

**DOMESTIC
INTELLIGENCE:
OUR RIGHTS
AND SAFETY**

Faiza Patel, editor

BRENNAN CENTER FOR JUSTICE
AT NEW YORK UNIVERSITY SCHOOL OF LAW

**DOMESTIC INTELLIGENCE:
OUR RIGHTS AND OUR SAFETY**

Faiza Patel, editor

About the Brennan Center

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 constitutional protection 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.

The Brennan Center would like to acknowledge The Atlantic Philanthropies, CS Fund/Warsh-Mott Legacy, Democracy Alliance Partners, Herb Block Foundation, Open Society Foundations, and the Security & Rights Collaborative, a Proteus Fund initiative, for their generous support of our Liberty & National Security Program.

The editor would like to thank R. Kyle Alagood, Sadia Ahsanuddin, Madeline Friedman, Elizabeth Goitein, Seth Hoy, Kimberly Lubrano, Jim Lyons, Jeanine Plant-Chirlin, Desiree Ramos Reiner, and Frederick A.O. Schwarz, Jr., for their invaluable input and assistance, and Michael Waldman and John Kowal for their guidance and support.

The editor also greatly benefited from conversations with Zachary Carter, Glenn Fine, Lawrence Pedowitz, SungHee Suh, Stephen Schulhofer, and the Muslim American Civil Liberties Coalition. In addition, we are grateful for the advice and comments of Jethro Eisenstein, Udi Ofer, Hina Shamsi, Shirin Sinnar, and Matthew Waxman.

The essays and transcripts in this document emerged from a symposium hosted by the Brennan Center on March 18, 2011. Intelligence Collection and Law Enforcement: New Roles, New Challenges, brought together an array of perspectives to discuss the implications on civil liberties of the new roles that evolved for law enforcement officials post 9/11. Transcripts have been edited for clarity and accuracy.

CONTENTS

FOREWORD <i>by Michael Waldman</i>	IX
INTRODUCTORY ADDRESS: “AN INQUIRY INTO EXTREME IDEOLOGY AND VIOLENT ACTION SHOULD BE A BROAD-BASED EXAMINATION...”: <i>The Honorable Bennie G. Thompson</i>	I
KEYNOTE ADDRESS: “OUR COUNTERTERRORISM EFFORTS ARE GUIDED BY SEVERAL CORE PRINCIPALS...” <i>The Honorable John O. Brennan</i>	5
PART ONE: INTELLIGENCE COLLECTION BY STATE AND LOCAL LAW ENFORCEMENT	15
INTRODUCTION: <i>Faiza Patel</i>	17
“LAW ENFORCEMENT’S CORE VALUES SHOULD BE PREDICATED ON THE CONSTITUTION, THE BILL OF RIGHTS, CIVIL RIGHTS, AND HUMAN RIGHTS...”: <i>The Honorable Leroy D. Baca</i>	23
THE EXPANDING STATE AND LOCAL INTELLIGENCE ENTERPRISE AND THE THREAT TO CIVIL LIBERTIES: <i>Michael German</i>	25
“THE DEPARTMENT OF HOMELAND SECURITY HAS A RESPONSIBILITY... TO CONTRIBUTE TO A ROBUST INFORMATION SHARING ENVIRONMENT...”: <i>Kara Dansky</i>	37
AMERICAN POLICING AND THE INTERIOR DIMENSION OF COUNTERTERRORISM STRATEGY: <i>Matthew Waxman</i>	41
AN HISTORIC PERSPECTIVE OF INTELLIGENCE GATHERING: <i>Frederick A.O. Schwarz, Jr.</i>	53
PART TWO: THE FIRST AMENDMENT AND DOMESTIC INTELLIGENCE GATHERING	57
INTRODUCTION: <i>Elizabeth Goitein</i>	59
“TO THINK CLEARLY ABOUT THE FIRST AMENDMENT, IT IS USEFUL TO IDENTIFY BASIC PRINCIPLES BEFORE TRYING TO RESOLVE PARTICULARLY DIFFICULT OR VEXING ISSUES...”: <i>Geoffrey R. Stone</i>	65

FBI SURVEILLANCE AND CUSTOMS AND BORDER PATROL QUESTIONING: IMPACT ON THE FIRST AMENDMENT RIGHTS OF THE AMERICAN MUSLIM COMMUNITY: <i>Nura Maznavi & Jawziya Zaman</i>	69
PROTECTIONS FOR FIRST AMENDMENT-PROTECTED SPEECH AND RELIGION WHEN INVESTIGATING TERRORISM: <i>Kate Martin</i>	79
PART THREE: REGULATION OF DOMESTIC INTELLIGENCE GATHERING AND POTENTIAL FOR REFORM	85
INTRODUCTION: <i>Emily Berman</i>	87
NATIONAL SECURITY VS. DEMOCRACY IN AMERICA: <i>Shahid Buttar</i>	93
“[O]UR DOMINANT NOTION OF PRIVACY IS TOO LIMITED TO DO THE WORK NECESSARY FOR EFFECTIVE REGULATION OF DOMESTIC INTELLIGENCE.”: <i>Aziz Huq</i>	101
ENDNOTES	105
ABOUT THE CONTRIBUTORS	131

FOREWORD

On September 20, 2001, when President George W. Bush declared a global war on terror, he set in motion an unprecedented expansion of the nation's intelligence services in a bid to detect and thwart possible attacks both at home and abroad.

More than a decade later, the end of the war on terror may be in sight, but America remains in a perpetual state of emergency. At one level, these policies have been hugely successful. Despite initial fears, the September 11, 2001 attacks did not commence a sustained period of domestic violence. Although there have been a handful of smaller attacks, such as the recent Boston Marathon bombing, it remains true that widespread domestic terrorism has failed to materialize. This must be counted as a significant victory, and our national security apparatus surely deserves enormous credit. But the war on terror has been marked by a major, often unremarked shift – with uncounted costs and unresolved challenges.

Counterterrorism efforts, once traditionally the mandate of the federal government, are now aggressively pursued at the state and local levels. In addition to the FBI, state police and local sheriffs have entered the fray. No longer confined to their traditional mission of preventing and investigating crime, police departments are now equipped with extensive resources and powers to collect intelligence and conduct surveillance. At the same time, in the wake of the Boston Marathon bombing, we learned that the system will not prevent all attacks.

These new powers of intelligence collection and their lack of structured oversight have gone largely unexamined and unchecked. Restrictions have been relaxed on how the government gathers, shares, and uses information that is not related to any suspicion of criminal or terrorist activity. The few remaining curbs are inadequate to contain the rapid improvements in surveillance technology, which has spawned new ways to gather information on Americans.

Such lapses in accountability, oversight, and intelligence structure threaten to erode both our safety and civil liberties.

Counterterrorism efforts, whether pursued by an FBI agent or a beat cop, should be guided by sound theory and practice, not stereotypes and the politics of fear. America's vast intelligence network requires thoughtful and consistently enforced standards. Above all, we must demand that law enforcement is held accountable

to the people whose lives they have pledged to protect. These new and powerful members of the intelligence community must be constrained by checks and balances, respect for fundamental constitutional rights, and the rule of law.

This collection of essays and remarks and the symposium that inspired them are crucial first steps in ensuring that our nation's domestic intelligence infrastructure is true to our values. The strength of this volume lies in the diversity of its contributions. The Brennan Center for Justice at the New York University School of Law brought together policymakers, government leaders, scholars, civil rights lawyers, and law enforcement officials to examine law enforcement's role in intelligence collection. There are no easy answers and, at times, there is sharp disagreement. Nevertheless, as our counterterrorism efforts evolve, this conversation is vital to protect our essential freedoms and the foundation of American democracy.

Michael Waldman
President
Brennan Center for Justice

INTRODUCTORY ADDRESS

“AN INQUIRY INTO EXTREME IDEOLOGY
AND VIOLENT ACTION SHOULD
BE A BROAD-BASED EXAMINATION...”

TRANSCRIPT OF REMARKS

The Honorable Bennie G. Thompson
Ranking Member
House Committee on Homeland Security

I'm one of those individuals who has been on the Homeland Security Committee ever since it was a select committee, when it was created [in 2002]. A select committee is a committee with no jurisdiction. So you say, “Why in the world would you want to be on a committee with no jurisdiction, no authority in law?” Well, if you could see the future, you understood homeland security would be important. Some of us saw the future and got on the committee and labored in the vineyard until we received authority and jurisdiction. We're still trying to consolidate the jurisdiction. We're kind of split between several other committees, but basically the buck starts with the Homeland Security Committee.

The only other anecdotal comment I'd like to make before I go through my prepared presentation is that I'm a product of the South. So much of my framework for work on the committee comes from being a student at Tougaloo College. I met Martin Luther King, Jr. on the college campus. And I found out that because I was in the meeting, my state government decided to spy on me because I was somehow one of those radicals who had talked about the Constitution and freedom and equality in the State of Mississippi.

And one of the good things is, when I finally got to Washington, I had an opportunity to see my entire file. And so I saw a lot. My government is good at keeping up with me. That also leads me to say that sometimes we spend a lot of money on unnecessary things. Me being at an ACLU meeting does not mirror or require the amount of expenditure of public resources — you can just ask for the minutes of the meeting. And you can get them, so it's not a big deal.

I'd like to acknowledge the Brennan Center's report *Rethinking Radicalization*.¹ Radicalization recruitment and violent extremism is an issue that my colleagues and I in Congress have dealt with for several years. The ideology of what actually drives an individual of any race or ethnicity to commit violent acts are very complex issues that both the legislative and executive branches are still grappling to comprehend.

I'm sure many of you followed the committee's hearing on radicalization and the American Muslim community. As you know, I wholeheartedly disagreed with the premise of the hearing and requested Chairman [Rep. Peter] King to broaden the hearing's scope.

You see, as a Member of Congress I took an oath to support and defend the Constitution of the United States. And from my understanding, the First Amendment of the Constitution protects the freedom of religion and freedom of speech. This hearing overstepped those bounds and made law-abiding Americans unnecessarily uncomfortable. In addition to the hearing overstepping the bounds of the Constitution, an inquisition into the Muslim community ignored the facts that the Brennan Center's report [*Rethinking Radicalization*] reiterated: violent extremism knows no race, religion, or ethnicity.

As ranking member and former chairman of the Committee on Homeland Security, I take threats to our nation's safety and security very seriously. I firmly believe that an inquiry into extreme ideology and violent action should be a broad-based examination. I agree that homegrown terrorism and the Jihadist threat deserve continuing attention; however, narrowly focusing our attention on a particular religious or ethnic group lacks clarity and common sense. Today's terrorists do not share a particular ethnic, educational, or socioeconomic background.

Recently, when state law enforcement agencies were asked to identify terrorist groups in their states, Muslim extremists ranked 11th on a list of 18. Further, according to a study conducted by the Institute for Homeland Security Solutions, only 40 out of 86 terrorist cases examined from 1999 to 2009 had links to Al Qaeda.

According to the Southern Poverty Law Center, in 2010 the number of active hate groups in the U.S. topped 1,000 for the first time, and the anti-government movement expanded dramatically for the second straight year. This study indicated that several factors, including resentment over the change in racial demographics of the country, frustration over the lagging economy, and the mainstreaming of conspiracy theories contributed to the rise in the anti-government movement. Law enforcement agencies identified Neo-Nazis, environmental extremists, and anti-tax groups as more prevalent and dangerous than Muslim terrorist organizations. The sophisticated explosive device found recently along a parade route in Washington, D.C., on Martin Luther King Day, an act of domestic terrorism clearly motivated by racist ideology, should prove that other groups are just as willing and able to carry out horrific attacks on Americans.

