigation simply based on somebody’s race”¹⁷⁹ or “solely for the purpose of monitoring activities protected by the First Amendment.”¹⁸⁰ The question is not, however, whether investigative activity will be motivated by race, religion, national origin, or political belief *alone*. Problematic profiling consists not only of relying en-

tirely on characteristics like race or religion, but of taking them into account, in the absence of any particularized suspicion indicating that such characteristics are relevant, and making law enforcement decisions based even in part on such factors. Reliance on that criteria—that an officer has engaged in racial profiling only when the single factor, i.e., race, religion, ethnicity, etc., is used to make a law enforcement decision—comes close to defining the problem of our existence. It would not prohibit many inappropriate uses of these characteristics. For instance, it would not prohibit an officer from making decisions based on two factors, such as ethnicity and gender, like investigating males of Arab descent *because* they are males of Arab descent. Nor would it bar decisions based on the use of race and place, such as pulling over black drivers in white neighborhoods because they are blacks in white neighborhoods.

Any meaningful restriction on the use of race, religion, national origin, or political belief would allow such characteristics to be taken into account only when there is some indication that they are relevant to a particular description of someone or some group engaged in particular criminal activities.

Moreover, while Justice Department rules place some limits on the use of race only in traditional law enforcement activities, and they include an explicit exception for “law enforcement activities and other efforts to defend and safeguard against threats to national security.”¹⁸¹ Thus the new Guidelines do nothing to prevent allowing race to be considered as a factor in intelligence-collection activities, or in, for example, developing terrorist profiles.¹⁸²

The profiling risk that the Guidelines pose is not limited to the factors of race, religion, ethnicity, or national origin. They also threaten expressive activity.

Because the new Guidelines do not preclude the use of race or religion as a factor, profiling on the basis of “race plus” or “religion plus” the activities listed above can expose a large population of innocent people to the invasion of privacy that comes with being subjected to an FBI preliminary investigation. Indeed, as law enforcement officials told *The Associated Press*, “[a]mong the factors that could make someone the subject of an investigation is travel to regions of the world known for terrorist activity ... along with the

person’s race or ethnicity.”¹⁸³ Thus, for example, every individual of Pakistani origin who travels to Pakistan to visit family members is at risk of being subjected to an FBI investigation merely on that basis. So is every South Asian man who takes a photograph of the Brooklyn Bridge.

Indeed, the DIOG explicitly envisions community mapping based on ethnicity. Such activity is justified by the possibility that concentrations of certain ethnic communities provide an opportunity for “identified terrorist subjects from certain countries [to] relocate to blend in and avoid detection.”¹⁸⁴ In other words, ethnic profiling is already an express part of agency policy.

The profiling risk that the Guidelines pose is not limited to the factors of race, religion, ethnicity, or national origin. They also threaten expressive activity. Admittedly, the Guidelines preclude investigations *solely* for the purpose of monitoring activities protected by the First Amendment, and when investigations implicate First Amendment

rights, there are heightened notice and approval requirements.¹⁸⁵ But these minimal precautions are insufficient to negate the Guidelines' threat to expressive activity. After all, it is much easier to identify those who share the political beliefs or the religion of a particular group of terrorists than to identify and locate those actually plotting harm. It was thus the groups seen to espouse unpopular ideology who were the targets of FBI harassment and disruption during the Cold War. And, more recently, law enforcement officials have inappropriately surveilled, infiltrated, or collected information on anti-war protesters, anti-death penalty groups, and other political dissenters.¹⁸⁶

Despite the government's disavowal of Islam as the enemy, many of our post-9/11 counterterrorism efforts have focused on communities of people who happen to be Muslim, Arab, or South Asian. Many will argue that, because the terrorist threats with which we are most concerned emanate from those espousing an extremist misinterpretation of the Muslim faith, and because many of those hail from majority Arab or South Asian nations, counterterrorism efforts should focus on those groups or on those who come from countries with majority Muslim, Arab, or South Asian populations. But this means of "focusing" investigations is misplaced. To be sure, the threat posed by this sort of violent extremism is real, but in combating this threat we cannot indict the millions of law-abiding people who happen to be part of the communities from which the threat may emanate. In the past, law enforcement organizations have successfully policed groups engaged in organized violence—like the mafia or the KKK—without trenching on the civil liberties of the entire Italian-American or Southern Christian communities. They have also been able to focus on anti-abortion groups that sometimes resort to violence without infiltrating all Catholic and evangelical Christian churches, despite knowing that violent anti-abortion activists are often ideologically motivated. Of course the vast majority of Muslims are not terrorists. Consequently, any counterterrorism policy aimed at collecting information from within those communities, in the absence of a factual predicate indicating that criminal or espionage-related activity is ongoing, will be sweeping in massive amounts of information about law-abiding citizens.

There is general consensus that profiling is ineffective; nonetheless, law enforcement has engaged in several tactics targeted predominantly at the Muslim community as a whole, and with unfortunate effects. Indeed these many domestic anti-terror policies do not seem to have made us safer—in fact, the opposite might be true. In some cases, data collected under these programs remains unanalyzed, wasting countless man hours. In other cases, the policies have simply undermined the relationship between the Muslim community and law enforcement, alienating the very people whose cooperation is most essential to effective counterterror efforts.

Consider, for example, the many post-9/11 measures—some implemented by the FBI, others implemented by other government agencies—that were targeted directly at the whole Muslim community. In the days and months after the attack, thousands of individuals were subjected to interviews with the FBI.¹⁸⁷ While the interviews were labeled as "voluntary," they took place at the same time as widespread roundups and detentions of Muslim Middle Easterners. Interviewees therefore were likely to fear what might happen should they refuse to talk to government officials. Moreover, while the interviews did not directly concern immigration issues, an interviewee's immigration status also could render an invitation to participate in a voluntary interview much more coercive than the label "voluntary" might indicate.¹⁸⁸ All of these individuals were men hailing from countries with predominantly Muslim populations, even though they had no ties to terrorism and there was no basis to suspect such ties.¹⁸⁹

The government also established a mandatory registration program, the National Security Entry-Exit Registration System (NSEERS), which required men over the age of 16 from about 25 countries—countries that have predominantly Muslim populations or are located in the Middle East¹⁹⁰—to register with the federal government, be photographed and fingerprinted, and periodically re-register. And in 2004, Operation Front Line, an effort to disrupt potential plots surrounding the presidential election, saw immigration officials target more than 2,500 immigrants, 79% of whom were from Muslim-majority countries. These individuals were asked what they thought of America, whether violence was preached at their mosques, and whether they had access to biological or chemical weapons.¹⁹¹

And the Muslim Advocates' study of the border-crossing experiences of members of the MASA community revealed what seems to be a pattern of intrusive questioning by customs agents regarding individuals' religious practices, political views, and charitable giving, as well as searches of their electronic devices.¹⁹²

The Mukasey Guidelines and the accompanying DIOG both extend to the FBI even more investigative discretion than it enjoyed in the aftermath of 9/11 and seem to embrace certain forms of religion- or ethnicity-based decisionmaking. The likelihood of investigative activity focused disproportionately on discrete racial, ethnic, religious, or political groups—such as MASA communities or political dissenters—is significant.

The likelihood of a return on the investment of resources such a policy represents is low. At the same time, the costs it imposes are quite high.

Again the post-9/11 programs are illustrative. Two years after the FBI conducted its “voluntary” interview program, neither DOJ nor FBI had bothered to analyze the data collected in the interviews and had no plans to do so.¹⁹³ According to agents, the interviews were a waste of time and “produced exactly no useful information.”¹⁹⁴ In the two years after 9/11, the NSEERS program registered over 83,000 individuals, sought out 8,000 men of Arab and Muslim descent for FBI interviews, and placed more than 5,000 foreign nationals in preventive detention. Of those thousands of individuals, not one was convicted of a terrorist crime; the government discontinued the mandatory periodic re-registration element due to its inefficiency.¹⁹⁸ And the 2004 Operation Front Line effort to disrupt potential plots surrounding the presidential election failed to yield actionable information. None of those interrogated were charged with national security offenses; the offenses that were charged were largely immigration violations.¹⁹⁹ Together, these initiatives represented a massive investment of law enforcement resources in unpredicated investigative activities that yielded negligible security gain.

These failures should come as no surprise. Instrumental objections to racial profiling as a law enforcement strategy are legion and well-documented.²⁰⁰ And the Justice Department itself has acknowledged that racial profiling does not work.²⁰¹ There are, of course, extreme examples of failed efforts to use profiling as a law enforcement tool. For example, “the FBI sifted through customer data collected by San Francisco-area grocery stores in 2005 and 2006, hoping that sales records of Middle Eastern food would lead to Iranian terrorists.”²⁰² But there is general consensus among experts that even less extreme versions of racial, ethnic, or religious profiling are also ill-advised.

In fact, in the wake of 9/11, a group of senior U.S. intelligence specialists warned against using such profiling as a means of combating terrorism.²⁰³ One of them noted that “fundamentally, believing that you can achieve safety by looking at characteristics instead of behaviors is silly.”²⁰⁴

Even assuming that an accurate racial, ethnic, religious, or political profile could be generated for some crimes—a dubious proposition—aspiring criminals could simply adapt to the profile, exploiting it to evade detection. In the context of terrorism, would-be perpetrators anticipate and work around profiling practices, choosing “front men” who do not fit the profile. For example, the perpetrators of terrorist plots against Israeli air passengers have included, among others, a heavily pregnant Irishwoman (herself an unwitting courier), Japanese men, and a Nicaraguan.²⁰⁵ Similarly, suicide bomb plotters in Israel have adjusted to profiling by selecting women and children as bombers and by disguising bombers in secular or even Orthodox Jewish clothing.²⁰⁶ And FBI Director Mueller has recognized that “the threat from radicalization has evolved A number of [recent] disruptions occurred involving extremists from a diverse set of backgrounds, geographic locations, life experiences, and motivating factors.”²⁰⁷ In other words, there is no such thing as a terrorist “profile.”

The ineffectiveness of profiling as a law enforcement tactic (not to mention the constitutional problems it raises²⁰⁸) led the Justice Department to ban the use of race as a factor in determining whether and whom to investigate in the general criminal context. The Department’s prohibition, however, does not extend to other aspects of minority status, such as religion or political ideology; nor does it apply to “law enforcement activities and other efforts to defend and safeguard against threats to national security or the integrity of the Nation’s borders.”²⁰⁹ The national security exemption, in particular, is a puzzling one. While one might argue about whether national security justifies the individual indignities imposed by profiling, the Justice Department has never explained why national security justifies using a technique that the agency itself describes as ineffective. In any event, the new Guidelines, which cover criminal investigations as well as national security and domestic intelligence collection, leave the door to profiling wide open.

Reliance on racial, ethnic, religious, or political profiling is not only ineffective; it is also affirmatively counterproductive in several respects. First, profiling can waste resources²¹⁰ by allocating money and manpower inefficiently.²¹¹ Relatedly, when law enforcement officials focus on traits like race or religion, they are more likely to overlook signs that actually do indicate heightened likelihood of criminal intent.²¹² The shortcut that profiling may seem to provide is simply no substitute for the investigation of substantive leads indicating possible criminal or terrorist activity.

Profiling on the basis of race, religion, or ethnicity also harms counter-terrorism efforts by alienating MASA communities in the U.S. In discussing racial profiling of African Americans, the Justice Department has warned of “a strong connection between perceptions of race-based stops by police and animosity toward local and state law enforcement.” Such animosity, in turn, makes individuals less inclined to report crimes and suspicious activity; to answer police inquiries and testify as witnesses; to affirmatively come forward with evidence; and to serve as impartial, open-minded jurors.

The need for healthy police-community relations is especially strong in counterterrorism work. To foil potential attacks, law enforcement needs accurate tips. Such tips are most likely to come from “people who live in the communities where sleeper cells reside and can tell authorities who’s new in a neighborhood and who seems to have income without holding a job.”²¹⁴ A recent example comes from the case of five Washington, D.C.-area Muslim men arrested in Pakistan on suspicion of traveling there to join al Qaeda. It was the men’s families who alerted authorities when they became suspicious of their sons’ activities.²¹⁵ And the prosecutions of the so-called “Lackawanna Six” came only after “Lackawanna’s Yemeni community itself brought the men to the FBI’s attention.”²¹⁶ Successful counterterrorism policy thus requires forging a cooperative relationship with communities likely to learn of impending terrorist plots.²¹⁷ Such a cooperative relationship can exist only if there is confidence on the part of the relevant communities that the means of investigating, disrupting, and prosecuting terrorist activity are legitimate, without bias, and consistent with due process of law.²¹⁸

By broadly targeting the very people most likely to be able to help, however, the FBI destroys this confidence, sowing the seeds of distrust and contentiousness rather than cooperation and partnership.²¹⁹ Profiling thus interferes with law enforcement agents’ essential task of developing relationships with the communities they police.

Successful counterterrorism policy requires forging a cooperative relationship with communities likely to learn of impending terrorist plots. Such a cooperative relationship can exist only if there is confidence on the part of the relevant communities that the means of investigating, disrupting, and prosecuting terrorist activity are legitimate, without bias, and consistent with due process of law.