In addition, terrorist groups are not the only threat. According to the Department of Homeland Security, lone wolves and small terrorist cells may be the single most dangerous threat we face. Attacks are just as likely to come from lone wolf extremists like James Wenneker von Brunn, the Holocaust Memorial Museum shooter,² Jared Lee Loughner, who is charged with a tragedy in Tucson, Arizona,³ as they are for Muslim extremist groups. And what do von Brunn and Loughner have in common with Muslim extremists like Nidal Hasan, the Fort Hood shooter,⁴ and Colleen LaRose, also known as Jihad Jane?⁵

All allegedly espoused radical views on the Internet through extremist websites, chat rooms, and popular websites.

This starkly illustrates what should be common sense. The most effective means of identifying terrorists is through their behavior, not ethnicity, race, or religion. While knowing these facts put us at an advantage, just being aware is not enough. The nation's law enforcement resources are already stretched thin. We must ensure that we are using these resources to yield the best results. One of your other presenters today actually was my witness at the hearing last week — a wonderful person, the Sheriff of Los Angeles County, Sheriff [Leroy] Baca gets it. Many people thought, "Why would Democrats pick a Republican as their witness for the hearing?" Well, Sheriff Baca understands that you have to engage communities in order to receive intelligence as to what's going on. But you also have to instill confidence in the community that they won't be betrayed, nor intimidated, or outed if that intelligence is forthcoming. If you do it the other way, then the information necessary to secure our communities from any group will be lessened. And good law enforcement will dictate that you have to engage communities rather than intimidate communities.

So I pay special tribute to Sheriff Baca and his men and women in uniform. But the other thing I'll confess to this group, is that members of Congress really don't know everything. Sometimes we pretend we do, but in reality we depend on individuals like you to provide the research, the encouragement, the advocacy for your issues so that we get it right. This country is only as good as its people. And unless we continue to promote the active involvement of all its people, we won't get it right.

Lastly, I think we have to understand that whatever we do has ramifications internationally. So if we start showing that we are picking on any particular group in America just because of who they are, then clearly there are other people in other parts of the world that will take advantage of that. So when we say on our committee — some of the conventional thought is that we are to profile all Muslims. We can't do that. Or if someone says we have too many mosques in America — we can't promote that school of thought because both schools of thought create opportunities for bad people to do mischief other places.

Now, how can good people like you help us? Apart from what you do, we all have to be committed to making sure we help keep this country safe. Unfortunately, we can invent every piece of technology known to man and potentially bad things will still happen. So people have to become involved in the process too. You say, "Well, what can I do? I'm just a lawyer trying to make a living," a research assistant or religious person." Well, all of us — the term we adopted last year was, "See something, say something." Very simple.

You can help us. For a person from Mississippi to encourage people to participate in government and help us keep it safe is something I learned because I trust my government. I trust my federal government to get it right. I've still got a few issues state and local, but I'm working on them, too. But I do trust my federal government

to get it right. So more or less, we have to maximize our efforts to counter violent extremism and radicalization in this country. If we're going to move forward, we have to recognize and protect this nation.

Our Constitution is a sacred document. The First Amendment talks about individual thought and speech being protected. Under the Fourth Amendment, Americans also enjoy significant privacy rights. I don't think Big Brother should be peeping in our bedrooms or any other thing. There are ways that we can get intelligence without infringing on the rights of people.

KEYNOTE ADDRESS

“OUR COUNTERTERRORISM EFFORTS ARE GUIDED BY SEVERAL CORE PRINCIPALS...”

TRANSCRIPT OF REMARKS

The Honorable John O. Brennan

Director

Central Intelligence Agency

*Former Deputy National Security Advisor for Homeland Security
and Counterterrorism*

I very much wanted to join you to discuss a subject that I deal with directly every day and which is vital to our national security — the role of law enforcement in the post-9/11 era. And I want to take this opportunity to put that work in a broader context — the principles and policies that are guiding the President and his administration as we work to prevent acts of terrorism against the American people.

Nearly ten years after the September 11th terrorist attacks, the United States remains at war with Al Qaeda and its associated forces. Because of the relentless pressure to which we’ve subjected it, the senior Al Qaeda leadership is increasingly hunkered down in its safe haven in Pakistan’s tribal regions. Still, it retains the intent and capability to attack the U.S. homeland and our allies abroad.

Despite having its ideology rejected by the overwhelming majority of Muslims and being at its weakest point since 2001, the threat from Al Qaeda is diversifying. Groups and individuals have sprung up in places like Pakistan, Yemen and North Africa, and seek to commit violent acts to further Al Qaeda’s murderous agenda.

We have also seen this problem begin to manifest itself here at home. A very small but increasing number of individuals here in the U.S. have become captivated by these violent causes, seeking to commit violent acts here at home — their plots were disrupted in Washington, D.C., Oregon, and Maryland during the past year alone. Others have traveled abroad to join the ranks of international terrorist groups and work to further their cause.

Though it has changed significantly over the past ten years, the threat from Al Qaeda and its adherents represents the preeminent counterterrorism challenge we face today, and protecting the American people from this threat remains our highest national security priority.

Some suggest this is largely a military and intelligence challenge with a military and intelligence solution. Our military and our intelligence professionals — and the unique capabilities they offer — are an essential part of our counterterrorism efforts. But, to argue that they are the only solution — or that we should place limitations on other tools and capabilities — is a misunderstanding of the complexity of the problem that we face.

Confronting this complex and constantly evolving threat does not lend itself to simple, straightforward solutions. No single tool alone is enough to protect the American people against this threat. We need to use all these tools, together. That is what the Obama Administration is doing. So, our counterterrorism efforts are guided by several core principles.

First, our highest priority is — and always will be — the safety and security of the American people. The United States Government has no greater responsibility.

Second, we will use every lawfully available tool at our disposal to keep the American people safe — military, intelligence, homeland security, law enforcement, diplomacy, and financial at all levels of the government, working seamlessly.

Third, even as we are unyielding in pursuit of those who would do us harm, we will remain true to the values and ideals that have always defined us as a nation. Only by adhering to our values are we able to rally individuals, communities, and entire nations to the cause of protecting the world against the threat posed by Al Qaeda.

Fourth, we will be pragmatic, not ideological — making decisions not on the basis of preconceived notions of which tool is perceived to be “stronger,” but based on the evidence of what works, what will actually keep America safe.

Fifth, we must retain the necessary flexibility to address each threat in a way that best serves our national security interests. When confronting the diverse and evolving threat from Al Qaeda and its adherents, different circumstances will call for different tools.

Guided by these principles, the administration has worked hard over the past two years to establish a counterterrorism framework that is effective and sustainable. This includes the two tools you have gathered to discuss today — law enforcement and intelligence.

The intersection of these two has at times become a subject of intense debate. But to draw the conclusion that the use of law enforcement tools prior to 9/11 somehow hindered our efforts to protect the American people, and that we should therefore abandon the use of law enforcement in this conflict, would be a mistake. In the aftermath of 9/11, the challenges we had to overcome to effectively confront the terrorist threat to this country proved to be much more complicated than ever before. As a result, much of what we have seen over the past ten years has been an evolution — to find flexible and effective ways to leverage all of our capabilities to confront an evolving threat, including our law enforcement and our intelligence capabilities.

Law enforcement and intelligence are not mutually exclusive. In fact, they can and must reinforce one another. Intelligence is absolutely critical to identifying

and disrupting terrorist networks. It empowers law enforcement, informing their operations and enabling them to identify and disrupt plots before they are carried out. And intelligence often plays a critical role as evidence at criminal trials.

Law enforcement is equally indispensable. Through aggressive investigations, we have been able to identify members of terrorist networks and detect their plots. The tools available to law enforcement allow us to act swiftly to disrupt the plots we uncover, and to incapacitate dangerous individuals through successful prosecution and conviction. Law enforcement also has a well-proven track record of gathering vital intelligence through interrogation. When faced with the fair but heavy hand of American justice, terrorists have offered up valuable intelligence about Al Qaeda and other terrorist groups.

Our challenge, therefore, has been to carefully integrate intelligence and law enforcement — consistent with our values and the rule of law — to ensure that they complement and reinforce each other.

After 9/11, our law enforcement and intelligence communities had to adapt, gain new tools and authorities, restructure, and change their cultures and operations. We updated and improved our criminal code to better empower law enforcement to disrupt plots before they take innocent lives. We eliminated the so-called “wall” to allow intelligence and law enforcement personnel to work together, a critical step toward better integration of our law enforcement and intelligence tools.

The USA PATRIOT Act and amendments to the Foreign Intelligence Surveillance Act provided our counterterrorism community with enhanced investigative authorities. We reorganized our intelligence, law enforcement, and counterterrorism communities to enable them to function more effectively as a whole. The Federal Bureau of Investigation has been further integrated into the [U.S.] Intelligence Community, and continues its transformation into an intelligence-driven organization.

Each of these steps has transformed law enforcement into a more effective counterterrorism tool, one that can be used preemptively — before an attack is attempted, before a bomb goes off. And because they remain bound by our laws and our Constitution, there will always be checks on the use of these law enforcement tools, to ensure they remain consistent with our laws and our values. As a result, today, we are better positioned to protect the American people.

That does not mean that our work is done. When it comes to the detention, interrogation and prosecution of suspected terrorists, our record is clear. Spanning two consecutive administrations, we have successfully leveraged our criminal justice system to protect the American people against the threat from Al Qaeda. According to its own figures, the Bush Administration used federal courts to prosecute suspected terrorists — including several apprehended overseas — on hundreds of occasions, including Zacarias Moussaoui, Richard Reid, Ahmed Omar Abu Ali, Ehsanul Sadequee, Oussama Kassir, and many others.

Today, this impressive record of arrest and prosecution of terrorist suspects in

federal court is, unfortunately, frequently forgotten, which has prompted a debate over how best to handle, prosecute and punish those accused of trying to attack our country. That debate has, at times, been conflated with another important and consequential debate that we are engaged in with respect to the future of Guantanamo.

And nowhere does the intersection of law enforcement and intelligence — not to mention our Constitution and our values — come together as starkly as it does in Guantanamo. Before 2009, few counterterrorism proposals garnered as much support on both sides of the political aisle — from [former Secretary of State and Chairman of the Joint Chiefs of Staff] Colin Powell to President [George] Bush and [Sen.] John McCain — as the proposal to close Guantanamo.

This administration, for the first time, consolidated all information about the detainees held there, and departments and agencies identified the most appropriate disposition for each individual, and recommended that we bring several individuals to justice for their crimes. The administration remains committed to the closure of Guantanamo — to do what is in the national security interest of this country — and we have continued to move forward with key elements of our plan, including restarting military commissions and providing those who will continue to be held a thorough process of periodic review to ensure their detention is necessary and justified.

But support for closing Guantanamo has inexplicably waned, and some in Congress have sought to impose unprecedented restrictions on the President's discretion to transfer and prosecute the individuals held there.

Some have argued that all of these cases should be tried in military commissions and have sought to bar the executive branch from prosecuting any Guantanamo detainees in our Article III courts.

Where we believe a military commission is appropriate, we will move forward. However, where the evidence suggests our federal courts are more likely to produce a result that is consistent with our national security, we will push Congress to repeal these restrictions so that we can take the steps necessary to bring those individuals to justice. Repeal of these unprecedented encroachments on executive authority is critical, so that we can make informed decisions about where to bring terrorists to justice, transfer those it is no longer in our interest to detain, and achieve an essential national security objective — the closure of the detention center at Guantanamo Bay.

Even as we deal responsibly with those in our custody, we face the challenge of dealing with those we capture or arrest in the future. When arresting terrorist suspects, we must balance at least four critical national security objectives. First, disrupt the terrorist-related activity of the individual, including ongoing plots to kill innocent people. Second, gather any intelligence the individual may have that could enable us to identify and disrupt additional plots against the U.S. and our allies. Third, protect the intelligence, including sources and methods, which allowed us to identify or disrupt that individual and his activities. Finally, where the individual poses an enduring threat — as is often the case in terrorism investigations — provide for the sustainable incapacitation of that individual.