FBI Director Mueller denies that the new Guidelines have this effect, but there is significant evidence to the contrary. Distrust of law enforcement, along with the government’s practice of using preliminary interviews as a basis for later pressure to act as an informant or even as the basis for criminal charges, has led many community groups to “strongly urge individuals not to speak with law enforcement officials without the presence or advice of an attorney.”²²⁰ And the infiltration of mosques has caused increased tension nationwide between Muslim communities and law enforcement, leading several Muslim groups to threaten to suspend most contacts with the FBI over the issue.²²¹ Several recent investigations where informers have infiltrated mosques and promoted terror plots “have sown a corrosive fear” among many Muslims “that F.B.I. informers are everywhere, listening.”²²² And the use of informants in mosques in Southern

California has “frayed relations between the FBI and Muslims” to the point that one Muslim community leader observed that “people cannot be suspects and partners at the same time.”²²³ An empirical study of the Muslim-American community in New York indicates that the tendency to withdraw cooperation with law enforcement based on perceptions of profiling is not merely anecdotal but represents a community-wide trend.²²⁴ Perhaps it is no coincidence that the families who reported their suspicions regarding their missing sons hail from the jurisdiction of the FBI’s Washington field office, which has engaged in productive outreach to the local Muslim and Arab communities, meeting with leaders, fielding questions, and participating in community activities.²²⁵

So in the absence of sufficient oversight and accountability mechanisms in place to curtail inappropriate use of factors such as race, religion, national origin, or political opinion, investigators' efforts to detect terrorist plots could be less effective under the new Guidelines. Conversely, requiring more tailored collection of information based on factual predicates could increase the likelihood that the government will identify and obtain information that is actually effective in preventing terrorist activity.

Profiling has other negative effects as well. Religious or ethnic profiling imposes significant social burdens on the profiled community. It causes humiliation, feeds "social opprobrium that leads to hate crimes"²²⁶ and discrimination, and perpetuates racial inequality. It sends the message to minorities that they are viewed at all times as potential criminals; that they are not valued members of society; and that they cannot rely on the police for protection.²²⁷ This message risks breeding anger, cynicism, and lack of respect for government more generally.²²⁸ As one report put it, "[o]ver the long term, [racial profiling] leaves persons of color with a sense of powerlessness, hostility, and anger."²²⁹ Moreover, profiling that targets minorities exaggerates any differences that do exist between that community and the population at large. Significantly higher rates of minority interaction with law enforcement perpetuate and exacerbate inequality, negative stereotypes about minorities, and discrimination and violence based on these stereotypes.²³⁰ No community should be singled out and burdened with the consequences that flow from being treated as if its members are more likely to engage in criminal or terrorist activity.

4. *Risks of Excessive Collection*

Effective crime and terrorism prevention is not necessarily aided by the collection of *more* information; it is aided by the collection of more of the *right* information, and the tools to analyze that information effectively. If increased investigative discretion and the expansion of unfocused investigative activities results in crowding government databases with irrelevant information, it could render investigative efforts less effective.

Take the Guidelines' permissiveness regarding the collection of information at the assessment stage. Allowing the FBI to target for investigation people for whom there is no factual predicate of criminal activity or threatening behavior increases the amount of information, already vast, that the Bureau will collect. This, in turn, increases the raw material that analysts and agents must examine and analyze. According to FBI Director Mueller, "the FBI receives well over 100 different feeds of criminal and terrorist data from a variety of sources."²³¹ Consequently, "[i]t is a great challenge to ensure that intelligence analysts are able to efficiently understand and analyze the enormous volume of information they receive."²³² Yet a recent Inspector General report noted that the Bureau had failed to review "significant amounts" of wiretapped phone calls and intercepted emails, in part due to a lack of qualified translators.²³³ Even useful information can only further our security interests if we devote the time and resources to effective analysis—a task that increases in difficulty as the volume of information rises. Resources might be better allocated to more analysis capacity, rather than more (over)collection.

Note that high profile “intelligence failures” have, as a rule, resulted not from the lack of information, but from the inability to effectively process that information. Consider the recent Christmas Day bombing attempt aboard flight 253 from Amsterdam to Detroit. Government agencies were in possession of all of the pieces of information necessary to have detected and prevented the bombing plot.²³⁴ But intelligence agencies were unsuccessful in “connecting the dots” or in moving aggressively to identify the threat posed to the U.S. homeland by Al Qaeda in the Arabian Peninsula.²³⁵ Similarly, while some have cited the 9/11 attacks as a justification for expanding the executive’s information-gathering authorities, the failure of U.S. intelligence and law enforcement agencies to detect and prevent the 9/11 plot also resulted, in part, from their failure to examine or follow up on information that they had already collected.²³⁶

Another stark example of this phenomenon comes from across the Atlantic. A government report about the investigation into the British subway bombings of July 7, 2005, revealed that two of the attack’s perpetrators had been on law enforcement’s radar prior to the bombings.²³⁷ In fact, the mastermind of the plot, Mohammed Sidique Khan, had crossed paths with British law enforcement on multiple occasions dating back to 1993.²³⁸ Khan and a co-plotter, Shehzad Tanweer, had been identified as “desirable” targets of further investigation and had surfaced four times during an investigation into a plot to detonate fertilizer bombs in the U.K.²³⁹ But due to a lack of resources, the U.K. police never followed up on the men. In fact, “resources were so stretched agents could not even assess whether ‘desireable’ targets should be examined in more detail.”²⁴⁰ The lesson is clear: if limited investigative resources are diverted into massive, untargeted surveillance efforts—as appears to have been the case in Great Britain²⁴¹—fewer man hours are available to pursue leads turned up during other investigations or to analyze information already in the government’s possession.²⁴²

These examples illustrate that the FBI’s investment of time, energy, and resources might be more fruitfully spent on efforts to remedy the problems identified by the White House review of the Christmas Day incident—better coordination among elements of the intelligence community; improving information technology capabilities; and ensuring a comprehensive, functioning process for tracking terrorist threat reporting.²⁴³

B. Operational Considerations Do Not Justify the 2008 Changes

Given the possible harms associated with the authorities the Mukasey Guidelines bestow on the FBI, the onus should be on the Bureau to make a particularly strong case to justify such changes. After all, as the 9/11 Commission noted, “[t]he burden of proof for retaining a particular governmental power should be on the executive, to explain (a) that the power actually materially enhances security and (b) that there is adequate supervision of the executive’s use of the powers to ensure protection of civil liberties.”²⁴⁴ In the case of the Mukasey Guidelines, the executive has thus far failed to make either case. The Justice Department has offered several reasons that the Guidelines were changed, some of which contradict one another, and none of which is persuasive.

On the one hand, the Justice Department has downplayed the extent to which the Guidelines expand the FBI’s powers. Changes to the general crimes and criminal intelligence investigations sections have been described as merely the “eliminat[ion of] the artificial distinctions in the way surveillance may be conducted under different sets of guidelines.”²⁴⁵ FBI Director Mueller assured Congress that “the new guidelines are not designed to give the FBI any broad

new authorities. The guidelines remove the last vestige of the wall separating criminal and national security matters.”²⁴⁶ And in describing the Guidelines’ domestic-intelligence-collection provisions, former Attorney General Mukasey noted that “this authorization isn’t new; the FBI has long had the authority to collect intelligence in the United States.”²⁴⁷ Some government officials have even claimed that these Guidelines extend no new powers to the Bureau at all. In a media briefing, a senior DOJ official proclaimed that “[w]e’re not getting any new power. . . . There’s no new power there. . . . [T]his is not a new power that the FBI has been given . . . that we didn’t previously have.”²⁴⁸

At best, these claims fail to tell the whole story. Take, for example, the FBI’s position regarding the three most controversial tactics permitted under the Mukasey Guidelines’ “assessments.”²⁴⁹ The FBI has claimed that, under the pre-2008 Guidelines (i.e., the Ashcroft Guidelines), it could use pretext interviews, conduct physical surveillance, and task informants at the “assessment” level in the general crimes context but not in the national security context.²⁵⁰ The consequence, according to FBI officials, was that it could use these techniques to determine whether someone was selling drugs at a bar, but not whether someone was raising money for Hezbollah at this same bar.²⁵¹

But this claim mischaracterizes the Ashcroft Guidelines. There is no “assessment” level in those Guidelines. There are preliminary inquiries or full investigations, each of which requires some factual predicate.²⁵² And there is the “prompt and extremely limited checking out of initial leads,” which was the only level of activity that can take place in the absence of a predicate.²⁵³ It is possible that this “extremely limited” checking of leads *might* have been interpreted to permit the sort of techniques at issue here, if it were not for a second crucial fact about the Ashcroft Guidelines: They explicitly prohibited both pretext interviews and physical surveillance absent supervisory authorization at the preliminary inquiry stage.²⁵⁴ Thus the FBI claimed to have the power under the Ashcroft Guidelines at a non-existent “assessment” level to use tactics that actually required both supervisory approval and some information indicating the possibility of criminal activity. “Threat assessments” were permitted in the Ashcroft era under the 2003 National Security Investigation Guidelines, but by the FBI’s own admission, the techniques at issue here were prohibited in those assessments.²⁵⁵

Moreover, this first justification for amending the Guidelines—that they do not work any significant change in the FBI’s authorities—is belied by a second justification that these same government officials have offered for the changes: that the current Guidelines provide tools necessary to the FBI’s newly emphasized preventive role.²⁵⁶ If the Guidelines truly provide no new authorities to the FBI, how do they aid in prevention in ways that the Ashcroft Guidelines did not? Indeed, the Ashcroft Guidelines already emphasized prevention as a “central mission,” and included several provisions aimed at empowering and enabling this element of the FBI’s activities.²⁵⁷ In asserting that the Mukasey Guidelines are necessary for terrorism prevention, the Bureau makes no mention of how its activities were unacceptably constrained by the Ashcroft Guidelines, which were drafted for the same purpose and envision many of the same practices.

The FBI also argues that the Mukasey Guidelines are necessary to remedy the flaws in the FBI’s procedures that contributed to the failure to discover the 9/11 plot. In making this argument at a congressional hearing, FBI Director Mueller cited the now-well-known Phoenix Memo, a memo drafted by an FBI agent in Phoenix, Arizona, warning of risks posed by Middle Eastern men enrolling in flight training school.²⁵⁸ The memo, however, hardly illustrates a

lack of information-gathering capacity by the FBI. The memo was unsuccessful in preventing 9/11 not because it contained insufficient information, but because managers at FBI headquarters, the Osama Bin Ladin unit, and the New York field office failed to review or act on it prior to 9/11. Even if the memo had received more attention, there is of course no guarantee that the 9/11 plot would have been derailed. But the very existence of the memo shows that the FBI was entirely capable, even under the Reno-era Guidelines, of collecting the information necessary to safeguard against at least some terrorist attacks.

While multiple investigations into the causes of the 9/11 attacks identified flaws in the FBI's use and handling of intelligence leading up to 9/11,⁵⁹ none of those flaws was the result of overly restrictive FBI investigative Guidelines. The problem was not an inability to collect necessary information; it was a failure to effectively and efficiently manage, share, or analyze the information already collected. This problem might justify consolidating responsibilities for crime-prevention and intelligence-collection within the FBI, or encouraging increased coordination between the FBI and other government agencies. But it does not justify the expansion of investigative authority contained in the Mukasey Guidelines.

Another proffered justification for the Mukasey Guidelines is that a consolidation of multiple sets of Guidelines and a harmonization of their rules was necessary to resolve inconsistencies and to reduce confusion among agents.²⁶⁰ According to this argument, an investigation is an investigation, and the rules should not differ depending on whether the investigation is conducted in order to solve a crime or to gather intelligence.

But the Guidelines were developed to require different standards in different contexts for a reason. The purpose for which an investigation is initiated, the amount of evidence that the feared harm is imminent, the possible harm involved—all are arguably relevant to what sort of action the FBI should be permitted to take. In short, context matters. And a one-size-fits-all investigative approach, while appealing for its administrative simplicity, is not the way to pursue all of the FBI's many goals—solving crimes, preventing crimes, protecting civil liberties, collecting valuable foreign intelligence—most effectively.

Take, for example, the difference between investigations of general crimes and criminal-intelligence investigations. Investigations of general crimes tend to end with a decision to prosecute or not to prosecute. As the Guidelines historically have acknowledged, they are consequently more circumscribed in scope and tend to be shorter in duration than intelligence investigations.²⁶¹ In intelligence investigations of criminal organizations, by contrast,

the organization provides a life and continuity of operation that are not normally found in a regular criminal activity. As a consequence, these investigations may continue for several years. Furthermore, the focus of such investigations 'may be less precise than that directed against more conventional types of crime. . . . For this reason the investigation is broader and less discriminate than usual.'²⁶²

Exposing the ways in which a power is exercised provides a natural check on its abuse. This natural check exists in the criminal context in ways that it does not for intelligence investigations.

Accordingly, durational limits on general crimes investigations have been shorter than those for intelligence investigations.

Similarly, earlier iterations of the Guidelines precluded the use of preliminary inquiries in the criminal intelligence context, requiring evidence to reach the level of a “reasonable indication” of relevant activity before permitting the FBI to initiate investigative activity. This distinction is sensible when viewed

in context. General crimes investigations have a close nexus to the commission of a particular crime. Intelligence investigations, on the other hand, are more undefined; there is no specific crime “to provide a framework for the investigation,”²⁶³ which increases the risk that they will be undertaken without sufficient basis or will include information about law-abiding citizens.