There can, at times, be tension between these objectives, so our core principles and values must guide our every step. When confronted with the question of where to bring someone to justice, we cannot base our decisions on preconceived notions about which system is “stronger” or “more effective” in the abstract. The factual and legal complexities of each case, and relative strengths and weaknesses of each system, must guide our decisions to ensure success. Otherwise, dangerous terrorists could be set free — intelligence lost and lives put at risk.

Terrorists arrested inside the U.S. will, as always, be processed exclusively through our criminal justice system. As they should be. The alternative would be inconsistent with our values and our adherence to the rule of law. Our military does not patrol our streets or enforce our laws in this country. Nor should it. Every single suspected terrorist taken into custody on American soil — before and after the September 11th attacks — has first been taken into custody by law enforcement. Our criminal justice system provides all of the authority and flexibility we need to effectively combat terrorist threats within our borders. In the aftermath of 9/11, two individuals taken into custody by law enforcement were later transferred to military custody. And after extensive litigation and significant cost, both were transferred back to law enforcement custody and prosecuted.

Similarly, when it comes to U.S. citizens involved in terrorist-related activity, whether they are apprehended overseas or here at home, we will process them exclusively through our criminal justice system. There is bipartisan agreement that U.S. citizens should not be tried by military commissions. Since 2001, two U.S. citizens were held in military custody, and after years of controversy and extensive litigation, one was released; the other was prosecuted in federal court. Even as the number of U.S. citizens arrested for terrorist-related activity has increased, our civilian courts have proven they are up to the job — providing all of the flexibility and authority we need to counter the threat.

The U.S. cannot expect to detain its way out of this problem. Recreating another Guantanamo runs contrary to our national security interests. So, we must work with our partners to empower them to assist us in our efforts to bring terrorists to justice. In many cases, their home country, the country in which they are apprehended, or the country they seek to attack may have a similar interest — to arrest and prosecute them. Where our partners have the capability to do so, we often work with those countries to assist them in those efforts — by sharing evidence or making witnesses available — to ensure that our collective interests are protected. Where countries lack the capability to lawfully detain and prosecute terrorists, we must work with them to develop the capabilities to mitigate the threat these individuals pose to their people and ours. Our long-term security requires that they build and maintain the capacity to provide for their own security, to root out the Al Qaeda cancer that has manifested itself within their borders and to prevent it from returning.

Where other countries are unwilling or unable to eliminate the threat an individual or network poses, we will continue to act, consistent with our legal

obligations, to eliminate the threat. Where we take custody of an individual, we will maintain appropriate policies and mechanisms to preserve our ability to bring that individual to justice — in our civilian courts and our reformed military commissions.

Our legal authority to use military commissions to prosecute terrorism suspects is not limited to Guantanamo, and we will not limit it to Guantanamo as a policy matter. We will reserve the right, where appropriate, to prosecute individuals we capture in the future in reformed military commissions.

Our federal courts are unrivaled when it comes to incapacitating dangerous terrorists. Since 2001, the Department of Justice has convicted hundreds of individuals in terrorism-related cases. In many cases, the individuals have received lengthy prison sentences, and have provided significant and valuable intelligence. Law enforcement, including our federal courts, has been an indispensable part of our strategy to protect the American people, essential to efforts to disrupt, dismantle and defeat Al Qaeda and its adherents. Where this option best protects the full range of U.S. security interests and the safety of the American people, we will not hesitate to use it.

This is not a radical idea. As former Attorney General John Ashcroft said, “Our priority should be a priority of preventing further terrorist attacks...” As he explained, “[T]o automatically allocate people from one system to another without understanding what best achieves that priority would ... be less than optimal.”

Some argue that military commissions are inherently more effective and therefore more appropriate for trying suspected terrorists. Yet our federal courts are time-tested, have resulted in far more detentions and convictions, and have produced much longer sentences on average than military commissions. In choosing between our federal courts and military commissions in any given case, this administration will remain focused on producing the right result.

Because of bipartisan efforts to ensure that military commissions provide all of the core protections that are necessary to ensure a fair trial, there are remarkable similarities between commissions and our federal courts. The reformed military commission system includes the attributes Americans believe are necessary to ensure a fair trial: presumption of innocence; proof beyond a reasonable doubt; an impartial decision maker; the right to counsel, including the right to choose counsel; government-provided representation for those who cannot afford to pay; a right to be present during court proceedings; a right to exculpatory evidence; and a right to present evidence, compel witnesses and compel favorable witness testimony.

In 2009, Congress agreed to replace the original, untested system for protecting classified information in military commission proceedings. They did so by largely codifying the rules that have proven extremely effective in our federal courts — a testament to the strength of our federal courts in protecting intelligence and comfort that our commissions will do the same going forward.

In some cases, there are advantages to military commissions. There is greater

flexibility to admit hearsay evidence. Confessions can be introduced in military commissions even if Miranda warnings were not issued, but they have to be reliable and, except in limited circumstances, voluntary.

Though others, such as the former Assistant Attorney General for National Security David Kris, have spoken eloquently about the relative merits of both systems, the advantages of our federal courts often are under-appreciated. Our federal courts have a significantly broader scope — a substantially longer list of offenses can be leveraged to prosecute terrorists regardless of the terrorist organization they belong to. Federal courts provide greater clarity and predictability; decades of experience prosecuting terrorists in this system allows us to predict with a greater degree of certainty the admissibility of evidence or even the likely outcome. Federal courts provide a greater degree of finality — the results of successful prosecutions are more sustainable because the validity of the offenses and the system as a whole are less susceptible to legal challenge. Finally, federal courts facilitate cooperation with our partners in bringing terrorists to justice — some of our most important allies will not hand over terrorists, or the evidence needed to convict them, unless we commit to using it only in our federal courts.

Because of the reforms passed by Congress, we succeeded in bringing the military commission system in line with the rule of law, and with our values. Today, both systems — the federal courts and military commissions — can be used to disrupt terrorists' plots and activities, to gather intelligence, and to incapacitate them through prosecution. But, we must let the facts and circumstances of each case determine which tool we use. That is the only way to ensure we achieve the result that best serves the safety and security of the American people.

As a former career intelligence professional, I understand the value of intelligence. And, when it comes to protecting the American people from Al Qaeda and its adherents, intelligence is critical to identifying and disrupting their plots, as well as dismantling their network. One of our greatest sources of information about Al Qaeda, its plans, and its intentions has been the members of its network who have been taken into custody by the U.S. and our partners overseas. Wherever possible, we must maintain a preference to take custody of terrorists, to preserve the opportunity to elicit information that is vital to the safety and security of the American people. Those who suggest that this administration has shied away from detention ignore the fact that, for a variety of reasons, reliance upon U.S. detention for individuals apprehended outside of Afghanistan and Iraq began declining precipitously years before this administration came into office.

After ten years of relentless pressure, our adversaries have become adept at avoiding areas where they are susceptible to capture — and into places where the ability of the U.S. to capture and detain them is limited.

Arguing that the decline in military detention or detention by the CIA results in a decline in intelligence also ignores the vital intelligence we gain from individuals in the criminal justice system. That is often a very difficult task, but in this case,

the facts do not lie. In the past two years alone, our criminal justice system has proven to be an extremely valuable intelligence collection tool. We have successfully interrogated several terrorism suspects who were taken into law enforcement custody and prosecuted, including Faisal Shahzad, Najibullah Zazi, David Headley, and many others.

Perhaps no single case has generated as much controversy as that of Umar Faruq Abdulmutallab, charged with attempting to blow up a plane over Detroit. I know that many argued that he should have been placed in military custody and that he should not have been given his Miranda warnings. But, the fact is that his arrest ultimately produced valuable information, and there's no reason to believe that placing him in military custody would have produced a better result from an intelligence collection perspective, or would have done so more quickly.

The flexibility and leverage that the criminal justice system provides to gather intelligence — before and after arrest, through proffers and plea agreements, and in some cases even after conviction or sentencing — is undeniable. So we have sought to empower our counterterrorism professionals to leverage the strengths of this system to gather critical intelligence.

And, where appropriate, we have made adjustments — to enhance our ability to collect intelligence through interrogation.

Consistent with our laws and our values, the President unequivocally banned torture and other abusive interrogation techniques, categorically rejecting false assertions that these are the most effective means of interrogation.

The President approved the creation of a High-Value Detainee Interrogation Group, or HIG, to integrate the most critical resources from across the government — experienced interrogators, subject matter experts, intelligence analysts, and linguists — to conduct or assist in the interrogation of those terrorists, both at home and overseas, with the greatest intelligence value. Through the HIG, we bring together the capabilities that are essential to effective interrogation, and have the ability to mobilize them quickly and in a coordinated fashion.

Some suggest getting terrorists to talk is as simple as withholding Miranda warnings. Assertions that Miranda warnings are inconsistent with intelligence collection ignores decades of experience to the contrary. Miranda warnings have not proven to be an impediment in most cases. Though some have refused to provide information in the criminal justice system, the same can be said of many held in military or intelligence custody from Afghanistan to Guantanamo.

But, Miranda warnings have, in several cases, been essential to our ability to keep dangerous individuals off the streets, as post-Miranda admissions have led to successful prosecutions and long-term prison sentences.

Rather than succumb to the false choice between intelligence collection and a sustainable disposition for the individual, we must make informed decisions, based on the evidence and the circumstances of each case, to maximize our intelligence collection and our ability to keep dangerous individuals behind bars.

Where our laws provide additional flexibility, we must empower our counterterrorism professionals to leverage it. The Supreme Court has recognized an exception to Miranda, allowing statements to be admitted if they are prompted by concerns about public safety. Applying that ruling to the more complex and diverse threat of international terrorism can be complicated, but our law enforcement officers deserve clarity. And that is why at the end of 2010, the FBI provided guidance to agents on use of the public safety exception to Miranda, explaining how it should apply to terrorism cases. The FBI has acknowledged that this exception was utilized last year, including during the questioning of Abdulmutallab and Faisal Shahzad. When the immediate threat to public safety was addressed, Miranda warnings were provided, and as the public now knows, intelligence collection did not end; it continued.

The evolution that began following the 9/11 attacks continues. Where possible, we should develop more effective and flexible tools, or strengthen the ones we have, to empower our counterterrorism professionals to succeed, while upholding the values and freedoms that make this country great. Combating terrorism requires a practical, flexible, results-driven approach that is consistent with our laws and our values. It is essential to our effectiveness, as well as our ability to sustain that strategy over time. Our criminal justice system, even though it is just one tool in this fight, embodies each of these things. Where it is available, it is, quite simply, one of the best counterterrorism tools we have to disrupt, dismantle, and defeat Al Qaeda and its adherents. It has demonstrated unrivaled effectiveness, unquestioned legitimacy, and the flexibility to preserve and protect the full spectrum of our national security objectives.

A rigid approach to the custody, questioning, and prosecution of terrorist suspects, by contrast, would be ineffective; unnecessarily complicating our efforts to counter the complex and diverse threat from Al Qaeda and its adherents and putting at risk the security of the American people. The executive branch, regardless of the administration in power, needs the flexibility to make well-informed decisions about how to handle terrorist suspects — based on the unique circumstances of each case and the advice of experienced professionals. A one-size-fits-all policy in the area of detention and prosecution would be harmful to our national security.

To achieve and maintain the appropriate balance, Congress and the executive branch have to work together. There have been and will continue to be many opportunities to do so in a way that strengthens our ability to defeat Al Qaeda and its adherents. As we do so, the Obama Administration will be guided by the principles I have laid out here today.

And finally, as we meet here today, a process of political transformation is underway in many parts of the Middle East, an area that I have focused on throughout most of my professional career. But even as I watch history being made in the Middle East, with the political landscape being changed in ways that were difficult to imagine just two or three months ago, I am mindful of how fortunate we are to live in a society where respect for rule of law and a set of universal rights and freedoms is the norm. And I am truly inspired by the determination and

courage of those who pursue one of the most basic of those universal rights — the right to live in a society that respects the rule of law. If we have learned anything about ourselves and about our values in the period since 9/11, it is that respect for the rule of law is not something to be called upon only when it is easy or convenient. Rather, it is the very hallmark of our democracy and our social compact as a nation. I believe that we operate outside that framework and code at our own peril, and I am proud to represent a President, and an administration, and a nation, that feels the same way.