Moreover, general crimes investigations are conducted with relative transparency, whereas intelligence investigations are, as a rule, conducted in secret. Exposing the ways in which a power is exercised provides a natural check on its abuse. This natural check exists in the criminal context in ways that it does not for intelligence investigations. Introducing evidence secured through a wiretap or a “sneak and peek” search in a criminal trial provides an opportunity for the validity of that wiretap and that search to be challenged by a criminal defendant. The target of a wiretap or a search in an intelligence investigation, on the other hand, may never even know about the investigation, much less have a chance to challenge its legitimacy.

Consider the 2004 incident in which an FBI Joint Terrorism Task Force requested grand jury subpoenas to be issued to Drake University and several anti-war protesters seeking records regarding the purpose of and attendance at an anti-war gathering that had taken place on the Drake campus.²⁶⁴ When news of the subpoena became public, the ensuing outrage prompted the subpoenas to be withdrawn.²⁶⁵ By contrast, when the government requests information as part of an intelligence investigation, through NSLs or so-called “business records” requests, “[n]o person shall disclose to any other person” the fact that the request was made.²⁶⁵ Only the recipient of such requests can challenge their legitimacy. Publicity can provide no check on misuse of the power. Notably, in each instance in which an NSL has been challenged, it has been withdrawn.²⁶⁷

Under the circumstances of intelligence investigations, keeping the FBI on a tighter rein, avoiding a free-ranging investigation before there is a reasonable indication of criminal activity, represents a logical precaution and reduces the risk that law-abiding Americans will be subject to undue intrusions into their privacy. As one intelligence expert put it, “[b]ecause the safeguards against overreaching or abuse are weaker in intelligence operations than they are in criminal investigations, powers granted for intelligence investigations should be no broader or more inclusive than is absolutely necessary” and they “should be accompanied by rigorous oversight by Congress, and where appropriate, by the courts.”²⁶⁸ The fact that a particular activity under a particular level of supervision is permitted in the criminal context is thus not necessarily justification for employing that same tactic in the intelligence-collection context.

Of course, some investigations might appropriately be labeled as falling under more than one investigative category. Investigations into an international terrorist organization's U.S. activities, for example, would qualify as a foreign intelligence, criminal intelligence, and general crimes investigation all at once. In such circumstances, the FBI should have the discretion and flexibility to employ the framework that most makes sense given the facts of the case. But the simple fact that some investigations might transcend an easy label is no reason to jettison merely for convenience's sake the rules that developed—for good reasons—to apply different standards in different contexts.

The alleged differences among various sets of guidelines have also been described as “problematic from a compliance standpoint.”²⁶⁹ In other words, rather than teach agents to operate in compliance with existing guidelines, the guidelines should be changed to make compliance easier.

It is certainly true that the FBI has a history of spotty compliance with the rules to which it is subjected. From the use of confidential informants to National Security Letters and beyond, the FBI has shown time and again that it struggles to comply with restrictions imposed upon it. A 2005 report by the Justice Department's Inspector General, for example, revealed that agents failed to secure the proper authorization for the use of confidential informants²⁷⁰ and the initiation or extension of investigations,²⁷¹ and failed to maintain the required documentation regarding agents' visits to public gatherings and events.²⁷² A 2007 internal review of the FBI's use of National Security Letters (NSLs) unearthed a host of problems, including erroneous reports to Congress regarding the use of NSLs,²⁷³ the fact that 22 of 77 files examined contained violations of the rules governing NSLs,²⁷⁴ and the fact that the FBI circumvented requirements of NSL authorities or issued NSLs in violation of FBI policy and the Attorney General's guidelines for FBI National Security Investigations.²⁷⁵ More recently, the Inspector General issued a scathing report documenting the FBI's systemic use of unlawful means of acquiring thousands of telephone records over the course of several years, as well as its “ineffective” post hoc efforts to justify this breach of law and policy.²⁷⁶ And a September 2010 report from the Inspector General, prompted by media reports suggesting that the FBI had targeted organizations for investigation on the basis of First-Amendment-protected activity found “troubling” results. While not motivated by groups' expressive activities, across a range of investigations, agents improperly collected and retained information; initiated investigations with insufficient justification; and labeled as “terrorism investigations”—thereby making available additional powers—matters having nothing to do with what most Americans would consider terrorism.²⁷⁷ On several occasions they also permitted investigations to continue far beyond the point at which they should have been closed, improperly keeping the targets of these investigations on watch lists, allowing the government to track their travel and investigate their associates, for years.²⁷⁸ And most recently, the Inspector General reported the agents cheated on the exam designed to test their knowledge of the rules by which they must comply.²⁷⁹

The solution to compliance problems, however, is not to eliminate the rules that are being broken. It is true that guidelines imposing minimal constraints are more likely to produce stellar compliance levels. But recall that in the pre-Guidelines era an unfettered, unconstrained FBI embarked on surveillance, intelligence, and investigative activities so objectionable that Congress nearly enacted statutory limits. It was these types of

abuses that the Guidelines were imposed to prevent, and it is the risk of these types of abuses that continues to demand meaningful Guidelines. Indeed, if the FBI can be expected to continue its tendency to operate beyond the scope of its authorities from time to time, all the more reason to tailor those authorities as narrowly as possible. The FBI's history of overreaching in the course of well-intentioned efforts to fight crime and protect national security argues for more robust constraints, not fewer. As one member of Congress put it when assured by FBI Director Mueller that the FBI would not abuse the authorities extended to it, "We understand your assurances. We've heard them before. And that is why we are skeptical."²⁸⁰

With regard to the specific complaint that different standards for different types of investigations causes confusion among agents, the response is simple: law enforcement officials operate under different standards depending on the investigative context in all manner of ways. They may make a felony arrest in a public place with no warrant, but they must secure a warrant to make an arrest inside a home.²⁸¹ When arresting the driver of a car, they may search the car's interior, but they may not search the trunk unless they have probable cause to do so.²⁸² Officers may enter a private home with no warrant when exigent circumstances require it, but not under normal circumstances.²⁸³ All of these rules—and many, many more imposed on the activities of law enforcement officers by statute or by the Constitution—obligate officers to learn the rules and apply them to different factual situations. If agents feel they need legal advice to execute this obligation, they should be encouraged or required to work in tandem with the appropriate U.S. Attorney's office, as they often do in run-of-the-mill criminal investigations. The existence of circumstance-based distinctions in the Guidelines for the FBI's investigative activity should not pose an insurmountable practical obstacle to effective law enforcement.

One reason offered by the former Attorney General for the changes in Guidelines is, however, spot-on. "These new guidelines," said Michael Mukasey, will "reflect that the FBI is an intelligence agency."²⁸⁴ In short, the FBI wants the authority—the freedom—to collect, at will, all available information, using an arsenal of highly intrusive investigative tools. In that regard, it seeks to eliminate any "distinction in the Bureau between law enforcement and intelligence."²⁸⁵ This authority may be sought for the most noble of purposes, to protect our Nation from threats to its security. But in granting this power without sufficient constraints on its use, we forget the lessons of history and expose ourselves to equally ominous threats: threats to our freedom, to our privacy, and to the values that make the Nation worth defending. This was the conclusion of the Church Committee faced with the Cold War's threat of nuclear holocaust in 1976. Our conclusion today, faced with the threat of extremist violence, should be no different.

III. RECOMMENDATIONS

The dearth of information available regarding the FBI’s implementation of the Guidelines and their effectiveness, the risks to civil liberties described in this report, and concerns regarding the stringency of FBI oversight call for some revisions. In order to know more about the use and efficacy of the Guidelines and to guard against the risks that they pose, the Attorney General and Congress, in consultation with other stakeholders,²⁸⁶ should consider two types of modifications to the Guidelines.

Oversight Recommendations

Both Congress and the Justice Department should act to ensure vigorous oversight of the Guidelines’ use. There must be meaningful internal and external checks on the vast powers the FBI have been granted. The following recommendations would accomplish this goal:

1. *Restore the requirements of prior approval for initiating, conducting, and continuing or extending investigations, as well as durational limits on investigations to the Guidelines.*
 - The FBI’s history proves that, even acting in good faith and with the best of intentions, FBI agents will not infrequently venture beyond the limits of their powers.
 - Since the Guidelines inception, they have relied on prior authorization requirements and durational limits to guard against the risk of improper use of investigations or investigative techniques. In jettisoning these safeguards, the 2008 Guidelines increase both the likelihood and frequency of violations.
2. *Require records of prior approval to be in writing and kept on record.*
 - A recordkeeping requirement both encourages better compliance with supervisory approval obligations and creates a data trail to facilitate internal and external reviews of the FBI’s use of its authorities.
3. *Implement a robust system of oversight and review of the Guidelines’ implementation and efficacy within the Justice Department.*
 - Under the Patriot Act reauthorizations in 2005, the Department of Justice Office of the Inspector General (OIG) is required to review “the effectiveness and use, including any improper or illegal use, of national security letters issued by the Department of Justice.”²⁸⁷
 - A similar requirement should be enacted for review of the Guidelines. The Department of Justice Inspector General—in consultation with the Privacy and Civil Liberties Oversight Board—should prepare and release annually a report about how the Guidelines are being used. The Inspector General must be given full access to all relevant information, as well as the authority to interview FBI officials.
 - Like the NSL audits, the report should include “an examination of the use” of the Guidelines; “a description of any noteworthy facts or circumstances, including any improper or illegal use” of Guidelines’ authorities; and “an examination of the effectiveness of the Guidelines,” including the importance of the information acquired, the manner such information is collected, retained,

analyzed, and disseminated, whether and how often the Department of Justice used such information either to produce an analytical intelligence product or in criminal proceedings, and how often each investigative technique was employed.²⁸⁸

- Note that OIG review of the FBI's use of NSLs has been extraordinarily effective in identifying violations and recommending means to avoid such violations in the future.
- A classified version of this report should be made available to all Members of Congress; a public version that provides aggregate numbers should also be released.

4. *Congressional Review.*

- Congress also should exercise vigorously its oversight authority to police the FBI's use of its authorities. Congress has multiple tools at its disposal to do so. It can hold oversight hearings—in fact, congressional committees regularly hold hearings related to oversight of the FBI. The use and effectiveness of the Guidelines should figure more prominently in those hearings, or separate hearings should be scheduled. Congress also could choose to task the General Accounting Office (GAO) with responsibility for conducting audits of the FBI's use of the Guidelines. While the GAO has statutory authority to access data, documents, and personnel, the FBI is not always entirely cooperative.²⁸⁹ FBI officials must insist that employees cooperate fully with any congressional or GAO reviews.

Substantive Recommendations

Regardless of what additional procedural protections are implemented, some elements of the FBI's existing powers simply permit too much government intrusion into the lives of innocent Americans and therefore should be curtailed in the following ways:

1. *Prohibit the FBI from using highly intrusive investigative techniques unless there is some basis in fact to suspect wrongdoing.*²⁹⁰

- This would prohibit tailing someone, posing as other people in order to mine information from neighbors and acquaintances, and recruiting informants to glean more information in the absence of some factual basis for suspicion.
- This prohibition, summarily overturned by the 2008 Guidelines, was enshrined in all previous iterations of the Guidelines for decades. It is the single most important safeguard against profiling and other forms of abuse, and the government has offered no persuasive justification for its sudden disappearance.

2. *Require agents to use the least intrusive investigative technique that is likely to prove effective.*

- The “least intrusive method” requirement has been part of the Guidelines since their inception. The current, equivocal language on this requirement in the Guidelines and the DIOG should be amended to stress its importance, even in terrorism investigations.

3. *Prohibit improper consideration of race, religion, ethnicity, national origin, or First-Amendment-protected activity in investigative decisions.*

- Addressing this issue is most urgent in the context of rules regarding use of informants to collect information about First-Amendment-protected activity, such as infiltration of a place of worship or political gathering. Such activities should require higher levels of predication and more aggressive oversight of investigative decisions than activities that do not implicate Americans' constitutional rights.
- Even outside the First Amendment context, however, reform is necessary. One standard to consider was recently implemented by the Office of the Director of National Intelligence (DNI). The standard for use in the DNI's Information Sharing Environment (ISE)-Suspicious Activity Reporting (SAR) system adopts a "behavior-focused approach to identifying suspicious activity" based on the standard announced in *Terry v. Ohio*,²⁹¹ 392 U.S. 1 (1968). It requires that "race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion (except if used as part of a specific suspect description)."²⁹² This type of limitation on the use of these factors to justify law enforcement activity is crucial.

CONCLUSION

The time to act is now—before the Guidelines result in widespread and unwarranted intrusions into Americans' privacy, harmful religious and ethnic profiling, and the divergence of scarce resources to ineffective and indiscriminate collection of information.

The changes recommended above will go a long way to reduce the risk of excesses that the current Guidelines permit. They would reinvigorate the substantive standards on which investigative activity should be predicated and would ensure that intrusive investigative methods are used only when necessary. And they would impose internal and external checks to guarantee the lawful, effective use of the powers conferred on federal agents. In short, they would safeguard Americans' rights of privacy, free expression, association, and religion as well as help to focus investigative activity where there are indications of threats. The result will be a safer, more just America.

ENDNOTES

- ¹ See generally GEOFFREY R. STONE, *PERILOUS TIMES: FREE SPEECH IN WARTIME* (2004).
- ² MICHAEL B. MUKASEY, U.S. DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS § II(B)(4)(a)(i) [hereinafter "Mukasey Guidelines"], available at <http://www.justice.gov/ag/read-ingroom/guidelines.pdf>.
- ³ President Barack Obama, Remarks by the President on a New Beginning at Cairo University (June 4, 2009) ("America is not—and never will be—at war with Islam.") (transcript available at http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-at-Cairo-University-6-04-09/); President George W. Bush, Remarks at the United Nations General Assembly (Sept. 19, 2006) ("Extremists [in the Middle East] spread propaganda claiming that the West is engaged in a war against Islam. This propaganda is false We respect Islam.") (transcript available at <http://www.un.org/webcast/ga/61/pdfs/usa-e.pdf>).
- ⁴ John O. Brennan, National Security Advisor for Counterterrorism, Remarks at the Center for Strategic and International Studies (May 26, 2010); RICK "OZZIE" NELSON & BEN BODURIAN, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES, *A GROWING TERRORIST THREAT?: ASSESSING "HOMEGROWN" EXTREMISM IN THE UNITED STATES* vi (2010); STAFF OF S. COMM. ON HOMELAND SEC. AND GOVERNMENTAL AFFAIRS, 110TH CONG., REP. ON VIOLENT ISLAMIST EXTREMISM, THE INTERNET, AND THE HOMEGROWN TERRORIST THREAT 4 (2008).
- ⁵ E.g., Michelle Shephard, *Terror Analysis: The Danger of Dismissing the Absurd*, THE STAR, Aug. 27, 2010 (quoting a scholar specializing in the psychology of radicalization as saying that "much of what seems to radicalize is the perception of a war against Islam"), available at <http://thestar.com/news/canada/article/853336--terror-analysis-the-danger-of-dismissing-the-absurd>.
- ⁶ Jonathan Weisman, *Protests, Rhetoric Feed Jihadists' Fire*, WALL ST. J., Aug. 23, 2010, at A4 (noting that private security consultant believes that jihadists use anti-Muslim rhetoric in the US to "make the case that the U.S. is indeed at war with Islam"); NELSON & BEN BODURIAN, *supra* note 4, at vi.
- ⁷ Weisman, *supra* note 6; Dina Temple-Raston, *Rancor Over Mosque Could Fuel Islamic Extremists*, NPR, Aug. 24, 2010 (quoting American suspected terrorist leader Anwar Al-Awlaki asking potential recruits in the U.S. how they can have loyalty to a U.S. government "that is leading the war against Islam and Muslims"), available at <http://www.npr.org/templates/story/story.php?storyId=129387963&ft=1&f=129387963>.
- ⁸ See *supra* notes 4-7; David Nakamura & Javed Hamdard, *Petraeus condemns Fla. church's plan to burn Korans*, WASH. POST, Sept. 7, 2010 (warning that Americans burning Korans could "'endanger troops' and damage the U.S. war effort in Afghanistan"); Marc Sageman & Richard A. Clarke, *A Strategy for Fighting International Islamist Terrorists*, 618 ANNALS AM. ACAD. POL. & SOC. SCI. 223, 224 (2008); *Hearing on Terrorist Use of the Internet for Strategic Communications before the H. Permanent Select Comm. on Intel.* 110th Cong., 6 (written statement of Bruce Hoffman).
- ⁹ U.S. DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, *A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS* 257-72 (2010).
- ¹⁰ *Id.* at 276-79.

¹¹ *Id.* at 279-85.

¹² *Id.* at 70.

¹³ Fusion Centers were designed to improve the sharing of anti-terrorism intelligence among different state, local and federal law enforcement agencies. But from their inception, the threat Fusion Centers pose to civil liberties has been apparent. An ACLU report warned that they are characterized by ambiguous lines of authority, excessive secrecy, troubling private-sector and military participation, and a bent toward suspicionless information collection and data-mining. MIKE GERMAN & JAY STANLEY, *WHAT'S WRONG WITH FUSION CENTERS?* 3, 5 (2007). Since that report was published, “news accounts have reported overzealous intelligence gathering, the expansion of uncontrolled access to data on innocent people, hostility to open government laws, abusive entanglements between security agencies and the private sector, and lax protections for personally identifiable information.” MIKE GERMAN & JAY STANLEY, *FUSION CENTER UPDATE 1* (2008).

¹⁴ Press Release, ACLU, Fusion Center Encourages Improper Investigations of Lobbying Groups and Anti-war Activists (Feb. 25, 2009), *available at* <http://www.aclu.org/technology-and-liberty-/fusion-center-encourages-improper-investigatins-lobbying-groups-and-anti-war>.

¹⁵ Teresa Watanabe & Scott Glover, *Man Says He Was Informant for FBI in Orange County*, L.A. TIMES, Feb. 26, 2009, at B1, *available at* <http://articles.latimes.com/2009/feb/26/local/me-informant26>.

¹⁶ U.S. Dep’t of Justice, FBI, Memorandum regarding International Terrorism Matters (May 23, 2001); U.S. Dep’t of Justice, FBI, Memorandum regarding History/Background of the Environmental Rights Movement (Aug. 29, 2005); Press Release, Documents Obtained by ACLU Expose FBI and Police Targeting of Political Groups (May 18, 2005).

¹⁷ U.S. Dep’t of Justice, FBI, Memorandum regarding International Terrorism Matters (Feb. 26, 2003).

¹⁸ U.S. DEP’T OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, *A REVIEW OF THE FBI’S INVESTIGATION OF CERTAIN DOMESTIC ADVOCACY GROUPS* 188 (2010); *see also id.* at 186-88.

¹⁹ Already the seeds of distrust sown by the FBI in the American Muslim community have grown into obstacles to fruitful investigation. *See infra* notes 213-225 and accompanying text.

²⁰ RICHARD THORNBURGH, U.S. DEP’T OF JUSTICE, *THE ATTORNEY GENERAL’S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND DOMESTIC SECURITY/TERRORISM INVESTIGATIONS* § III (1989) [hereinafter “Thornburgh Guidelines”], *available at* <http://www.justice.gov/ag/readingroom/generalcrimea.htm>.

²¹ Mukasey Guidelines, *supra* note 2, at Intro, A.3.

²² WILLIAM FRENCH SMITH, U.S. DEP’T OF JUSTICE, *THE ATTORNEY GENERAL’S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND DOMESTIC SECURITY/TERRORISM INVESTIGATIONS* § III (1983) [hereinafter “Smith Guidelines”].

²³ Thornburgh Guidelines, *supra* note 20, § III.

²⁴ *Id.*

²⁵ Instead, there are individual statutory provisions that authorize certain activities by the FBI. Specifically, statutory provisions authorize the FBI to detect and prosecute offenses against the United States; to assist in the protection of the President; to investigate matters under the control of the Departments of Justice and State; to collect crime records and to provide training for state and local law enforcement; and to carry firearms, serve warrants, and make arrests. Don Edwards, *Reordering the Priorities of the FBI in Light of the End of the Cold War*, 65 ST. JOHN'S L. REV. 59, 67 & nn.31-33 (1991) (identifying and citing relevant statutory provisions).

²⁶ See, e.g., U.S. CONST. amend. IV; 50 U.S.C. §§ 2510-2520; 50 U.S.C. §§ 1801-1818. It should be noted that, like the Guidelines themselves, the statutory limits on FBI investigative activities also have been relaxed significantly since 9/11 by statutes such as the USA PATRIOT Act of 2001, Pub. L. No. 107-56, and the Foreign Intelligence Surveillance Act Amendments Act of 2008, Pub. L. No. 110-261.

²⁷ Memo from Charles Doyle, Senior Specialist, American Law Division, CRS, to Senate Select Committee on Intelligence 4 (Sept. 22, 2008) (on file with the Brennan Center) [hereinafter "CRS Memo"] (citing *Final Report of the Senate Select Comm. to Study Government Operations: Intelligence Activities and the Rights of Americans, Book II*, S. REP. NO. 94-755, at 10-1 (1976) [hereinafter "Church Comm. Report"]; see also ELMER STAATS, U.S. COMPTROLLER GEN., GENERAL ACCOUNTING OFFICE, FBI DOMESTIC INTELLIGENCE OPERATIONS—THEIR PURPOSE AND SCOPE: ISSUES THAT NEED TO BE RESOLVED, at 198-99 (1976), available at <http://archive.gao.gov/f0202/093784.pdf> ("Some methods used to accomplish the objective were summarized in a Department of Justice press release of November 18, 1974 . . . as: 1. Sending anonymous or fictitious materials to groups of members. 2. Disseminating public information to media sources. 3. Leaking informant-based or nonpublic information in media sources to expose the nature, aims, and membership of the various groups. 4. Advising local, State, and Federal authorities of civil and criminal violations by group members. 5. Using informants to disrupt a group's activities by causing dissension or exploiting disputes. 6. Informing employees, credit bureaus, and creditors of member's activities, to adversely affect subjects' credit standings or employment status. 7 Informing businesses and persons with whom members had economic dealings of members' activities, to adversely affect their economic interests. 8. Interviewing members to let them know that the FBI was aware of their activities and to develop them as informants. 9. Attempting to use religious and civil rights leaders and organizations in disruptive activities. 10. Acting in the political or judicial processes, usually involving release of FBI file information. 11. Establishing sham organizations for disruptive purposes. 12. Informing subjects' families or others of radical or immoral activity.").

²⁸ FBI History, FBI, <http://www.fbi.gov/libref/historic/history/text.htm> (last visited Oct. 5, 2010). The Bureau of Investigation primarily investigated violations of laws involving national banking, bankruptcy, naturalization, antitrust, peonage, land fraud, and the Mann Act. *Id.*

²⁹ *Id.*; FREDERICK A.O. SCHWARZ JR. & AZIZ HUQ, UNCHECKED & UNBALANCED: PRESIDENTIAL POWER IN A TIME OF TERROR 15 (2007).

³⁰ Edwards, *supra* note 25, at 67.

³¹ *Id.* at 68.

³² CRS memo, *supra* note 27, at 2.

³³ Edwards, *supra* note 25, at 68; CRS memo, *supra* note 27, at 3 (describing investigations into the KKK and racketeering enterprises as well as the establishment of FBI lists, such as the Communist Index, the Rabble-Rouser Index, and others).

- ³⁴ See generally Church Comm. Report, Books II & III, *supra* note 27.
- ³⁵ Church Comm. Report, Book III, *supra* note 27, at 1.
- ³⁶ See generally Church Comm. Report, Book III, *supra* note 27.
- ³⁷ See *id.*
- ³⁸ SCHWARZ & HUQ, *supra* note 29, at 27.
- ³⁹ E.g., Church Comm. Report, Book VI, *supra* note 27, at 5 (statement of Frederick A.O. Schwarz Jr.) (describing the tendency of intelligence investigations, once started, to “go on and on like a river without stop, and without regard to whether or not information has been collected which is of any use” in detecting wrongdoing); SCHWARZ & HUQ, *supra* note 29, at 31-32 (describing widespread long-term investigations of civil rights and women’s rights groups and leaders, despite a lack of evidence suggesting that their purposes and activities were anything but lawful).
- ⁴⁰ CRS memo, *supra* note 27, at 4.
- ⁴¹ Church Comm. Report, Book III, *supra* note 27, at 79-183; see also Tom Lininger, *Sects, Lies, and Videotape: The Surveillance and Infiltration of Religious Groups*, 89 IOWA L REV. 1201, 1211-1212 (2004) (describing FBI’s investigation of King); SCHWARZ & HUQ, *supra* note 29, at 22-23, 34-35 (same).
- ⁴² U.S. DEPT. OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, THE FEDERAL BUREAU OF INVESTIGATION’S COMPLIANCE WITH THE ATTORNEY GENERAL’S INVESTIGATIVE GUIDELINES 35 (2005) [hereinafter “AGG Compliance Report”].
- ⁴³ *Id.* at 35 (quoting *Legislative Charter for the FBI, Hearings Before the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary*, 96th Cong. 3 (1980) (Statement of Benjamin R. Civiletti, U.S. Att’y Gen.)).
- ⁴⁴ E.g., *FBI Oversight: Hearings Before the Subcomm. on Civil and Constitutional Rights of the House. Comm. on the Judiciary*, 94th Cong., 263 (1976).
- ⁴⁵ The Guidelines, officially entitled Domestic Security Investigation Guidelines, “were intended, in part, to diminish the perceived need for legislation to regulate and restrict the FBI’s use of informants.” *United States v. Salemme*, 91 F. Supp. 2d 141, 190-91 (D. Mass. 1999).
- ⁴⁶ AGG Compliance Report, *supra* note 42, at 36 (quoting Edward H. Levi, U.S. Att’y Gen.).
- ⁴⁷ *FBI Oversight: Hearings Before the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary*, 94th Cong., 261 (1976) (testimony of Att’y Gen Levi).
- ⁴⁸ Editorial, *Some Guidelines for the F.B.I.*, WASH. POST., Jan. 15, 1985, at A16.
- ⁴⁹ This set of guidelines was officially entitled the “Domestic Security Investigation Guidelines.”
- ⁵⁰ DOMESTIC SECURITY INVESTIGATION GUIDELINES, § I.A (Mar. 10, 1976) (hereinafter “Levi Guidelines”).

⁵¹ EDWARD H. LEVI, U.S. DEP'T OF JUSTICE, DOMESTIC SECURITY INVESTIGATION GUIDELINES § I.A (1976) [hereinafter "Levi Guidelines"].