PART ONE

**INTELLIGENCE COLLECTION BY STATE AND LOCAL
LAW ENFORCEMENT**

INTRODUCTION

Faiza Patel

*Co-Director, Liberty & National Security Program
Brennan Center for Justice*

In the past decade, state and local law enforcement agencies have become more and more involved in counterterrorism efforts that have traditionally been the preserve of the federal government. While crime prevention has always been a goal of local law enforcement agencies, the prevention of terrorist attacks has become a central part of their mission and for some, even their primary mission. Consistent with this shift, police departments have increasingly focused their resources on intelligence gathering. As Department of Homeland Security (DHS) Secretary Janet Napolitano has stated: “Increasingly, state, local, and tribal law enforcement officers...are on the frontlines of detection and prevention.”¹

The three main pathways through which state and local law enforcement agencies become involved in federal counterterrorism and intelligence gathering are:

- Joint Terrorism Task Forces (JTTFs), which are operationally focused teams run by the Federal Bureau of Investigation made up of personnel from federal, state, and local law enforcement agencies.² Prior to 9/11, there were 35 such teams; currently 103 JTTFs are operating around the country.³
- Fusion centers, which were developed in the aftermath of 9/11, initially as a way to respond to the threat of terrorism (although their mandate has expanded to cover ordinary crime and sometimes also natural disasters).⁴ Created and operated by states and localities, fusion centers receive funding and personnel resources from the federal government.⁵ Federal, state, and local law enforcement officials are co-located at these centers, which collect, analyze, and disseminate information.⁶

- Suspicious Activity Reporting (SAR), a system by which state and local police departments collect information — both of a criminal and non-criminal nature and from both government and private sources — which may be indicative of a future terrorist or criminal act.⁷ This information is then fed into a local database and should be vetted before it is shared widely within the law enforcement community through the Information Sharing Environment.⁸

In addition to these mixed federal/state/local mechanisms, some police departments have reconstituted intelligence gathering capabilities that were dismantled in the wake of the police spying scandals in the 1950s and 1960s. The New York City Police Department (NYPD) is perhaps the best-known example of a police department that is engaging in intelligence collection on a large scale.⁹

These developments require a shift from thinking about counterterrorism as a federal project to thinking about it as one that integrates state and local law enforcement as well. This, in turn, requires us to consider questions about the efficacy and appropriateness of using local police to gather intelligence about the communities that they serve.

In his remarks during the symposium, Professor Matthew Waxman of Columbia Law School noted that one's view of the extent to which local law enforcement should become involved in counterterrorism could depend on the contours of the perceived threat. In his view, if foreign terrorist organizations are considered the main threat to American security, federal law enforcement has comparative advantages in investigating well-organized, transnational terrorist organizations. These include a knowledge base, technical capabilities, and a robust network of relationships abroad with foreign intelligence services. In contrast, if small, homegrown terrorist groups pose the primary threat, local law enforcement, with its large numbers, familiarity with nearby communities, and relationships with the citizenry, may be better suited to the task.¹⁰ Of course, the extent of the "homegrown" threat is hotly disputed¹¹ and often the subject of political grandstanding.¹²

Even assuming that there is a significant "homegrown" threat, is local law enforcement best suited to lead the response? Another contributor, Michael German of the American Civil Liberties Union, thought not. He noted that the post-9/11 preventive policing imperative means that law enforcement officials are frequently examining behavior that is not criminal in and of itself. Rather they are puzzling through innocuous bits of information to see if they portend an attack. As an example, he pointed to investigations of violent extremism involving Muslims. The danger is that local police — who are unlikely to be sophisticated about either Islam or signs of terrorist activity — might mistakenly latch onto common religious behavior as indicators of terrorism.

The potential for police conflation of religious behavior with terrorism is exacerbated by the lack of training of the type that would enable police to accurately

and responsibly investigate violent extremism. Recent revelations about the training materials used by the FBI and the Department of Justice have prompted comprehensive internal reviews.¹³ The situation is no better in local police departments. For example, the NYPD report *Radicalization in the West* — which has been widely criticized for oversimplifying the path to terrorism and suggesting that the tendency to become a terrorist can be apparent in innocuous behavior such as becoming increasingly devout or growing a beard¹⁴ — is frequently used by local cops trying to understand terrorism.¹⁵ The problem with this sort of oversimplified training, German explained, is that it focuses investigative resources on individuals who happen to share certain visible characteristics, rather than on suspicious behavior.

At DHS, the Office of Civil Rights and Civil Liberties (CRCL) is responsible for helping to shape the Department's policy and practices to ensure respect for civil rights. Kara Dansky explained that many of CRCL's activities are aimed at protecting against the types of risks identified by German.

For example, DHS reviews intelligence products that are disseminated through the Office of Intelligence and Analysis to ensure they do not describe incidents of actual or perceived racial or ethnic profiling, violations of constitutional rights or other civil rights and civil liberties issues. CRCL also trains intelligence analysts before they are deployed to fusion centers to improve awareness of civil rights and civil liberties issues in intelligence operations. Interestingly, while DHS's activities are focused on those *analyzing* the information, the local police *collecting* the information that constitute part of German's concerns may not be covered. Rather, these police tend to develop their own training, which is financed but not controlled by DHS. This has led to significant unevenness in training and concerns that the instruction itself is biased.¹⁶

Knowledge of the communities they police is often identified as part of the added value that local police bring to counterterrorism intelligence operations. This is, however, a double-edged sword. When law enforcement uses the mantle of community policing to pursue an intelligence-driven agenda, communities are quick to discern the true purpose. This tends to undermine hard-won relationships and to increase distrust and reluctance to talk to the police.¹⁷ Programs that intrude into the daily lives of residents — such as the NYPD's infiltration of the city's Muslim communities — are likely not conducive to the type of information exchange that our counterterrorism agencies are seeking.¹⁸ The situation may be compared to immigration enforcement. Many police chiefs have objected to participating in federal immigration programs because they engender distrust of local police and discourage immigrants from engaging with law enforcement.¹⁹

An important element of how intelligence gathering by local police affects community relations is the extent to which these efforts are regarded as legitimate. Sheriff Leroy Baca of the Los Angeles County Sheriff's Department explained that in order to maintain the good relationships that are essential to public trust policing, police departments must carefully select the sort of information they collect and

analyze. He stated that his department, for example, only aggregates information on criminal activities and excludes data on political, religious, and social views, except as it specifically relates to criminal activity. In Sheriff Baca's view, communities have historically had minimal qualms with regard to information gathering, so long as it has a criminal nexus.

The approach advocated by Sheriff Baca would have the added benefit of avoiding intrusion into First Amendment-protected activities such as speech and religion. Some cities, such as San Francisco and Seattle, have local laws that specifically prohibit their police departments from collecting information on residents' political, religious, and social views unless there is a nexus with criminal or terrorist activity.²⁰ Compliance with these laws, however, has been spotty, particularly when local police are cooperating with federal officials in JTTFs.

Recently, the issue received renewed attention in San Francisco with the release of the Memorandum of Understanding between the FBI and the San Francisco Police Department (SFPD). Under the agreement, the SFPD was bound by the FBI's guidelines but in case of a conflict between those and local law "the standard or requirement that provides the greatest organizational protection or benefit will apply, unless the organizations jointly resolve the conflict otherwise."²¹ In response to concerns about this vague provision, SFPD Police Chief Greg Suhr adopted a Police Bureau Order that clarified that "SFPD officers shall work with the JTTF only on investigations of suspected terrorism that have a criminal nexus."²² The Order also stated that where California statutory law is more restrictive than comparable federal law, SFPD officers assigned to the JTTF must follow California statutory law.²³

The San Francisco experience may be regarded as an example of Professor Waxman's theory that local governments and the values of the communities that local police departments serve will serve as a check on overbroad intelligence gathering.

Another risk of a broad intelligence collection mandate, highlighted by German, is the opening of doors to abuse, specifically that the mandate will be executed in a selective and discriminatory manner. For example, there have been a slew of reports indicating that law enforcement is monitoring political and social protesters such as anti-war groups and environmental activists. If activity that is regarded as suspicious is defined too broadly — say, taking photographs of infrastructure such as bridges — then police will have to decide which of the many people conducting these activities to question and report. If history is any guide, their suspicions will fall on minorities and others regarded as outside the mainstream.²⁴

A final issue raised by Waxman was the need for oversight of intelligence collection in order to prevent abuse by the authorities and ensure that national security resources are properly directed. The federal experience has shown, however, that crafting such an oversight structure in the national security context is quite a difficult matter. The type of oversight structure best suited to local law enforcement's unique characteristics remains an open question.

The contributors' discussion of these issues suggested that incorporating state and local police into the federal government's counterterrorism efforts carries with it risks to community relations as well as to civil liberties. Some of these risks have been considered and efforts have been made to mitigate them — for example, through the training conducted by DHS and efforts to clarify what constitutes racial, ethnic, or religious profiling when deciding what information can be identified as suspicious activity and included in law enforcement databases. However, others, in particular the impact on local police's role with respect to communities, have not been sufficiently addressed. Finally, if local law enforcement is going to collect intelligence, it is critical to have in place robust oversight mechanisms to guard against abuses and ensure that those charged with oversight have the resources and expertise to carry out their mandate. These mechanisms must be developed because the federal government does not exercise direct control over local intelligence collection generally and fusion centers in particular, while states and localities are rarely attuned to the need for ongoing oversight.

“LAW ENFORCEMENT’S CORE VALUES
SHOULD BE PREDICATED ON THE CONSTITUTION,
THE BILL OF RIGHTS, CIVIL RIGHTS,
AND HUMAN RIGHTS...”

TRANSCRIPT OF REMARKS

The Honorable Leroy D. Baca
Sheriff
Los Angeles County Sheriff's Department

My points are relative to the intelligence matters that involve the nation and my local department.

We can't accomplish the goals of safety for all unless we fully understand the community we are serving. Los Angeles is unique. It is the epicenter of diversity because of our vast Asian population. We even surpass New York in terms of diversity.

We are involved with the FBI, the Joint Terrorism Task Forces, and the Los Angeles Police Department. The Sheriff's Department has deputy sheriffs who are federalized. They work in the federal system. They are managed by the federal authorities. But, at the next level, we deal with a joint regional intelligence center that former Los Angeles Police Chief William J. Bratton and I created. Basically, it deals with non-secret, non-classified open source forms of information.

For the most part, all criminal intelligence in Los Angeles County is shared across policing jurisdictions. Our theory is that the more we share information about traditional non-terrorism-related criminal activity, the more the idea that terrorism is a crime will permeate our investigative culture. So we are criminal-based intelligence gathering as opposed to any other definition of intelligence.

We only collect data on the criminal-related activities of individuals, organizations, and groups. The Los Angeles County Intelligence System, the joint regional intelligence center that we operate, has guidelines that strictly prohibit the collection of data regarding political, religious, or social views, associations or activities except as it relates to criminal activity. We — the Sheriff's Department and the regional intelligence center that we operate — rely on federal intelligence collection standards.

In other words, we follow the federal law on collection, analysis, storage, dissemination, and retention of intelligence products. As for oversight, the Sheriff's Department, of its own volition, has its intelligence system examined by the Institute for Intergovernmental Research, more commonly known as IIR. IIR is the federal

contract training group for federal law on intelligence collection. Our guidelines are reviewed by this organization. This group found no compliance issues when it evaluated our joint regional intelligence center.

Obviously, confidential materials must be maintained in a secure environment free from intrusion. However, the Sheriff's Department is also committed to transparency about how it does its job.