⁵² *Id.*

⁵³ *Id.* § II.I. Levi also issued guidelines placing restrictions on the use of informants, which were revised by Attorney General Civiletti because of concerns over the conduct of some informants, FBI agents' knowledge of those activities, and promises of immunity for informants. AGG Compliance Report, *supra* note 42, at 39-46.

⁵⁴ Levi Guidelines, *supra* note 51, § II.E.

⁵⁵ *Id.*

⁵⁶ *Id.* § II.G.

⁵⁷ *Id.*

⁵⁸ *Id.* § II.H.

⁵⁹ *Id.* § II.F.

⁶⁰ *Id.* § II.I.

⁶¹ *Id.* § IV.A.

⁶² *Id.* § II.J; CRS memo, *supra* note 27, at 6.

⁶³ *See, e.g.*, AGG Compliance Report, *supra* note 42, at 3-4. In auditing the FBI's implementation of its authority to visit public places and attend public events to detect or prevent terrorist activities in the absence of any particularized evidence, the Inspector General found that the FBI failed to maintain records regarding the use of and compliance with this authority consistently. It went on to note that "[w]ithout access to data reflecting approval or documentation of such visits, we were unable to draw conclusions about the FBI's utilization of these authorities or its record of compliance with [them]." *Id.*

⁶⁴ Levi Guidelines, *supra* note 51, § II.B.

⁶⁵ *Id.* § II.D.

⁶⁶ *Id.* § II.I(4).

⁶⁷ Athan G. Theoharis, *FBI Surveillance: Past and Present*, 69 CORNELL L. REV. 883, 889 (1983).

⁶⁸ Mukasey Guidelines, *supra* note 2, § VII.S.2.

⁶⁹ AGG Compliance Report, *supra* note 42, at 59 ("Attorneys General and FBI leadership have uniformly agreed that the Attorney General Guidelines are necessary and desirable, and they have referred to the FBI's adherence to the Guidelines as the reason why the FBI should not be subjected to a general legislative charter or to statutory control over the exercise of some of its most intrusive authorities.").

⁷⁰ *Id.* at 36.

⁷¹ CRS memo, *supra* note 27, at 7.

⁷² Officially entitled “Attorney General’s Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations,” the Smith Guidelines expanded the domestic security investigations portion of the guidelines to apply explicitly to terrorism investigations.

⁷³ *See generally* Smith Guidelines, *supra* note 22.

⁷⁴ There were also guidelines governing the use of confidential informants, *see* AGG Compliance Report, *supra* note 42, at 63-136, as well as undercover operations, *see* AGG Compliance Report, *supra* note 42, at 137-68.

⁷⁵ Edwards, *supra* note 25, at 73-74.

⁷⁶ *Id.* at 73.

⁷⁷ *Id.* at 78-79.

⁷⁸ Levi Guidelines, *supra* note 50, § I.

⁷⁹ BENJAMIN R. CIVILETTI, U.S. DEP’T OF JUSTICE, THE ATTORNEY GENERAL’S GUIDELINES ON CRIMINAL INVESTIGATIONS OF INDIVIDUALS AND ORGANIZATIONS Intro (1980) [hereinafter “Civiletti Guidelines”]; Smith Guidelines, *supra* note 22, at Intro.

⁸⁰ Smith Guidelines, *supra* note 22, § III.B.3.

⁸¹ Racketeering enterprise investigations had been limited to cases involving violence, extortion, and public corruption, and did not include international terrorism enterprises; these restrictions were removed. *Compare* Thornburgh Guidelines, *supra* note 20, § III.A., III.B with JOHN ASHCROFT, U.S. DEPT’ OF JUSTICE, THE ATTORNEY GENERAL’S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND TERRORISM ENTERPRISE INVESTIGATIONS § III.A.2.a (2002) [hereinafter “Ashcroft Guidelines”], *available* at <http://www.fas.org/irp/agency/doj/fbi/generalcrimes2.pdf>; *see* CRS memo, *supra* note 27, at 14.

⁸² AGG Compliance Report, *supra* note 42, at 56.

⁸³ Dan Egan & Bob Woodward, *F.B.I. Probe of Al Qaeda Implies Wide Presence*, WASH. POST, Dec. 30, 2001, at A1; Robert M. Chesney, *The Sleeper Scenario: Terrorism-Support Laws and the Demands of Prevention*, 42 HARV. J. ON LEGIS. 1, 27-28 (2005); Lininger, *supra* note 41, at 1228.

⁸⁴ Ashcroft Guidelines *supra* note 81, § VI.

⁸⁵ Robert M. Chesney, *Civil Liberties ad the Terrorism Prevention Paradigm: The Guilt by Association Critique*, 101 MICH. L. REV. 1408, 1425 (2003) (quoting Attorney General Ashcroft).

⁸⁶ CRS memo, *supra* note 27, at 21.

⁸⁷ *Id.*

- ⁸⁸ Levi Guidelines, *supra* note 50, § II.I.
- ⁸⁹ Ashcroft Guidelines, *supra* note 81, at Intro. B.
- ⁹⁰ Levi Guidelines, *supra* note 50, § I.A.
- ⁹¹ Ashcroft Guidelines, *supra* note 81, at Intro. A. Previous guidelines also reference the “prompt and extremely limited checking out of initial leads,” *e.g.*, Civiletti Guidelines, *supra* note 79, § I.D, Smith Guidelines, *supra* note 22, § II.B, but they do not list them as a separate level of investigative activity the way the Ashcroft Guidelines do. Notably, under the Ashcroft Guidelines, the Justice Department’s Inspector General found that the FBI field offices in New York and Los Angeles had issued grand jury subpoenas without opening an investigation—a clear violation of the limits imposed by the guidelines. U.S. DEP’T OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, THE FEDERAL BUREAU OF INVESTIGATION’S TERRORIST THREAT AND SUSPICIOUS INCIDENT TRACKING SYSTEM viii-ix (2008).
- ⁹² Until the Ashcroft Guidelines in 2002, the Guidelines instructed that, as a general matter, inquiries and investigations should “be conducted with as little intrusion into the privacy of individuals as the needs of the situation permit.” CRS memo, *supra* note 27, at 13 (quoting Thornburgh Guidelines, § I). Similarly, with respect to general crimes, they provided that “[w]here a technique is highly intrusive, a supervisory agent shall approve its use in the inquiry stage only in compelling circumstances and when other investigative means are not likely to be successful.” *Id.* (quoting Thornburgh Guidelines, § II.B.); *see also* Gayle Horn, *Online Searches and Offline Challenges: The Chilling Effect, Anonymity, and the New FBI Guidelines*, 60 N.Y.U. ANN. SURV. AM. L. 735, 741 (2005).
- ⁹³ Ashcroft Guidelines, *supra* note 81, § I.
- ⁹⁴ *Id.* § IV.A.
- ⁹⁵ Smith Guidelines, *supra* note 22, § II.B.; *see also* Mitchell S. Rubin, *The FBI and Dissidents: A First Amendment Analysis of Attorney General Smith’s 1983 FBI Guidelines on Domestic Security Investigations*, 27 ARIZ. L. REV. 453, 454 (1985).
- ⁹⁶ Rubin, *supra* note 95, at 455.
- ⁹⁷ Ashcroft Guidelines, *supra* note 81, § I (“There is no separate provision for preliminary inquiries under the Criminal Intelligence Guidelines . . . because preliminary inquiries . . . may be carried out not only to determine whether the grounds exist to commence a general crimes investigation . . . but alternatively or in addition to determine whether the grounds exist to commence a racketeering enterprise investigation or terrorism enterprise investigation.”). Both the racketeering and terrorism portions of the Ashcroft Guidelines specify that information leading to a criminal intelligence investigation can come from a preliminary inquiry. *Id.* § III.A.2.b & III.B.1.b. AGG Compliance Report, *supra* note 42, at 171.
- ⁹⁸ *Id.* § II.B.
- ⁹⁹ *See id.* § VI.A. & B.
- ¹⁰⁰ *Id.*
- ¹⁰¹ U.S. DEP’T OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION’S USE OF NATIONAL SECURITY LETTERS 17 (2007).

- ¹⁰² Foreign Intelligence Surveillance Act Amendments Act of 2008, Pub. L. No. 110-261 (codified at 50 U.S.C. §§ 1881(d)(1)(A), 1881(a)(g)(4)).
- ¹⁰³ USA PATRIOT Act of 2001, Pub. L. No. 107-56 (codified as amended in scattered sections of U.S.C.) (amending requirements for accessing financial records, telephone service records, consumer reporting records).
- ¹⁰⁴ Levi Guidelines, *supra* note 50, §§ II.H., II.I. The Civiletti Guidelines applied similar restrictions to general crimes and racketeering investigations. For general crimes, a preliminary investigation could last only 60 days, and full investigations had to be approved by an FBI supervisor. Racketeering investigations were limited to cases involving violence, extortion, or public corruption unless the FBI Director and Attorney General approved. Civiletti Guidelines, *supra* note 79, § II.B. The Director or a designated Assistant Director could authorize racketeering enterprise investigations for 180 days, with the possibility of 180 day renewals. Civiletti Guidelines, *supra* note 79, § II.E.
- ¹⁰⁵ Levi Guidelines, *supra* note 50, § IV.A.
- ¹⁰⁶ Ashcroft Guidelines *supra* note 81, § II.B.3.
- ¹⁰⁷ *Id.* § III.A(5)(c), III.B.4.b.
- ¹⁰⁸ *Id.* § III.A(5)(a), III.B.4.a.
- ¹⁰⁹ Letter from Sens. Russell Feingold, Edward Kennedy, and Richard Durbin to Att’y Gen. Michael Mukasey (Aug. 20, 2008), *available at* <http://feingold.senate.gov/releases/08/08/20080820.html>.
- ¹¹⁰ Mukasey Guidelines, *supra* note 2, § I.D.1. They also incorporate rules formerly contained in the Supplemental Guidelines for Collection, Retention, and Dissemination of Foreign Intelligence; the Guidelines for Reporting and Use of Information concerning Violation of Law and Authorization for Participating in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence, or International Terrorism Intelligence Investigations; and the Guidelines for Reporting on Civil Disorders and Demonstrations Involving a Federal Interest.
- ¹¹¹ Mukasey Guidelines, *supra* note 2, at Intro. B.
- ¹¹² *Id.* § IV.
- ¹¹³ *Id.* § VI.
- ¹¹⁴ *Id.*
- ¹¹⁵ We have seen ample evidence of the FBI overstepping even quite permissive boundaries in its counterterrorism efforts. *See infra* notes 273-276 and accompanying text.
- ¹¹⁶ Mukasey Guidelines, *supra* note 2, § II.B.4.a.i.
- ¹¹⁷ *Id.* § II.B.4.

¹¹⁸ *Id.* § II.

¹¹⁹ Ashcroft Guidelines, *supra* note 81, at Intro. A.

¹²⁰ Mukasey Guidelines, *supra* note 2, § II.A.4.e.

¹²¹ *Id.* § II.A.4.f.

¹²² *Id.* § II.A.4.h.

¹²³ *Id.* § II. The Guidelines note that “the conduct of assessments is subject to any supervisory approval requirements prescribed by FBI policy.” *Id.* But there is no indication of what the FBI policy is, and the Guidelines themselves have no approval requirements.

¹²⁴ *Id.* § II.B. This name highlights the non-predicated nature of the “assessments.”

¹²⁵ *Id.* § II.B.2. As in the case of assessments, the Guidelines note that “the initiation of a predicated investigation requires supervisory approval at a level or levels specified by FBI policy.” *Id.* But, once again, there is no indication of what the FBI policy is, and the Guidelines themselves have no approval requirements.

¹²⁶ *Id.* § II.B.5. Sensitive investigative matters—investigation of a United States person, full investigations to obtain foreign intelligence, and enterprise investigations—require notification.

¹²⁷ *Id.* § II.B.4.a.ii.

¹²⁸ U.S. Dept. of Justice, Briefing with Department Officials on Consolidated Attorney General Guidelines (Sept. 12, 2008) (“The primary means of oversight are very intensive on-site audits of all national security and foreign intelligence cases. . . . We have eliminated certain reporting requirements and certain notice requirements.”) (statement of Senior Justice Department Official), *available at* <http://www.justice.gov/opa/pr/2008/September/08-opa-814.html>.

¹²⁹ See *infra* notes 273-275 and accompanying text.

¹³⁰ Both Muslim Advocates and the Electronic Frontier Foundation filed FOIA requests to obtain the DIOG, and filed suit after the FBI failed to produce them. *Muslim Advocates v. U.S. Dep’t of Justice*, No. 09-1754 (D.D.C. filed Sept. 16, 2009); *Electronic Frontier Foundation v. U.S. Dep’t of Justice*, No. 09-1151 (D.D.C. filed June 24, 2009). After the complaints were filed, the Justice Department released a heavily redacted version of the DIOG. Muslim Advocates has appealed pursuant to FOIA, seeking an entirely unredacted copy of the document. FOIA Appeal Letter from Brenda Abdelall to Melanie Ann Pustay, Director, Office of Information and Privacy, U.S. Dep’t of Justice (May 15, 2009), *available at* http://www.muslimadvocates.org/documents/FOIA_MA_%2005-15-09.pdf.