Every effort is made to ensure that collection, analysis, storage, and dissemination of information not only meets legal requirements, but community approval as well. Our focus is the criminal activities of gangs, organized crime, outlawed motorcycle gangs, narcotics groups, and terrorist groups. The information that we collect is shared with federal investigators, either in task forces, such as the FBI's joint terrorism task force, or in the joint regional intelligence center.

We participate in a local fusion center. Former Los Angeles Police Chief Bratton and I were the architects of this fusion center. We connect the all-crimes strategy within it. Our goal is to expand the center's reach from Southern California up to Las Vegas. We are also planning to connect the system laterally to all of Nevada and Arizona.

Since the data collection is for crime-related purposes, we want to make sure there is no conflict with federal agencies. We realize that the FBI is the lead investigative agency on terrorism. We have had very few instances where communities have objected to our intelligence gathering. Each Los Angeles Sheriff's Department case must have a criminal nexus to it. By staying within these guidelines, we are not taking a dragnet approach to particular communities.

The Sheriff's Department has a statutory mandate to locate, arrest, and incarcerate criminal offenders. It is all probable cause-based. There must be evidence. There must be a degree of substance.

We in law enforcement have to recognize who we are. Collecting information should only be done if there is a criminal nexus. It should be for that purpose and only that purpose. Law enforcement's core values should be predicated on the Constitution, the Bill of Rights, civil rights, and human rights. That is the culture of the Los Angeles County Sheriff's Department.

THE EXPANDING STATE AND LOCAL INTELLIGENCE ENTERPRISE AND THE THREAT TO CIVIL LIBERTIES

Michael German
Senior Policy Counsel
American Civil Liberties Union

INTRODUCTION

By their nature, all government intelligence operations pose a potential threat to civil liberties and democratic processes. The terrorist attacks of September 11, 2001, brought renewed interest in and attention to intelligence collection and information sharing as crucial components of national security. However, federal, state, and local law enforcement agencies have long claimed the authority to collect, analyze, and disseminate intelligence information. And too often, both in the past and in the present, they have used these powers in ways that violate the civil and political rights of Americans and undermine the rule of law. History shows that abuse increases whenever there is a perceived national security crisis or other threat to the existing social or political order. Curbing this abuse requires:

- strong guidelines that restrict the ability of law enforcement agencies to collect or disseminate personally identifiable information absent a legitimate law enforcement purpose and a reasonable factual basis to suspect the individual is involved in criminal activity;
- effective independent oversight of intelligence activity to ensure compliance with these guidelines; and
- public accountability to ensure members of the public know what intelligence systems exist and have reasonable access to this information to correct errors and redress abuse.

HISTORY OF ABUSE

The Senate Select Committee that investigated Cold War intelligence abuses by the Federal Bureau of Investigation (known as the “Church Committee” after its

chairman, Senator Frank Church) identified several characteristics of intelligence work that make it susceptible to abuse.¹ First, while the criminal justice system within which most law enforcement activity takes place incorporates procedural safeguards to protect individual rights and provide due process to those accused of wrongdoing, intelligence activities generally take place in secret, with little independent oversight and no opportunity for victims to defend themselves from improper or illegal government actions.

Second, the mission of intelligence work is often described in compelling but ambiguous terms that almost demand an overzealous approach. When “protecting national security” or “preventing terrorism” are the stated goals, intelligence agents tend to perceive restraint as recklessness in the face of catastrophic failure and independent oversight as a dangerous diversion from a critical mission. Traditional law enforcement methods exercised within constitutional boundaries are often perceived to be insufficient to such a critical task.² But, without clear guidelines limiting law enforcement intelligence activities and proper definitions for the terms used in describing these activities — the intelligence community cannot even agree on a definition of the term “intelligence”³ — there is a tendency toward mission creep. As a Church Committee witness explained:

“The risk was that you would get people who would be susceptible to political considerations as opposed to national security considerations, or would construe political considerations to be national security considerations, to move from the kid with a bomb to the kid with a picket sign, and from the kid with the picket sign to the kid with the bumper sticker of the opposing candidate.”⁴

So protecting national security from hostile foreign threats quickly leads to a search for a domestic threat from like-minded individuals or other “subversives” who would undermine the government from within or otherwise challenge the status quo, regardless of whether they used violence or any other illegal means. As the Supreme Court observed in *United States v. United States District Court (Keith)*, “History abundantly documents the tendency of Government — however benevolent and benign its motives — to view with suspicion those who most fervently dispute its policies.”⁵ Untethered from a criminal predicate, law enforcement officials working in intelligence soon begin to see themselves not just as enforcers of criminal laws, but as defenders of the existing social, moral, and political order.

Of course, abuses of intelligence powers have not been limited to federal law enforcement authorities. State and local police forces often maintained political intelligence units (sometimes called Anti-Subversive Squads, or Red Squads), which illegally spied upon and sabotaged a multitude of peaceful groups throughout the twentieth century, often based upon their First Amendment-protected beliefs,

associations, and activities.⁶ The “usual suspects” often included political “radicals” and “subversive agitators” such as trade unionists, civil rights activists, new immigrants, and racial and religious minorities.

Reforms initiated in the 1970s and '80s sought to limit such inappropriate intelligence activities by requiring a factual criminal predicate before police could gather, retain, or disseminate information about peoples' activities or associations. These included a federal regulation, 28 C.F.R. Part 23, which was designed to ensure that police intelligence operations are properly focused on illegal behavior by requiring that criminal intelligence systems receiving federal funds “collect information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.”⁷ The law also limits the dissemination of law enforcement intelligence to situations in which “there is a need to know and a right to know the information in the performance of a law enforcement activity.”⁸

Civil suits and public investigations regarding illegal police intelligence activities in many jurisdictions across the country, including New York City, Memphis, Seattle, Chicago, and Los Angeles, led to injunctions, settlements, consent decrees, and statutory limitations that all but banned police monitoring of political activities or other intelligence collection unless it was directly related to criminal activity.⁹ While law enforcement agencies bristled at these restrictions, and sometimes secretly violated them, they remained in place and the “reasonable suspicion of criminal activity” standard of 28 C.F.R. Part 23 became widely accepted within the law enforcement community.¹⁰

POST 9/11 CHANGES IN ATTITUDE AND ARCHITECTURE

The terrorist attacks of September 11, 2001, and the military actions that followed, created a national security emergency that fueled a reevaluation of the limits placed on intelligence collection within the federal government especially, but also on state and local law enforcement. Even though all of the conditions the Church Committee identified as conducive to abuse were readily apparent, many law enforcement agencies eagerly renewed intelligence programs with little regard for the historical warnings.

Even before 9/11, state and local law enforcement agencies had begun moving away from traditional criminal justice methods when dealing with political activists. During political demonstrations in 2000 and 2001, the Metropolitan Police Department in Washington, D.C., engaged in undercover infiltration of political advocacy organizations, unnecessary violence against peaceful protesters and hundreds of preemptive arrests to prevent demonstrations.¹¹ The public outrage led the D.C. City Council to protect demonstrators' First Amendment rights by passing legislation that regulated how the police train for, investigate, and manage public demonstrations, and required individualized probable cause to arrest protesters

involved in illegal activity. After 9/11, however, and despite the condemnation of the unlawful police tactics used in Washington, D.C., surveillance and infiltration of advocacy organizations and preemptive arrests became the methods of choice during protests in Miami in 2003,¹² New York in 2004,¹³ and Minneapolis in 2008.¹⁴

And state and local law enforcement also returned to the intelligence game in a major way. A concept called “Intelligence Led Policing” (ILP), developed in the United Kingdom in the late 1990s, became popular within U.S. law enforcement circles, though the definition of “intelligence” remained obscure.¹⁵ ILP has been described as the gathering and analysis of “intelligence” in the pursuit of proactive strategies “geared toward crime control and quality of life issues.”¹⁶ Another law enforcement official described ILP as policing that is “robust enough” to resist “terrorism as well as crime and disorder.”¹⁷

While state and local police had long participated in federal anti-terrorism programs, such as the FBI’s Joint Terrorism Task Forces (JTTF), after 9/11 they also created their own multi-jurisdictional intelligence centers, which soon became known as intelligence fusion centers.¹⁸ Despite the strictures of federal regulations (28 CFR Part 23), the federal government encouraged this expansion of the state and local police mission beyond criminal law enforcement by contributing financial resources, personnel and guidance.

FUSION CENTERS

Intelligence fusion centers grew in popularity among state and local law enforcement as those authorities sought to establish a role in defending homeland security by developing their own intelligence capabilities. These centers evolved largely independent of one another, beginning in about 2003, and were individually tailored to meet local and regional needs. In addition to federal, state, and local law enforcement, fusion centers often included emergency response agencies, military and National Guard troops, and even private companies. Today, more than seventy-two fusion centers operate around the country with funding from the Department of Homeland Security (DHS), the Department of Justice (DOJ), and state and local law enforcement agencies.

In 2006, DHS and DOJ teamed up to produce voluntary guidelines that outlined the federal government’s vision for fusion centers, and sought to encourage and systematize their growth. The guidelines encouraged fusion centers to broaden their sources of information “beyond criminal intelligence, to include federal intelligence as well as public and private sector data.”¹⁹ Indeed, rather than feel restricted by federal intelligence collection regulations, Delaware State Police Captain Bill Harris, head of the Delaware Information Analysis Center (DIAC), appeared to feel constrained only by resources: “I don’t want to say it’s unlimited, but the ceiling is very high. . . . When we have the money, we’ll start going to those other agencies and say, ‘Are you willing to share that database and what would it cost.’”²⁰

The growth of fusion centers took place in the absence of any legal framework for regulating their activities, which quickly led to mission creep. Fusion centers originally justified as anti-terrorism initiatives rapidly drifted toward an “all crimes and/or all-hazards” approach “flexible enough for use in all emergencies.”²¹

In November 2007, the American Civil Liberties Union issued its first report on fusion centers, warning that these rapidly developing domestic intelligence operations put Americans’ privacy and civil liberties at risk. While all fusion centers are different, we identified five overarching problems that, left unchecked, could lead to abuse:

1. **Ambiguous Lines of Authority.** In a multi-jurisdictional environment it is unclear what rules apply and which agency is ultimately responsible for the activities of fusion center participants.
2. **Private Sector Participation.** Some fusion centers incorporate private-sector corporations into the intelligence process, potentially undermining laws designed to protect the privacy of innocent Americans, and increasing the risk of a data breach.
3. **Military Participation.** Some fusion centers include military personnel in law enforcement activities in troubling ways.
4. **Data Mining.** Federal fusion center guidelines encourage wholesale data collection and data manipulation processes that threaten privacy.
5. **Excessive Secrecy.** Fusion centers, like all intelligence operations, are characterized by excessive secrecy, which limits public oversight and undermines their ability to fulfill their stated mission by impairing access to essential information from other equally secretive fusion centers, bringing the ultimate value of the fusion center network into doubt.

Moreover, there are serious questions about whether data fusion is an effective means of preventing terrorism in the first place, and whether funding the development of these centers is a wise investment of finite public safety resources.

SUSPICIOUS ACTIVITY REPORTING PROGRAMS

In January 2008 the Office of the Director of National Intelligence (ODNI) Information Sharing Environment (ISE) Program Manager published functional standards for state and local law enforcement officers to report ‘suspicious’ activities to fusion centers and the ISE.²² The behaviors described as inherently suspicious and related to terrorism included such innocuous activities as photography, acquisition of expertise, and eliciting information. This began a proliferation of “suspicious activity reporting” (SAR) programs that encourage law enforcement officers, intelligence and homeland security officials, emergency responders, and even the public to report

the “suspicious” activities of their neighbors to law enforcement and intelligence agencies.²³ The Los Angeles Police Department, for example, issued a special order that stated the policy of the LAPD to “gather, record, and analyze information, of a criminal or non-criminal nature, that could indicate activity or intention related to either foreign or domestic terrorism.”²⁴ That report included a list of sixty-five behaviors that LAPD officers are required to report, including using binoculars, taking pictures or video footage “with no apparent aesthetic value,” drawing diagrams, taking notes, and espousing extremist views.²⁵ The FBI created its own SAR program called eGuardian, which was redundant to the ISE and contained looser standards.

The problem is that many of the behaviors these SAR programs identify as precursors to terrorism include benign activities like taking pictures, drawing diagrams and taking notes, which are so commonplace they could easily be used as proxy justifications for police stops based on race or other prohibited factors where there is no reasonable basis for suspicion of wrongdoing.²⁶ SAR programs also increase the probability that innocent people will be stopped by police and have their personal information collected for inclusion in law enforcement and intelligence data bases.

With new intelligence sharing systems like fusion centers and the DNI’s ISE and the FBI’s eGuardian program, information improperly collected by local police in any city or small town in America can now quickly end up in federal law enforcement and intelligence databases.

LACK OF TRAINING AND THE EROSION OF REASONABLE STANDARDS

While state and local law enforcement agencies eagerly initiated intelligence operations and analysis programs, few had any real training in counterterrorism or intelligence analysis. Recent reports indicate that many of the counterterrorism training programs that state and local law enforcement officers attend are taught by unqualified instructors who express politically-biased and racist positions. Political Research Associates (PRA) evaluated several prominent counterterrorism training programs and instructors across the country.²⁷ The investigation found that many counterterrorism instructors express anti-Muslim opinions that claim Islam is a terrorist religion and that Muslims represent a terrorist “Fifth Column” within the United States.²⁸ PRA found that these training programs serve to increase racism against Muslims and impede law enforcement efforts to protect national security by providing poor guidance on what constitutes a legitimate threat, and undermining the relationship between law enforcement and the Muslim community in America.

Washington Monthly also reported on a three-day counterterrorism training given to local law enforcement officers in Florida. The instructor professed to teach the law enforcement officers about the “fundamentals of Islam,” but instead told them that any Muslim wearing a headband wants to be a martyr, if a Muslim’s lips are moving it means he is praying, and that terrorists are known for wearing mustaches and beards.²⁹ He reportedly stated that if a person pulled over in a traffic stop has a

Muslim name on his or her driver's license, it constitutes probable cause for an arrest.

Unfortunately, there is no effective accreditation process for counterterrorism instructors, no consistent standards for quality or veracity for counterterrorist training programs, and no legitimate peer review process.³⁰ Some of the instructors at these trainings have no law enforcement, military, or counterterrorism experience at all.³¹ Despite this, many of these trainings are not only subsidized by state and federal governments, they are also endorsed by DHS.³²

The Proliferation of Discredited “Radicalization” Theories

Federal, state, and local law enforcement agencies have also promoted unsubstantiated and largely discredited theories that individuals who become terrorists pass through a discernible “radicalization” process. This concept was popularized by a 2007 New York Police Department (NYPD) report, *Radicalization in the West: The Homegrown Threat*, which purported to identify a four-step radicalization process through which terrorists progress.³³ What is dangerous about the report is that each step involves constitutionally-protected religious and associational conduct, and the authors ignore the fact that millions of people may progress through one, several, or all of these stages and never commit an act of violence.

The NYPD report drew quick condemnation from the civil liberties and Muslim communities. The Brennan Center for Justice issued a memo complaining of the report’s “foreseeable stigmatizing effect, and its inferential but unavoidable advocacy of racial and religious profiling.”³⁴ New York City Muslim and Arab community leaders formed a coalition in response to the NYPD report and issued a detailed analysis criticizing the NYPD for wrongfully “positing a direct, causal relation between Islam and terrorism such that expressions of faith are equated with signs of danger” and potentially putting millions of Muslims at risk.³⁵ Unfairly focusing suspicion on a vulnerable community also threatens to create the very alienation that effective and proper counterterrorism policies should seek to avoid.³⁶

Indeed, contrary to the NYPD study, a 2008 analysis by the United Kingdom’s domestic intelligence service, MI5, which was based on hundreds of case studies of individuals involved in terrorism, concluded that there is no single identifiable pathway to extremist violence. It further concluded that religiosity is not a reliable indicator of terrorist behavior because “a large number of those involved in terrorism do not practice their faith regularly.”³⁷ The MI5 study concluded that the British government should support tolerance of diversity and protection of civil liberties, conclusions that were echoed in a National Counterterrorism Center (NCTC) paper published in August 2008. In exploring why there was less violent homegrown extremism in the United States than the United Kingdom, the NCTC paper authors cited the diversity of American communities and the greater protection of civil rights as key factors.³⁸

The significant shortcomings with the NYPD's report became so evident that the Department was compelled to insert a "Statement of Clarification" in 2009 that explained:

"NYPD understands that it is a tiny minority of Muslims who subscribe to Al Qaeda's ideology of war and terror and that the NYPD's focus on Al Qaeda inspired terrorism should not be mistaken for any implicit or explicit justification for racial, religious or ethnic profiling. Rather, the Muslim community in New York City is our ally and has as much to lose, if not more, than other New Yorkers if individuals commit acts of violence (falsely) in the name of their religion. As such, the NYPD report should not be read to characterize Muslims as intrinsically dangerous or intrinsically linked to terrorism, and that it cannot be a license for racial, religious, or ethnic profiling."³⁹

More important, the statement of clarification said, "This report was not intended to be policy prescriptive for law enforcement."⁴⁰

Unfortunately, the NYPD failed to retract the report altogether and inserted the clarification without public announcement, so it received little publicity.⁴¹ As a result, the NYPD report is still being referenced uncritically in academic and official government publications. A report by the Senate Homeland Security and Governmental Affairs Committee entitled *Violent Islamist Extremism, The Internet, and the Homegrown Terrorism Threat* ignored the criticisms and flaws of the NYPD report and simply restated the NYPD's flawed "radicalization" theories in arguing for a national strategy "to counter the influence of the Ideology."⁴²

EVIDENCE OF ABUSE

Given the secrecy of police intelligence activities, it is impossible to know the true extent of abuse of these new or reclaimed authorities, but the ACLU has documented surveillance or obstruction of First Amendment activities by federal, state, and local law enforcement in thirty-three states and the District of Columbia.⁴³ This abuse takes three forms: the improper targeting and collection of personal information of innocent individuals, the improper analysis of information, and the improper use and dissemination of that information.

Improper Targeting and Collection of Personal Information of Innocent Individuals

In 2008, the ACLU of Maryland exposed an extensive Maryland State Police (MSP) spying operation that targeted at least twenty-three non-violent political advocacy organizations based solely on the exercise of their members' First Amendment rights.⁴⁴ The MSP surveillance activities were aimed at an array of

political and religious organizations, including peace advocates like the American Friends Service Committee (a Quaker organization) and Women in Black (a group of women who dress in black and stand in silent vigil against war), immigrants rights groups like CASA of Maryland, human rights groups like Amnesty International, anti-death penalty advocates like the Maryland Citizens Against State Executions, and gay rights groups like Equality Maryland, among others. None of the MSP reports from these operations suggested any factual basis to suspect these groups posed any threat to security. Not surprisingly, no criminal activity was discovered during these investigations, some of which lasted as long as fourteen months. Despite this lack of evidence, the MSP labeled many of these activists “terrorists,” distributed information gathered in their investigations widely among Maryland law enforcement and intelligence agencies — including a local police representative of the FBI’s Joint Terrorism Task Force, a National Security Agency security official, and an unnamed military intelligence officer — and uploaded the activists’ personal information into a federal drug enforcement and terrorism database.⁴⁵

In Colorado, the FBI JTTF and local police recorded and shared the names and license plate numbers of environmental activists at a peaceful demonstration.⁴⁶ In California, Sheriff’s Homeland Security Unit Officers infiltrated union demonstrations against Safeway supermarkets.⁴⁷ In Minnesota, the weekend before the Republican National Convention, Ramsey County Sheriff’s deputies and St. Paul police conducted preemptive raids against a video journalist group, I-Witness, whose documentation of police misconduct during the 2004 Republican National Convention was instrumental in overturning criminal charges against protesters. Police also conducted several other raids, apparently in coordination with the FBI, and made preemptive arrests of people planning to protest at the convention.⁴⁸ These are just a few examples.

In addition to unconstitutional surveillance of protest groups, the proliferation of SAR programs could be partly to blame for recent abuses of First Amendment rights regarding photography and videography. For example, in New York police illegally detained a Muslim-American journalism student for taking photographs of flags for a class assignment, copied her driver’s license, and deleted the photographs.⁴⁹ Police in Washington detained an artist and Associate Professor of Fine Art at the University of Washington for taking pictures of power lines.⁵⁰ She was frisked, handcuffed, and placed in the back of the police car, and warned that she would be contacted by the FBI about the incident. Police in New Jersey illegally detained, handcuffed, and searched Khalia Fitchette, a high school honors student, for taking a picture on a public bus.⁵¹ The ACLU of New Jersey is currently representing Ms. Fitchette in a suit against the Newark Police Department. A California fusion center analysis of FBI eGuardian threat reports for August 2009 confirms that “suspicious photography” accounted for a substantial share of SAR reporting, exceeded only by “suspicious vehicles.”⁵²

SAR programs also contribute to abuses regarding the free exercise of religion. They encourage citizens to engage in hyper-vigilant reporting of religious activities to police that they deem “suspicious.” In Chicago, state and local police, in conjunction

with a JTTF, engaged in a three-day manhunt for a Muslim man whom civilians reported as acting suspiciously when he used a hand counter to keep track of his daily prayers.⁵³ There have also been instances where civilians report suspicious activity, and those complaints are the basis for restricting the exercise of First Amendment activities. One recent example occurred on a flight to Los Angeles where passengers reported “suspicious” activity to the flight crew when three Orthodox Jews engaged in a prayer ritual. The men were escorted off the plane upon landing, detained, and questioned before being released.⁵⁴

Racial profiling results in another form of improper intelligence collection. The New York Civil Liberties Union obtained “stop and frisk” data from the NYPD that revealed that almost 9 out of 10 of the nearly 3 million people it stopped since 2004 were non-white.⁵⁵ And though the NYPD should have been using the reasonable suspicion standard required under *Terry v. Ohio*,⁵⁶ only about 10 percent of those stopped by the NYPD actually received summonses or were arrested.⁵⁷ In fact, in 2010, the NYPD reported a 3.5 percent rise in street stops in response to increased suspicious activity reporting, bringing the total number of stops to 601,055, with only 7 percent of the stops resulting in an arrest.⁵⁸ Yet the NYPD collected and retained the personal information of the innocent people it stopped in its intelligence databases, along with the guilty.⁵⁹ In effect, NYPD was creating a massive database of innocent people of color in New York City. Such racial disparities in stop and frisk data should be a warning to police departments implementing new SAR programs.