¹³¹ *E.g.*, Mukasey Guidelines, *supra* note 2, § II.A.2; *Oversight of the Federal Bureau of Investigation: Hearing Before the Senate Judiciary Comm.*, 110th Cong. (Sept. 17, 2008) (FBI Director Mueller describing FBI policies that implement the Guidelines’ “framework” and supplement their provisions).

¹³² U.S. DEP’T OF JUSTICE, FBI, DOMESTIC INVESTIGATIVE OPERATIONAL GUIDELINES, § 3 [hereinafter “DIOG”] (requires FBI activity to “[e]nsure that civil liberties and privacy are protected,” “[c]onduct no investigative activity solely on the basis of activities that are protected by the First Amendment or solely on the basis of

the race, ethnicity, national origin, or religion of the subject”); *id.* at § 4 (“Because our ability to achieve our mission requires that we have the trust and confidence of the American public, and because that trust and confidence can be significantly shaken by our failure to respect the limits of our power, special care must be taken by all employees to comply with these limitations.”).

¹³³ *E.g., id.* § 5.8(B).

¹³⁴ *Id.* § 4.4.

¹³⁵ *Id.* § 4.4(D).

¹³⁶ Mukasey Guidelines, *supra* note 2, § I.C(2)(a); DIOG, *supra* note 132, § 4.4(E).

¹³⁷ *E.g.,* DIOG, *supra* note 132, §§ 3, 5.1.

¹³⁸ U.S. DEP’T OF JUSTICE, CIVIL RIGHTS DIVISION, GUIDANCE REGARDING THE USE OF RACE BY FEDERAL LAW ENFORCEMENT AGENCIES (2003) [hereinafter “Justice Department Guidance on Use of Race”] (emphasis added).

¹³⁹ DIOG, *supra* note 132, § 4.2(B).

¹⁴⁰ *Id.* § 4.3(D).

¹⁴¹ *Id.* § 4.3(C).

¹⁴² Richard Winton, Jean-Paul Renaud, & Paul Pringle, *LAPD To Build Data on Muslim Areas*, L.A. TIMES, Nov. 9, 2007, at A1; Richard Winton & Teresa Watanabe, *LAPD’s Muslim Mapping Plan Killed*, L.A. TIMES, Nov. 15, 2007, at A1; *see also* Letter to Commander Michael P. Downing, Counter-Terrorism/Criminal Intelligence Bureau, Los Angeles Police Department from Ranjana Natarajan & Peter Bibring, Staff Attorneys, ACLU of Southern California, Farhana Y. Khera, Muslim Advocates, Shakeel Syed, Islamic Shura Council, Hussam Ayloush, Council on American Islamic Relations (Nov. 8, 2007), *available at* http://www.aclu-sc.org/attach/m/muslim_mapping_letter.pdf (expressing “grave concerns” about the LAPD’s community-mapping plans).

¹⁴³ *E.g.,* DIOG, *supra* note 132, §§ 4.2, 5.3, 5.4, 6.3, 7.6.

¹⁴⁴ *Id.* § 5.4.

¹⁴⁵ *Id.* §§ 5.8, 11.

¹⁴⁶ *Id.* §§ 5, 6, 7, 11.

¹⁴⁷ *Id.* §§ 5, 6, 7.

¹⁴⁸ *Id.* § 10.

¹⁴⁹ The FBI likely would argue that shielding its investigative techniques from public scrutiny is necessary to prevent from evading detection the potential criminals and terrorists that investigations are meant to thwart. And in the context of particular investigations, this concern is a significant one. With respect to cloaking

entire policies in secrecy, however, this justification rings hollow. Simply publishing the conditions under which an FBI agent is permitted to attend religious gatherings and what sort of information she is permitted to collect there will not tip off anyone that an agent plans to visit a certain place of worship at a certain time in order to discover whether anyone is advocating use of violence there. Just as the rules regarding the permissible use of electronic surveillance are published in the U.S. Code, the rules regarding other investigative techniques should be subject to public scrutiny.

¹⁵⁰ Dana Priest and William M. Arkin, *Top Secret America, A Hidden World, Growing Beyond Control*, WASH. POST, July 19, 2010, at A1.

¹⁵¹ Mukasey Guidelines, *supra* note 2, § II.

¹⁵² This scheme is made up of statutes, regulations, and programs throughout multiple government agencies. *See, e.g.*, USA PATRIOT Act of 2001, Pub. L. No. 107-56; Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511; Foreign Intelligence Surveillance Act of 1978 Amendments Act, Pub. L. No. 110-261(2008).

¹⁵³ James Bamford, *Who's in Big Brother's Database?*, 56 NEW YORK REV. OF BOOKS 17 (2009).

¹⁵⁴ *Id.*

¹⁵⁵ *Id.*

¹⁵⁶ Ryan Singel, *Newly Declassified Files Detail Massive FBI Data-Mining Project*, WIRED, Sept. 23, 2009, *available at* <http://www.wired.com/threatlevel/2009/09/fbi-nsac/>.

¹⁵⁷ *Id.*

¹⁵⁸ U.S. DEP'T OF JUSTICE, FBI, THE NATIONAL SECURITY ANALYSIS CENTER, AN ELEMENT OF THE FBI'S NATIONAL SECURITY BRANCH (2006) *available at* http://www.wired.com/images_blogs/threatlevel/2009/09/nsac_data_sets.pdf.

¹⁵⁹ Mukasey Guidelines, *supra* note 2, § II.

¹⁶⁰ *Id.* § VI.B, VI.C, VI.D.

¹⁶¹ Floyd Abrams, *The First Amendment and the War Against Terrorism*, 5 U. PA. J. CONST. L 1, 6 (2002).

¹⁶² SCHWARZ & HUQ, *supra* note 29, at 31-36 (describing the Church Committee's findings regarding the FBI's politically motivated investigations into organizations such as the NAACP, the Socialist Workers Party, the Women's Liberation Movement, and members of the media).

¹⁶³ Edwards, *supra* note 25, at 73.

¹⁶⁴ *Id.* at 72-78.

¹⁶⁵ *Id.* at 73.

¹⁶⁶ *Id.* at 78-79.

- ¹⁶⁷ MUSLIM ADVOCATES, UNREASONABLE INTRUSIONS: INVESTIGATING THE POLITICS, FAITH & FINANCES OF AMERICANS RETURNING HOME 6-7 (2009), *available at*, http://www.muslimadvocates.org/documents/Unreasonable_Intrusions_2009.pdf; *see also* Press Release, Council on American-Islamic Relations, CAIR-WA Meets with DHS, CBP On Border Profiling (Aug. 20, 2009) [hereinafter CAIR-WA 2009 Press Release].
- ¹⁶⁸ Eric Lichtblau, *F.B.I. Tells Offices to Count Local Muslims and Mosques*, N.Y. TIMES, Jan. 27, 2003, at A13; Curt Anderson, *F.B.I. Calls its Mosque Survey Part of Broad Security Plan*, L.A. TIMES, Jan. 29, 2003, at A16. This measure was later justified as necessary to prevent hate crimes. Larry Witham, *F.B.I. Defends Inclusion of Mosques in Crime Survey*, WASH. TIMES, Feb. 7, 2003, at A12.
- ¹⁶⁹ U.S. DEPT. OF JUSTICE, FINDINGS AND RECOMMENDATIONS OF THE SUSPICIOUS ACTIVITY REPORT (SAR) SUPPORT AND IMPLEMENTATION PROJECT Appx. B (2008). In response to criticisms from civil libertarians, the FBI revised its definition of “suspicious activity” to include only “observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.” MARK A. RANDOL, CONGRESSIONAL RESEARCH SERVICE, TERRORISM INFORMATION SHARING AND THE NATIONWIDE SUSPICIOUS ACTIVITY REPORT INITIATIVE: BACKGROUND AND ISSUES FOR CONGRESS 10 (2009).
- ¹⁷⁰ Press Release, FBI, Connecting the Dots Using New Technology (Sept. 12, 2008) (FBI press release using taking pictures of the Brooklyn Bridge as an example of possibly threatening behavior).
- ¹⁷¹ *See* MITCHELL D. SILBER & ARVIN BHATT, NEW YORK POLICE DEPARTMENT, RADICALIZATION IN THE WEST: THE HOMEGROWN THREAT 6-7 (2007); MUSLIM AMERICAN CIVIL LIBERTIES COALITION, COUNTERTERRORISM POLICY, MACLC’S CRITIQUE OF THE NYPD’S REPORT ON HOMEGROWN RADICALISM 6-7 (2008).
- ¹⁷² Paul Vitello & Kirk Semple, *Muslims Say F.B.I. Tactics Sow Anger and Fear*, N.Y. TIMES, Dec. 18, 2009, at A1.
- ¹⁷³ Teresa Watanabe & Paloma Esquivel, *OC Muslims say FBI Surveillance has a chilling effect*, L.A. TIMES, Mar. 1, 2009; *see also id.* (“Some average Muslims interested only in praying are avoiding mosques for fear of somehow being monitored or profiled.”).
- ¹⁷⁴ Lininger, *supra* note 41, at 1233-34 (citations omitted); *see also International Religious Freedom Report, Hearings Before the Subcomm. on Int’l Operations, House Int’l Relations Comm.*, 108th Cong. 67 (2002) (statement of Nihad Awad, Executive Director of Council on American-Islamic Relations) (at least three Muslim charities “have been effectively shut down”). These impediments to charitable giving infringe on religious freedom by interfering with Muslims’ ability to practice the duty of zakat (alms giving), a pillar of Islam. *Id.* at 67-68. Also troubling from a First Amendment perspective is the revelation from the Justice Department’s Office of the Inspector General that, in the course of three media leak investigations, the FBI improperly accessed the phone records and other calling activity of two reporters. U.S. DEPT. OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, A REVIEW OF THE FBI’S USE OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS 89 (2010). We cannot know how widespread such policy violations are, but it raises concerns.
- ¹⁷⁵ *Id.* at 1235-36; *see supra* Part I.A.
- ¹⁷⁶ Throughout this report, the word “profiling” refers to the practice of making law enforcement decisions—including who to target for investigation—on the basis of a particular characteristic, such as race, religion, ethnicity, national origin, or political belief, that has nothing to do with an increased likelihood of criminal activity, espionage, or threat to national security.

- ¹⁷⁷ See L. Song Richardson, *Arrest Efficiency and the Fourth Amendment*, __ MINN. L. REV. __ (forthcoming), at *12-20, available at <http://ssrn.com/abstract=1625755>; see also, e.g., Jerry Kang, Mahzarin R. Banaji, *Fair Measures: A Behavioral Realist Revision of "Affirmative Action"*, 94 CALIF. L. REV. 1063, 1073 (2006) (“[R]esearchers] found that implicit biases correlate with real-world behaviors like being friendly toward a target, allocating resource to minority organizations, and evaluating job candidates.”); Anthony G. Greenwald & Linda Hamilton Krieger, *Implicit Bias: Scientific Foundations*, 94 CALIF. L. REV. 945, 946 (2006) (“[T]he science of implicit cognition suggests that actors do not always have conscious, intentional control over the processes of social perception, impression formation, and judgment that motivate their actions.”); Alafair S. Burke, *Improving Prosecutorial Decision Making: Some Lessons of Cognitive Science*, 47 WM. & MARY L. REV. 1587 (2006) (discussing how different varieties of cognitive bias lead to irrational actions in discretionary prosecutorial decision-making); Chris Guthrie, Jeffrey J. Rachlinski, & Andrew J. Wistrich, *Inside the Judicial Mind*, 86 CORNELL L. REV. 777 (2001) (reporting study that showed evidence of cognitive bias in judicial decision-making); see also Burke, *supra*, at 1593-1601 (summarizing empirical literature about cognitive bias); Lininger, *supra* note 41, at 1210 (“[H]istory demonstrates that when investigative guidelines do not demarcate clear boundaries, law enforcement officials sometime employ highly intrusive techniques in investigating religious groups.”).
- ¹⁷⁸ As the Supreme Court has noted, protections against intrusive surveillance “become all the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs.” *United States v. United States District Court*, 407 U.S. 297, 319-20 (1972).
- ¹⁷⁹ Michael Mukasey, U.S. Att’y Gen., Address to the Oregon Anti-Terrorism Conference and Training (Aug. 13, 2008), available at <http://www.justice.gov/archive/ag/speeches/2008/ag-speech-0808133.html>.
- ¹⁸⁰ Mukasey Guidelines, *supra* note 2, § I.C.3.
- ¹⁸¹ Justice Department Guidance on Use of Race, *supra* note 138.
- ¹⁸² Lara Jakes Jordan, *Race Profiling Eyed for Terror Probes*, USA TODAY, July 2, 2008, http://www.usatoday.com/news/topstories/2008-07-02-926742133_x.htm.
- ¹⁸³ Jordan, *supra* note 182.
- ¹⁸⁴ DIOG, *supra* note 132, § 4.3.C.
- ¹⁸⁵ E.g., Mukasey Guidelines, *supra* note 2, § II.B.5.a.
- ¹⁸⁶ See *supra* notes 13-15 and accompanying text.
- ¹⁸⁷ David A. Harris, *The War on Terror, Local Police, and Immigration Enforcement: A Curious Tale of Police Power in Post-9/11 America*, 38 RUTGERS L. J. 1, 16 (2006).
- ¹⁸⁸ *Id.*
- ¹⁸⁹ *Id.*
- ¹⁹⁰ *U.S. to End Registration Program*, WASH. POST, Dec. 2, 2003, at A11.
- ¹⁹¹ Eric Lichtblau, *Inquiry Targeted 2,000 Foreign Muslims in 2004*, N.Y. TIMES, Oct. 31, 2008, at A17.