Improper Analysis of Information

The lack of standards and training in intelligence analysis has contributed to a number of factually erroneous and abusive fusion center reports. For example, the North Central Texas Fusion Center distributed a Prevention Awareness Bulletin that warned of a conspiracy between Muslim civil rights groups, lobbyists, anti-war organizations, hip hop bands, former Attorney General Ramsey Clark, former Rep. Cynthia McKinney, and the Department of Treasury, to push an “aggressive, pro-Islam agenda” and impose Shariah law in the United States.⁶⁰ A Virginia Fusion Center report identified state universities and historically black colleges as “nodes of radicalization” and went on to make the dubious claim that more than 50 different “terrorist and extremist” groups are actively operating in Virginia.⁶¹ Additionally, a Missouri Fusion Center strategic report on right-wing extremism claimed that supporters of Rep. Ron Paul could be members of anti-government militias,⁶² and a DHS analyst at a Wisconsin fusion center prepared a report about protesters on both sides of the abortion debate, despite the fact that no violence was expected.⁶³ Lastly, a Tennessee fusion center listed an ACLU letter to school superintendants urging schools to be respectful of all religious beliefs on its website’s map that highlighted “Terrorism Events and Other Suspicious Activity.”⁶⁴

Improper Use and Dissemination of Intelligence

Another significant form of abuse that has come to light as a result of state and local law enforcement intelligence gathering practices is the improper use and dissemination of that information. First, personal information stored on state databases is not always properly secured. An audit of the Massachusetts criminal records database revealed that police officers, court officers, probation officers or court employees improperly conducted hundreds of criminal record searches on celebrities such as actor Matt Damon and football player Tom Brady.⁶⁵

Abuse has also occurred when states have engaged in spying on political activists and fed that information to special interests. For example, ProPublica uncovered documents that revealed the Pennsylvania Office of Homeland Security (OHS) “has been gathering information on the peaceful political activities of environmental activists opposed to a controversial form of gas drilling called hydraulic fracturing, or ‘fracking.’” In addition, the documents suggest the Pennsylvania OHS was actively taking sides in the political dispute between environmentalists and drilling companies. According to the ProPublica documents, a private contractor was hired by the Pennsylvania OHS to supply anti-terrorism bulletins. These bulletins included overseas not only intelligence about possible new plots — but also items listing public meetings that anti-drilling activists planned to attend.⁶⁶

Another example of improper use of intelligence information is in the now infamous LACTEW scandal. *The San Diego Union-Tribune* exposed a scandal linking a police task force called the Los Angeles County Terrorism Early Warning Center (LACTEW) to an intelligence fiasco that can only be described as a “perfect storm” of the problems identified in the ACLU’s November 2007 fusion center report.⁶⁷ LACTEW, established in 1996, was described as the first fusion center and was recommended as a model for others.⁶⁸ The investigation exposed that a group of military reservists and law enforcement officers led by the co-founder of the LACTEW engaged in a years-long conspiracy to steal — and possibly share with private intelligence companies — highly classified intelligence files from the Strategic Technical Operations Center (STOC) located at the U.S. Marine Corps Base at Camp Pendleton, California, and secret surveillance reports from the U.S. Northern Command headquarters in Colorado Springs, Colorado. Some of the stolen files “pertained to surveillance of Muslim communities in Southern California,” including mosques in Los Angeles and San Diego, and revealed “a federal surveillance program targeting Muslim groups” in the United States. The conspiracy was uncovered when military personnel investigating a theft of Iraq war booty discovered a cache of highly classified documents in a Manassas, Virginia, storage locker. The LACTEW scandal is a prime example of the combination of overzealous intelligence collection and inadequate oversight leading to “an intelligence nightmare.”⁶⁹

It was also a civil liberties nightmare. Targeting religious groups for surveillance violates their First Amendment rights and exposes them to discriminatory enforcement. Broadly sharing the information collected with the military and private companies, and failing to protect it from unauthorized use, multiplies these violations and damages public trust in law enforcement.

CONCLUSION

History makes clear that without adequate training and sufficient standards to protect individuals' privacy and civil liberties, state and local police intelligence activities will not keep us safe and will only result in significant abuse of First and Fourth Amendment rights of innocent persons. The increase in law enforcement intelligence operations and the proliferation of fusion centers and SAR programs have predictably resulted in inappropriate and biased targeting of individuals and organizations for surveillance, improper collection of personal information, and flawed intelligence reporting. Restoring reasonable standards requiring a criminal predicate to justify intelligence activities and imposing effective oversight and public accountability will not cripple effective law enforcement, but instead will enhance it.

“THE DEPARTMENT OF HOMELAND SECURITY HAS
A RESPONSIBILITY ... TO CONTRIBUTE TO A ROBUST
INFORMATION SHARING ENVIRONMENT...”

TRANSCRIPT OF REMARKS

Kara Dansky
Senior Counsel

Center for Justice, American Civil Liberties Union

*Former Section Lead, Impact Assessment Section
Office for Civil Rights and Civil Liberties
U.S. Department of Homeland Security*

The Department of Homeland Security (DHS) has a responsibility that is consistent with the vision of Congress and the direction of the President to contribute to a robust information sharing environment. Consequently, DHS has focused on getting resources and information out of Washington and into the hands of state and local law enforcement to help combat threats in their communities.

Within DHS, I work at the Office for Civil Rights and Civil Liberties, which is commonly referred to as CRCL. CRCL is responsible for helping shape policy and practices that respect civil rights and civil liberties by evaluating and advising on a wide range of technical, legal, and policy issues across DHS programs and activities.

What I do specifically at CRCL is conduct civil rights and civil liberties impact assessments, which my office sometimes does at the direction of Congress, sometimes at the request of the Secretary, and sometimes at the discretion of my boss, Margo Schlanger, who is the Officer for Civil Rights and Civil Liberties.¹

We also investigate and resolve complaints filed by the public regarding DHS policies and actions, provide leadership for DHS’s equal employment opportunity programs, and engage with the public to ensure that ethnic and religious communities both understand DHS policies and procedures and are empowered to express concerns and seek information from DHS officials.

I want to offer some specifics about how we are involved in this effort. One of our major responsibilities is intelligence product oversight. We oversee the intelligence products for dissemination to state, local, and tribal law enforcement while enabling these products to be released in a timely fashion.

In particular, this means we review products and intelligence reports to ensure they do not describe incidents of actual or perceived racial or ethnic profiling, violations of constitutional rights, or other civil rights and civil liberties issues. For example, we work to ensure that the intelligence products the Department disseminates from the Office of Intelligence and Analysis do not attribute the bad actions of an individual to a group to which they belong or, likewise, attribute the actions of a group to an individual associated with that group who was not a participant in the actions.

I also want to say something about the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI). DHS works very closely with the program manager for the information-sharing environment and with the Justice Department on NSI. NSI is a partnership among local, state, tribal, and federal agencies for the purpose of sharing terrorism-related information.

The NSI is a tool for local law enforcement to connect the dots, to combat crime and terrorism by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing suspicious activity reports in a manner that rigorously protects the privacy and civil liberties of Americans. DHS has worked extensively with its interagency partners to develop a system for this nationwide initiative, including a functional standard for NSI reporting that has received approval from civil rights and civil liberties advocates and organizations.

In addition, what is called Functional Standard 1.5, which governs what information can be shared as part of the nationwide SAR initiative, states that only information reasonably indicative of terrorism-related crime can be part of the NSI shared space. In addition, we train frontline personnel on behaviors and actions associated with terrorism-related crime. We also implement an extensive review and vetting process for all suspicious activity reporting.

Specifically, this means that the information reported under the NSI must be reasonably indicative of terrorism-related crime before it is made available to other law enforcement entities. We also ensure that privacy, civil rights, and civil liberties policies are in place, which means establishing a clear and specific auditing and redress process. DHS also recognizes that information sharing cannot be confined to only the government, but requires public involvement.

To that end, DHS has licensed a very simple campaign first initiated here in New York. The “If You See Something, Say Something” campaign is designed to raise public awareness of potential behavioral indicators of terrorism and crime.

“If You See Something, Say Something” emphasizes the importance of reporting suspicious activity to proper law enforcement authorities. The campaign is not unlike the longstanding neighborhood watch programs that have been in place across the nation. “If You See Something, Say Something” alerts the public to the usefulness of observing and reporting potential criminal activity in their neighborhoods. The campaign takes a behavior-focused approach to identifying suspicious activity. Factors such as race, ethnicity, national origin, and religious

affiliation should not be considered to create suspicion, unless those attributes are used as part of a specific suspect description.

The public should be reporting on potential unlawful actions rather than beliefs, thoughts, ideas, expressions, associations, or speech unrelated to terrorism or other criminal activity. DHS is very involved in articulating these standards to the public.

Over the past year, DHS has expanded the “If You See Something, Say Something” campaign across the U.S., through partnerships with Wal-Mart, Mall of America, the American Hotel and Lodging Association, Amtrak, the Washington Metropolitan Area Transit Authority, the General Aviation Industry, the NFL, the NBA, the NCAA, and state and local fusion centers.

I want to address the fusion centers themselves and specifically the training that CRCL offers to fusion center analysts and staff.

As we all know, fusion centers are operated by state, local, and tribal entities. And because they are locally run and operated, there is no nationwide standard organizational model. Virtually all have missions that extend beyond anti-terrorism and characterize their scope of activities as all crimes. A majority of the staff are drawn from local law enforcement. Many centers also have fire service personnel, emergency managers, public health officials, private sector liaisons, and other civil personnel, and some have expanded their mission to all crimes and all hazards.

There are 72 centers recognized by governors in each state as primary points of contact, including 20 urban area security initiative locations in major cities such as Los Angeles.² It is a requirement for receiving DHS funding that all fusion centers have in place by the end of this month a privacy policy that is no less protective than the information-sharing guidelines.

Through a push of the DHS privacy office, 69 of the fusion centers currently have such a policy and we expect all operational fusion centers to have privacy policies in place by the end of this month.³ CRCL is acutely concerned with potential civil rights and civil liberties problems in the collection of intelligence by state and local law enforcement.

As I have mentioned, CRCL conducts training for many fusion centers. Our CRCL training is provided to all DHS officers or intelligence analysts before they deploy to fusion centers. Since 2009, CRCL staff has provided intensive training to nearly 850 staff from 26 fusion centers in 17 states. We have also trained the privacy civil liberties officers at 66 fusion centers to deliver their own privacy civil rights and civil liberties training to local fusion center staff.

We provide technical assistance, including a joint website with the Justice Department, to support these in-house fusion center training programs. Our goal is to train all privacy civil rights officers and enable continuous training on civil rights, civil liberties, and privacy issues to local fusion center staff. Generally, our training covers how to handle reports of these protected activities such as protests, exercise of religious freedom, freedom of association, the capture and retention of video feeds that have identified persons on tape, and the use of materially inaccurate or misleading

information. Our training discourages the targeting of communities based on the use of overly-broad demographic information and the collection of information on individuals that perpetuates any racial or ethnic stereotypes. We discuss the usefulness of community engagement to provide a level of government transparency, and encourage fusion centers to have in place sufficient redress mechanisms.

We also offer training on 28 C.F.R. Part 23 and guidance on multi-jurisdictional criminal intelligence systems.

AMERICAN POLICING AND THE INTERIOR DIMENSION OF COUNTERTERRORISM STRATEGY

Matthew Waxman

Professor of Law, Columbia University

Adjunct Senior Fellow, Council on Foreign Relations

Member of the Hoover Institution Task Force on National Security and Law

INTRODUCTION

In his book, *In the Shadow of the Garrison State*,¹ Aaron Friedberg examined what he referred to as “the interior dimension of American grand strategy” during the Cold War — that is, the shape, size, and composition of the domestic institutions and mechanisms through which the United States built and wielded power against the Soviet empire.² Similar to the recent alarm among some scholars about the extended state of emergency brought on by the 9/11 attacks,³ Harold Laswell and others had predicted in influential writings during the Second World War and early Cold War that a permanent state of national security crisis combined with massive investments in defense would dramatically erode freedoms and turn the United States into a “garrison state.”⁴ In explaining why that conversion never materialized, Friedberg argued that the forces Laswell and others feared were counterbalanced by opposing, anti-statist pressures in American politics and within American institutions. Not only did those pressures against expansions in government power help prevent the imposition of a garrison state, claimed Friedberg, but the resulting equilibrium helped win the Cold War over the long term: “By preventing some of the worst, most stifling excesses of statism, these countervailing tendencies made it easier for the United States to preserve its economic vitality and technological dynamism, [and] to maintain domestic political support for a protracted strategic competition...”⁵

As Cold War success had much to do with military and economic power, counterterrorism success in the post-9/11 world has much to do with information. And like the Cold War strive for power, the strive for more potent information gathering and analysis must be checked and meshed with other imperatives of policy and principle not only for their own sake but because too much or unrestrained government intrusion and surveillance would be counterproductive from a security standpoint.