- ¹⁹² MUSLIM ADVOCATES, UNREASONABLE INTRUSIONS: INVESTIGATING THE POLITICS, FAITH & FINANCES OF AMERICANS RETURNING HOME 6-7 (2009), *available at*, http://www.muslimadvocates.org/documents/Unreasonable_Intrusions_2009.pdf; *see also* CAIR-WA 2009 Press Release, *supra* note .
- ¹⁹³ David Harris, *Law Enforcement and Intelligence Gathering in Muslim and Immigrant Communities After 9/11*, 34 N.Y.U. REV. L. & SOC. CHANGE 123, 135 n.43 (2010); *see also* Lininger, *supra* note 41, at 1253 (noting that interviews and registration programs were a waste of resources).
- ¹⁹⁴ Lininger, *supra* note 41, at 1253, n.247.
- ¹⁹⁵ Dan Eggen, *U.S. Set to Revise How it Tracks Some Visitors*, WASH. POST, Nov. 21, 2003, at A1.
- ¹⁹⁶ DAVID COLE & JULES LOBEL, LESS SAFE, LESS FREE: WHY AMERICAN IS LOSING THE WAR ON TERROR 107 (2008).
- ¹⁹⁷ *Id.*
- ¹⁹⁸ *U.S. to End Registration Program*, *supra* note 190.
- ¹⁹⁹ Lichtblau, *supra* note 191.
- ²⁰⁰ *See infra* notes 205-218 and accompanying text for a critique of profiling as a law enforcement technique.
- ²⁰¹ Justice Department Race Guidelines, *supra* note 138 (“Racial profiling in law enforcement is not merely wrong, but also ineffective.”); *see also* *Oversight of the Federal Bureau of Investigation: Hearing Before the S. Judiciary Comm.*, 110th Cong. 22 (2008) (testimony of FBI Director Mueller) (agreeing that “it would be ineffective and counterproductive for the FBI to engage in racial profiling”).
- ²⁰² Jeff Stein, *FBI Hoped to Follow Falafel Train to Iranian Terrorists Here*, CONG. Q., Nov. 2, 2007. To its credit, the FBI did not allow this activity to continue for long. “It was torpedoed by the head of the FBI’s criminal investigations division, Michael A. Mason, who argued that putting somebody on a terrorist list for what they ate was ridiculous—and possibly illegal.” *Id.*
- ²⁰³ Bill Dedman, *Memo Warns Against Use of Profiling as Defense*, BOSTON GLOBE, Oct. 12, 2001, at A27.
- ²⁰⁴ *Id.*
- ²⁰⁵ Kim Zetter, *Why Racial Profiling Doesn’t Work*, SALON, Aug. 22, 2005, *available at* http://dir.salon.com/story/news/feature/2005/08/22/racial_profiling/index.html (last visited Oct. 6, 2010); K. Jack Riley & Greg Ridgeway, *Racial Profiling Won’t Stop Terror*, WASH. POST, Oct. 11, 2006, *available at* <http://www.rand.org/commentary/2006/10/11/WP.html>.
- ²⁰⁶ Jonathan B. Tucker, *Strategies for Countering Terrorism: Lessons from the Israeli Experience*, U.S. Dep’t. of Homeland Sec., *Journal of Homeland Security*, Mar. 1, 2003, *available at* <http://www.homelandsecurity.org/journal/Articles/tucker-israel.html>.
- ²⁰⁷ Peter Finn, *Al-Qaeda Likely to Try Small-scale Attacks on U.S., Officials Say*, WASH. POST, Sept. 23, 2010, at A9.

- ²⁰⁸ Attorney General Ashcroft proclaimed that “racial profiling is an unconstitutional deprivation of equal protection under our Constitution.” Thomas B. Edsall, *Black Caucus, Ashcroft Have Tense Meeting; Attorney General Cites ‘Candid Exchange’ and Stresses Agreement on Profiling*, WASH. POST, Mar. 1, 2001, at A6.
- ²⁰⁹ Justice Department Race Guidelines, *supra* note 138.
- ²¹⁰ See Edwards, *supra* note 25, at 61 (describing FBI’s admission regarding Cold War investigation that became wasteful); see also Lininger, *supra* note 41, at 1253 (“A strategy of targeting all Muslims simply because they share the same faith as the 9/11 hijackers makes as much sense as targeting all Catholics in organized crime investigations because the Gambino family is Catholic.”).
- ²¹¹ Lininger, *supra* note 41, at 1254-55 (resources and personnel allocated to counterterrorism threat posed by Muslims risks missing the next Timothy McVeigh or Unabomber).
- ²¹² Bruce Hoffman, *Defending America Against Suicide Terrorism*, in RAND CORPORATION, THREE YEARS AFTER: NEXT STEPS IN THE WAR ON TERROR 21 (2004).
- ²¹³ DEBORAH RAMIREZ, JACK MCDEVITT & AMY FARRELL, U.S. DEPT. OF JUSTICE, A RESOURCE GUIDE ON RACIAL PROFILING DATA COLLECTION SYSTEMS: PROMISING PRACTICES AND LESSONS LEARNED 4 (2000) (citing survey data); see also Tom R. Tyler & Cheryl J. Wakslak, *Profiling and Police Legitimacy: Procedural Justice, Attributions of Motive, and Acceptance of Police Authority*, 42 CRIMINOLOGY 253, 259, 261-62 (2004) (empirical studies found that “the authority of the policy is weakened” and support for police within the community reduced when people perceive them to be profiling); William Lyons, *Partnerships, Information and Public Safety*, 25 POLICING 530, 536 (2002) (noting that racial profiling is counterproductive because it makes it “more difficult for citizens in those communities with the information we seek to communicate effectively crime- or terror-related information, and thereby discourage[s] their willingness to work with the police”).
- ²¹⁴ Zetter, *supra* note 205; see also Tom R. Tyler & Jeffrey Fagan, *Legitimacy and Cooperation: Why Do People Help the Police Fight Crime in Their Communities?*, 6 OHIO ST. J. CRIM. L. 231, 262 (2008) (“The work of the authorities is more difficult, and is sometimes impossible, without the active cooperation of the people in the community.”).
- ²¹⁵ Jerry Markon, *FBI Walks Tightrope in Outreach to Muslims, Fighting Terrorism*, WASH. POST, Dec. 20, 2009, at A5.
- ²¹⁶ Harris, *supra* note 193, at 127-28. The Lackawanna case is not alone in this respect. *Id.* at 13 (noting a case in Toledo, Ohio in which the Muslim community played a role in providing information to the FBI).
- ²¹⁷ *Id.* at 13-14; Harris, *supra* note 187, at 46; *id.* at 47 (quoting former National Counterterrorism Coordinator for the National Security Counsel Richard A. Clarke); Lininger, *supra* note 41, at 1255; Lynn Bernabei & David Cole, Op-Ed, *Stereotyping Hurts the War; Little Cooperation in Finger-Pointing*, WASH. TIMES, Nov. 24, 2003, at A23; Lyons, *supra* note 213, at 537-39; see also Letter from Sens. Richard J. Durbin, Edward M. Kennedy, and Russell D. Feingold, to Michael Mukasey, Attorney General, Sept. 23, 2008 (“We are concerned that issuing new Attorney General Guidelines without a more transparent process will actually make the FBI’s job more, not less, difficult by exacerbating mistrust in communities whose cooperation the FBI needs.”); Peter Clarke, Speech at The Courts and Terrorism: Transatlantic Observations, Apr. 15, 2009 (“[I]t is far more difficult to carry out surveillance operations or deploy undercover officers, or even visibly uniformed patrol officers, within hostile or suspicious communities.”).

- ²¹⁸ Tyler & Fagan, *supra* note 214, at 263 (demonstrating empirically that people are more likely to view law enforcement officials as legitimate social authorities and thus to cooperate with and report crimes when they perceive the processes police use when dealing with members of the public as fair); Peter Clarke, Speech at The Courts and Terrorism: Transatlantic Observations, Apr. 15, 2009 (noting that communities are more likely to provide information to law enforcement when they are confident that the information “will be treated with discretion, properly evaluated, and used in a properly focused way”).
- ²¹⁹ *Oversight of the Federal Bureau of Investigation: Hearing Before the S. Judiciary Comm.*, 110th Cong. (Sept. 17, 2008).
- ²²⁰ Muslim Advocates, Muslim Lawyers Issue Urgent Community Advisory (Sept. 29, 2009) (advisory issued by Muslim Advocates on behalf of that organization as well as the National Association of Muslim Lawyers, Capital Area Muslim Bar Association, Florida Muslim Bar Association, Georgia Association of Muslim Lawyers, Michigan Muslim Bar Association, Muslim Bar Association of Illinois, Muslim Bar Association of New York, Muslim Bar Association of Southern California, Muslim Lawyers of Houston, New England Muslim Bar Association, New Jersey Muslim Lawyers Association).
- ²²¹ Markon, *supra* note 215.
- ²²² See Vitello & Semple, *supra* note 172.
- ²²³ Watanabe & Esquivel, *supra* note 173; see also William Fisher, *The Spies Who Came in from the Mosque*, HUFFINGTON POST.COM, Mar. 9, 2009.
- ²²⁴ See Tom R. Tyler, Stephen Schulhofer, & Aziz Huq, *Legitimacy and Deterrence in Counterterrorism Policing: A Study of Muslim Americans*, 44 LAW & SOC’Y REV. 365 (2010).
- ²²⁵ Markon, *supra* note 215.
- ²²⁶ Lininger, *supra* note 41, at 1247.
- ²²⁷ See David A. Harris, *The Stories, The Statistics, and the Law: Why “Driving While Black” Matters*, 84 MINN. L. REV. 265, 273-74 (1999) (interview with executive in his thirties, who says “When I see cops today, I don’t feel like I’m protected. . . . I do not feel safe around cops”); *id.* at 272 (interview with another executive, who says: “I’m not trying to bother nobody. But yet I got a cop pull me over says I’m weaving in the road. And I just came from a friend’s house, no alcohol, no nothing. It just makes you wonder—was it just because I’m black?”); see also ELIOT SPITZER, THE NEW YORK CITY POLICE DEPARTMENT’S ‘STOP & FRISK’ PRACTICES: A REPORT TO THE PEOPLE OF THE STATE OF NEW YORK FROM THE OFFICE OF THE ATTORNEY GENERAL 79 (1999) (narrative of a 54-year-old African American detained and patted down without apparent grounds by New York City police: “I was shocked and humiliated at being treated like a common criminal . . . I don’t trust police officers.”).
- ²²⁸ See Tom R. Tyler, *Procedural Justice, Legitimacy, and the Effective Rule of Law*, 30 CRIME & JUSTICE 283, 340-45 (2003) (noting that multiple studies have shown that people react negatively to use of profiling even if they themselves are not profiled and, by contrast, when law enforcement actions are perceived as fair, people are more likely to support police and to perceive law enforcement actions as legitimate).
- ²²⁹ PETER VERNIERO, ATT’Y GEN. OF NEW JERSEY, INTERIM REPORT OF THE STATE POLICE REVIEW TEAM REGARDING ALLEGATIONS OF RACIAL PROFILING 46 (1999), available at http://www.state.nj.us/lps/intm_419.

pdf; *see also* Lankford v. Gelston, 364 F.2d 197, 203-04 (4th Cir. 1966) (ordering injunction against discriminatory police practices and noting the devastating effects such practices have on police-community relations and the potential they have to spark violence).

²³⁰ *See* Dorothy E. Roberts, *The Social and Moral Cost of Mass Incarceration in African American Communities*, 56 STAN. L. REV. 1271, 1296 (2004) (“Mass incarceration seems to verify stereotypes about black criminality that originated in slavery and are part of a belief system premised on the superiority of whites and inferiority of blacks.”).

²³¹ *Securing America’s Safety: Improving The Effectiveness Of Antiterrorism Tools And Interagency Communication: Hearing Before The S. Comm On The Judiciary*, 111th Cong. 106 (2010).

²³² *Id.*

²³³ Charlie Savage, *F.B.I. is Slow to Translate Intelligence, Report Says*, N.Y. TIMES, Oct. 27, 2009, at A20. While these findings may indicate that insufficient resources have been invested in recruiting and training linguists, they also illustrate that the FBI is collecting massive amounts of material that it feels no urgency to analyze.

²³⁴ *Summary of WH Review of the December 25, 2009 Attempted Terrorist Attack at 2*, available at http://www.whitehouse.gov/sites/default/files/summary_of_wh_review_12-25-09.pdf.

²³⁵ *Id.* at 5.

²³⁶ *See infra* notes 258-259 and accompanying text.

²³⁷ Rachel Williams & Richard Norton-Taylor, *7/7 Bomb Attacks: Police and MI5 Cleared of Blame*, GUARDIAN, May 19, 2009, available at <http://www.guardian.co.uk/uk/2009/may/19/july-7-attacks-Mohammad-sidique-khan-shehzad-tanweer-leader-Sidique-Khan-encountered-security-services-10-times-before-bombings>.

²³⁸ Charlotte Gill & Lucy Ballinger, *MI5 had 7/7 Ringleader on ‘Radar’ 12 Times*, DAILY MAIL ONLINE, May 20, 2009, available at <http://www.dailymail.co.uk/news/article-1184234/MI5-7-7-ringleader-radar-12-times-MPs-report-fails-point-finger.html>.

²³⁹ Williams & Norton-Taylor, *supra* note 237; Duncan Gardham, *July 7 Leader Sidique Khan Encountered Security Services 10 Times Before Bombings*, TELEGRAPH, May 19, 2009, available at <http://www.telegraph.co.uk/news/uknews/law-and-order/5351318/July-7-leader-Sidique-Khan-encountered-security-services-10-times-before-bombings.html>.

²⁴⁰ Gill & Ballinger, *supra* note 238. The report characterized as “astounding” the fact that in 2004 MI5 could deploy resources sufficient to pursue only a fraction of all known threats. Williams & Norton-Taylor, *supra* note 237.

²⁴¹ Great Britain has become known for its broad and aggressive surveillance efforts. *See* Sarah Lyall, *Britons Weary of Surveillance in Minor Cases*, N.Y. TIMES, Oct. 25, 2009, at A1.

²⁴² The British surveillance system also failed to prevent a similar attack just two weeks later, which was unsuccessful only because of an explosives malfunction. The ringleader of this planned attack also was no stranger to law enforcement. He had been captured in surveillance photos of a jihadi training camp a year before the failed attack, had failed to appear for a court date, and was the subject of an outstanding arrest warrant at the

time of the attack. Sandra Laville, *21/7 Bombers: Ringleader Slipped Through Police Net*, GUARDIAN, July 10, 2007, available at <http://www.guardian.co.uk/uk/2007/jul/10/terrorism/topstories3>. As with the 9/11 attacks in the U.S. and the 7/7 bombings in London, the necessary information was there; the resources and focus necessary to follow up on it were not.

²⁴³ Summary of WH Review of the December 25, 2009 Attempted Terrorist Attack, *supra* note 234, at 5-6.

²⁴⁴ NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 394-95 (2004) [hereinafter "9/11 Commission Report"].

²⁴⁵ Michael Mukasey, Address at the Oregon Anti-Terrorism Conference and Training, *supra* note 179.

²⁴⁶ *Oversight of the Federal Bureau of Investigation: Hearing Before the S. Judiciary Comm.*, 110th Cong. 8 (2008) (testimony of FBI Dir. Robert S. Mueller).

²⁴⁷ Michael Mukasey, Address at the Oregon Anti-Terrorism Conference and Training, *supra* note 179; *see also* U.S. Dep't of Justice, Briefing with Dep't Officials on Consolidated Att'y Gen. Guidelines (Sept. 12, 2008) [hereinafter "Justice Department Briefing"].

²⁴⁸ Justice Department Briefing, *supra* note 247.

²⁴⁹ *See supra* notes 119-122 and accompanying text (describing pretext interviews, physical surveillance, and tasking informants).

²⁵⁰ Justice Department Briefing, *supra* note 247.

²⁵¹ *Id.*; *Oversight of the Federal Bureau of Investigation: Hearing Before the S. Judiciary Comm.*, 110th Cong. 7 (2008) (testimony of FBI Dir. Robert S. Mueller) (claiming the FBI could surveil a suspected counterfeit blue jeans smuggler but not a terrorist carrying a bomb). Set aside the fact that raising money for Hezbollah is, in fact, the crime of providing material support to a terrorist organization, 18 U.S.C. § 1339B, and thus an investigation into that activity should be able to go forward under the general crimes guidelines.

²⁵² Ashcroft Guidelines, *supra* note 81, at Intro. A & B.

²⁵³ *Id.* at Intro. A; *see also* Letter from Caroline Frederickson, Dir., Nat'l Office of the ACLU, to Glenn A. Fine, Inspector Gen. of the U.S. Dep't of Justice (Sept. 22, 2008) (asking the Inspector General to investigate whether Director Mueller's comments indicated that the FBI was engaged in investigative activities beyond the scope of what the then-existing Guidelines permitted).

²⁵⁴ Ashcroft Guidelines, *supra* note 81, § II.B.6.

²⁵⁵ Justice Department Briefing, *supra* note 247; U.S. DEPT OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES FOR FBI NATIONAL SECURITY INVESTIGATIONS AND FOREIGN INTELLIGENCE COLLECTION, § II.A (2003), available at <http://www.fas.org/irp/agency/doj/fbi/nsiguilines.pdf>.

²⁵⁶ Michael Mukasey, Address at the Oregon Anti-Terrorism Conference and Training, *supra* note 179; Justice Department Briefing, *supra* note 247.

²⁵⁷ *See supra* notes 84-85 and accompanying text.

- ²⁵⁸ See 9/11 Commission Report, *supra* note 244, at 272.
- ²⁵⁹ *Id.* at 269-76, 424-27; REPORT OF THE COMMISSION ON THE INTELLIGENCE CAPABILITIES OF THE UNITED STATES REGARDING WEAPONS OF MASS DESTRUCTION 281-82 (2005).
- ²⁶⁰ Michael Mukasey, Address at the Oregon Anti-Terrorism Conference and Training, *supra* note 179; Justice Department Briefing, *supra* note 247; *Oversight of the Federal Bureau of Investigation: Hearing Before the S. Judiciary Comm.*, 110th Cong. (Sept. 17, 2008).
- ²⁶¹ *E.g.*, Ashcroft Guidelines, *supra* note 81, § III.
- ²⁶² *Id.* (quoting *United States v. United States District Court*, 407 U.S. 297, 322 (1972)).
- ²⁶³ Thornburgh Guidelines, *supra* note 20, § III.
- ²⁶⁴ Ryan J. Foley, *Grand Juries Target US Anti-war Activists*, ASSOC. PRESS, Feb. 7, 2004.
- ²⁶⁵ Monica Davey, *Subpoenas on Antiwar Protest Are Dropped*, N.Y. TIMES, Feb. 11, 2004, at A18.
- ²⁶⁶ 18 U.S.C. § 2709(c); 50 U.S.C. § 1861.
- ²⁶⁷ See, e.g., Ryan Singel, *FBI Targets Internet Archive with Secret 'National Security Letter,' Loses*, WIRED, May 7, 2008, available at <http://www.wired.com/threatlevel/2008/05/internet-archiv/>.
- ²⁶⁸ *Continued Oversight of the USA PATRIOT Act: Hearings before the S. Judiciary Comm.*, 109th Cong. 343 (2005) (testimony of Suzanne E. Spaulding).
- ²⁶⁹ Justice Department Briefing, *supra* note 247.
- ²⁷⁰ AGG Compliance Report, *supra* note 42, at 92-93 (noting problems with 104 of 120 confidential informant files examined—a noncompliance rate of 87%).
- ²⁷¹ *Id.* at 172.
- ²⁷² *Id.* at 173.
- ²⁷³ U.S. DEP'T OF JUSTICE, FBI, OFFICE OF THE INSPECTOR GENERAL, *A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS* xvi-xviii (2007).
- ²⁷⁴ *Id.* at xxxi-xxxii.
- ²⁷⁵ *Id.* at xxxiv-xl. These compliance problems are not just a modern phenomenon. The Attorney General Guidelines for Undercover Operations, initially implemented in 1981, have been revised repeatedly in response to troubling use of informants. AGG Compliance Report, *supra* note 42, at 39-46, 55-59. For example, a House subcommittee investigation into the use of the Undercover Guidelines in “Operation Corkscrew,” a 1977-82 investigation into case-fixing in the Cleveland Municipal Court, found that “virtually every one of the principal safeguards was either directly violated, ignored, or administratively construed in a manner inconsistent with their stated purposes with profoundly disturbing results.” *Id.* at 45-46. Moreover, this was not an isolated instance, “but in fact reflect[s] a pattern of recurrent problems which are inherent in

the process.” *Id.* at 45-46. The 2005 Justice Department Inspector General’s report concluded that, historically, informants’ field activities have been subjected to insufficient oversight. *Id.* at 59. And in the case of the CISPES investigation, discussed above, the investigation itself was found to be overbroad, and “resulted in the investigation of domestic political activities protected by the First Amendment that should not have come under government scrutiny.” *Id.* at 52.

²⁷⁶ U.S. DEP’T OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, *supra* note 9, at 165, 9-134.

²⁷⁷ U.S. DEP’T OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, A REVIEW OF THE FBI’S INVESTIGATIONS OF CERTAIN DOMESTIC ADVOCACY GROUPS 62, 107, 140 (2010).

²⁷⁸ *Id.* at 122, 140.

²⁷⁹ U.S. DEPT. OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, INVESTIGATION OF ALLEGATIONS OF CHEATING ON THE FBI’S DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE (DIOG) EXAM 1-2, 30-33 2010.

²⁸⁰ *Oversight of the Federal Bureau of Investigation: Hearing Before the S. Judiciary Comm.*, 110th Cong. 14 (2008) (statement of Sen. Arlen Specter).

²⁸¹ *United States v. Watson*, 423 U.S. 411 (1976) (police may make felony arrest on a public place); *Payton v. New York*, 445 U.S. 573 (1980) (warrant necessary for arrests made in the home).

²⁸² *New York v. Belton*, 453 U.S. 454 (1981) (police may search the passenger compartment and the contents of any containers in the passenger compartment when arresting a driver); *Carroll v. United States*, 267 U.S. 132 (1925) (police officers may make a warrantless search of an automobile if they have probable cause to suspect that it contains contraband).

²⁸³ *Warden v. Hayden*, 387 U.S. 294 (1967) (officers in pursuit of a suspected armed felon may enter and search a house into which the suspect has fled with no warrant).

²⁸⁴ Michael Mukasey, Address at the Oregon Anti-Terrorism Conference and Training, *supra* note 179; *Oversight of the Federal Bureau of Investigation: Hearing Before the S. Judiciary Comm.*, 110th Cong. (Sept. 17, 2008) (“[T]he FBI has to expand its intelligence collection beyond that which is collected as part of predicated investigations. It must examine threats in a proactive fashion and not simply rely on information that is provided to us.”).

²⁸⁵ *Oversight of the Federal Bureau of Investigation: Hearing Before the S. Judiciary Comm.*, 110th Cong. 23 (2008) (testimony of FBI Dir. Robert S. Mueller).

²⁸⁶ The Justice Department gave the illusion, though without any substance, of consultation with stakeholders before implementing the current guidelines. After drafting the Guidelines, the Department invited members of civil liberties and Muslim community organizations to series of briefing sessions with the FBI’s General Counsel where proposed drafts of the new Guidelines and DIOG were distributed (and recollected at the end of the session) and discussed. By the time these briefings took place, however, the policies they described were already substantially complete—they were implemented just a week later—and the Bureau had already begun training on their basis. The current policy thus does not represent meaningful input from affected communities.

²⁸⁷ USA PATRIOT Improvement And Reauthorization Act of 2005, Pub. L. No. 109-177, § 119 (codified as amended in scattered sections of the U.S. Code).

²⁸⁸ *Id.*

²⁸⁹ *GAO's Work At The FBI: Access to Data, Documents, and Personnel, Hearing Before the S. Judiciary Comm.*, 107th Cong. (2001) (statement of Norman J. Rabkin, Managing Dir., Tax Admin. and Justice Issues).

²⁹⁰ This is a vital element of effective reform. If, however, this change is not made, then a restriction on the use of information gathered in the absence of any reason for suspicion must be implemented: The FBI should be barred from disseminating or utilizing information gleaned in the course of intelligence-collection operations for purposes other than the purpose for which it was collected. Because of the extraordinarily broad intelligence-collection authority inherent in non-predicated investigations, use of information obtained through those authorities should be limited to the purpose for which it was collected. In other words, if the FBI acquires bank records through an NSL, those records should be used only in the terrorism investigation for which they were sought. If the records uncover no ties to terrorism, but suggest some other financial crime, the FBI should not be permitted to use the information gained through an NSL to pursue non-terrorism crimes.

²⁹¹ 392 U.S. 1 (1968)

²⁹² See Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5, at 7, 29 (n. 11), *available at* http://www.niem.gov/pdf/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued.pdf.

NEW & FORTHCOMING BRENNAN CENTER PUBLICATIONS

Renewing Democracy After Citizens United
Susan Liss and Michael Waldman

Small Donor Public Funding: The NYC Experience
Susan Liss, Angela Migally

Voting Machine Errors
Larry Norden

New Politics of Judicial Elections 2000-2009
James Sample, Adam Skaggs, Jonathan Blitzer

Voter Registration in a Digital Age
Christopher Ponoroff, Edited by Wendy Weiser

Criminal Justice Debt: A Barrier to Reentry
Alicia Bannon, Mitali Nagrecha, Rebekah Diller

Buying Justice: The Impact of Citizens United on Judicial Elections
Adam Skaggs

Domestic Counter-Terrorism and Radicalization
Faiza Patel

Corporate Campaign Spending: Giving Shareholders a Voice
Ciara Torres-Spelliscy

Foreclosures: A Crisis in Legal Representation
Melanca Clark with Maggie Barron

Racial Disparities in Federal Prosecutions
Brennan Center for Justice & the National Institute on Law and Equity

For more information, please visit www.brennancenter.org.

BRENNAN
CENTER
FOR JUSTICE

at New York University School of Law

161 Avenue of the Americas
12th Floor
New York, NY 10013
www.brennancenter.org