Most recent legal scholarship and commentary about what, in Friedberg's terms, might be called "the interior dimension of American counterterrorism strategy" has focused on institutional features and macro-structural design at the *federal* level, including the realignment of federal departments and agencies and the relationships among the federal branches of government in exercising and regulating counterterrorism powers. This essay argues that another important interior axis of counterterrorism strategy is centralization versus localism, and especially the degree to which information and intelligence law and policy is driven by the federal government and national-level institutions versus by local governments and institutions.⁶

More specifically, this essay argues that a unique feature of American counterterrorism structural design is the very widely dispersed local control of some counterterrorism intelligence resources and institutions — a localized fragmentation of government power, the resilience of which has proven quite strong despite intense post-9/11 counterpressures and an historical pattern of institutional centralization in democracies during security crises. Whereas other essays in this volume focus on the impact of counterterrorism efforts on law and rights, this essay examines some of the possible strategic merits and drawbacks of intelligence localization, and it concludes with some observations about the future.

TERRORISM, INTELLIGENCE, AND THE LOCALIZATION OF AMERICAN POLICING

A major lesson of the September 11 attacks was the government's need to better collect, share, and analyze information. According to RAND intelligence expert and former Vice Chairman of the National Intelligence Council Gregory Trevorton: "The onset of an age of terror has highlighted the role of intelligence services in detecting and preventing possible terrorist acts."⁷ "If prevention is the name of the game," he continues, "the pressure on intelligence is extraordinary."⁸ The 9/11 Commission concluded that "[a] 'smart' government would *integrate* all sources of information to see the enemy as a whole."⁹ Many of the informational "dots" comprising the September 11 plot sequence had occurred and had been detected by someone, somewhere, at some level of government in the United States; others should have been seen and passed on, but were missed. Perhaps, it followed, the attacks could have been averted with better systems and policies to discern, analyze, assemble and act on such "dots" throughout the country, ultimately uncovering patterns and the plot.¹⁰

In addressing these post-9/11 intelligence challenges, the United States faced a particular constraint, though, in that so much of the government's capacity for these tasks — especially in terms of manpower — resides at the local level. Unlike democracies such as Israel that have national police forces,¹¹ or Britain and Germany that have regional police forces but high degrees of uniformity among just a few dozen such agencies,¹² policing and law enforcement in the United States — and therefore much of the natural capacity for domestic intelligence — is highly localized and heterogeneous. American police forces are mostly locally drawn and

locally controlled, and policing scholars generally regard the U.S. system as the most fragmented in the industrialized world.¹³

Numbers and counting methods vary, but most surveys estimate that there are more than 15,000 state and local law enforcement agencies throughout the United States, comprised of about 700,000 officers.¹⁴ Even before 9/11, these agencies and officers conducted many activities that could contribute directly or indirectly to counterterrorism intelligence, including routine patrolling, recording suspicious activities, collecting and sharing law enforcement and other data, community engagement, and infrastructure protection.¹⁵ Historically, the U.S. system of localized policing, in which these counterterrorism duties form just a small part and are often indistinguishable from other policing duties, has been resistant to any calls for centralization or consolidation, among other reasons because of a deeply entrenched American political culture favoring highly devolved law enforcement authority and because state and local governments and political leaders have such strong interest in retaining control over those instruments.¹⁶

Democracies often tend to centralize their domestic security functions in response to major terrorism threats, though.¹⁷ As Oren Gross and Fionnuala Ní Aoláin write in their volume on emergency powers in times of crisis, “Concepts such as separation of powers and federalism are likely to be among the first casualties when a nation needs to respond to a national emergency.”¹⁸ Looking to the past and across countries, they note that “in federal states one of the first ‘victims’ of exigencies and crises is the principle of federalism.”¹⁹ Against that historical backdrop, the high fragmentation of American policing might be viewed as a liability from a counterterrorism perspective, or it might have been expected to give way to irresistible unification pressures after 9/11. After all, terrorist networks and activities tend to span geographic areas — and therefore legal jurisdictions — thus severely complicating the challenges of sharing information and coordinating preventive activities within an institutionally fragmented system.²⁰

Faced with vast new intelligence demands after the 2001 Al Qaeda attacks, one option was for the U.S. federal government to expand dramatically its national-level, domestic intelligence bureaucracy and capabilities.²¹ The federal government did so in some major ways. Among other things, the FBI underwent structural realignment and expanded resources and legal authorities directed toward domestic intelligence,²² including shifting its priorities and allocation of personnel toward intelligence and terrorism prevention²³ and revising its guidelines for initiating inquiries and conducting investigations.²⁴ The new Department of Homeland Security, which Congress created in 2003, includes an Office of Intelligence and Analysis responsible for collection, analysis, and dissemination of domestic security threat information.²⁵ And the Intelligence Reform and Terrorism Prevention Act of 2004 established the Office of the Director of National Intelligence and the National Counterterrorism Center to coordinate intelligence activities among government departments and agencies.²⁶

Notably, though, the federal government resisted calls among some lawmakers and experts after 9/11 to even further centralize and consolidate domestic intelligence capabilities and efforts by creating a new federal domestic intelligence agency, perhaps modeled on the United Kingdom's MI5.²⁷ The 9/11 Commission strongly opposed the idea of creating a new domestic intelligence agency, proposing instead measures and coordination bodies to improve capabilities within and among existing agencies, including the thousands of state and local agencies that make up the vast bulk of American policing and law enforcement.²⁸ Congress has so far agreed with that approach, and the 2007 amendments to the Intelligence Reform and Terrorism Prevention Act require the President to take action to facilitate sharing of terrorism-related information among federal, state, and local entities.²⁹ In 2008, the Office of the Director of National Intelligence published its information sharing strategy, declaring “the imperative need of moving beyond considering State and local government to be only ‘first responders,’ preferring instead to thinking of them as the first line of defense in a very deep line of information assets.”³⁰

Besides expanding and consolidating capabilities in a dedicated domestic intelligence agency, another centralizing option after 9/11 was for the federal government to assume stronger, more formal control over state and local agencies and agents. Again, to some degree the government did so, but not in radical ways. The federal government was probably precluded constitutionally by the anti-commandeering doctrine articulated in *Printz v. New York* from directly conscripting local government agents into its own federal domestic intelligence programs.³¹ Although it might have been plausible for the federal government to challenge the anti-commandeering doctrine as inapplicable in defending against sufficiently grave national security threats — indeed, Justice Stevens argued in his *Printz* dissent the doctrine should be more flexible in national security or emergency contexts³² — the federal government instead used other familiar tools to exert influence over state and local police agencies and to induce alignment of their activities with federal initiatives.³³ These tools include information sharing arrangements, financial grants, and training programs designed to help bolster and coordinate local capabilities fielded and controlled by state, county, and city governments.

Although some observers and critics of these programs predicted that they would produce *de facto* a monolithic, nationalized intelligence bureaucracy because state and local governments would fall in behind or take their cues from the federal government,³⁴ localism with respect to intelligence law and policy has remained quite resilient. The structural architecture of U.S. domestic intelligence reflects — at least for now — something of equilibrium between centralization and localism.

On the one hand, the federal government is undeniably the dominant player in domestic intelligence, for reasons starting with the massive resources and bureaucracy it brings to bear (though one should be careful to note that the federal bureaucracy is not always itself tightly centralized; it has its own fragmentation among many intelligence entities and security components — such as those dedicated to criminal

investigation, border protection, immigration enforcement — with counterterrorism responsibilities). The federal government also exerts some central control by conditioning law enforcement and homeland security grants on compliance with federal policies and standards, and it exercises operational control over most major suspected terrorism investigations through FBI-led Joint Terrorism Task Forces, to which state and local law enforcement agencies contribute personnel, information, and other resources.³⁵

Alongside these elements of top-down, centralized control of counterterrorism efforts, however, one also sees patterns of legal diversity and policy independence and pushback. With respect to counterterrorism intelligence law, for example, municipal police departments' investigatory powers are limited by varying state laws and locally-set administrative guidelines that vary in their stringency.³⁶ Those investigatory powers are overseen by an assortment of institutional mechanisms, including state and local legislatures, agency oversight boards, external audits, and courts.³⁷ Additionally, local law enforcement agencies differ in how they codify and apply privacy guidelines to regulate collection, use, retention, and dissemination of data related to counterterrorism.³⁸

Moreover, for the most part local police counterterrorism activities are not neatly separable from their broader public order and service missions. With regard to federal homeland security grants to fund state and major urban area intelligence “fusion centers,” for example, states are using them to develop programs that, while compliant with federal standards, also reflect local policy priorities, including combating local violence and general crime.³⁹ Although some large municipal police departments have built specialized counterterrorism or intelligence units, a decade after 9/11 most police agencies continue to rely on the same internal organization, policing strategies, and basic methods that preceded the extended terrorism emergency — even as they take on a significant role in collecting, analyzing, and sharing terrorism-related information and contribute to a broader, national security enterprise.⁴⁰

In sum, the post-9/11 institutional structure of U.S. domestic counterterrorism — while mostly lodged in expanded and restructured federal agencies with vast powers, resources, and influence — includes the localized and highly fragmented system of American policing. The United States has not turned to radical alternatives such as displacing it with an entirely new federal domestic intelligence apparatus or formally conscripting local institutions and agents into existing federal agencies.

This arrangement could face renewed calls for major reform in the future if terrorist emergencies expose breakdowns or counterterrorism gaps at the state and local level. For the foreseeable future, though, a significant portion of domestic counterterrorism effort will reflect local political and institutional pressures, and some domestic counterterrorism intelligence and other preventive activity will not be neatly separable from the traditional functions and duties of local police agencies.

LOCALIZATION OF INTELLIGENCE: A STRATEGIC VIEW

I and others have argued that these localization pressures *may* help protect liberty against erosion by aggressive security policies,⁴¹ much as Friedberg argues that anti-statist ideology, institutions, and political pressure helped protect against Cold War transformation into a garrison state. What about a parallel to the second half of Friedberg's thesis, though, that those anti-statist pressures also turned out to be strategically valuable by promoting economic competitiveness and sustaining domestic political support for security policies, ultimately overburdening the adversary by flexibly adjusting to technological developments?⁴² Looking back a generation from now, will we view the localist ideology, institutions, and political counterpressures to centralization that shape American intelligence architecture today as having been an asset or a liability in effectively combating terrorism?

This Section maps some of the possible advantages and disadvantages of reliance on state and local policing as part of the domestic counterterrorism intelligence architecture, as well as the critical assumptions underlying prominent claims. Although this analysis focuses singularly on the goal of terrorism prevention, this is not to deny important links between counterterrorism strategy and civil liberties protection or other goals like fighting crime and providing services; indeed, as explained below, community perceptions about the way governments wield coercive or invasive powers may be a major factor in facilitating or disrupting intelligence efforts. Nor is it to deny that protecting American values, including freedoms and accountability, might in and of themselves also be considered "strategic" imperatives, especially insofar as terrorist enemies try to erode them while we try to protect them. Rather, the modest purposes here are to raise important questions about one important slice of the issues — the relationship between the localized structure of American policing and effective counterterrorism intelligence — by drawing on recent studies and empirical findings and to suggest avenues for additional research and analysis.

Local Knowledge and Terrorism Expertise

There is a dearth of systematic study of the effectiveness of state and local counterterrorism programs.⁴³ However, it could be argued that widely enlisting local agencies and agents into national counterterrorism intelligence initiatives is at best inefficient because they lack the necessary expertise on transnational terrorist networks as well as the necessary institutional priorities to identify, investigate, and track the most significant terrorism threats.⁴⁴ Federal training for local counterterrorism intelligence programs are mostly wasteful, the argument sometimes goes, and even counterproductive because they perpetuate ethnic and religious stereotypes and alienate minority communities.⁴⁵ Looking abroad, Kim Lane Scheppele has observed in some other major democracies like Spain and Germany the advantages of cultivating an elite, specialized corps of terrorism investigators, rather than spreading

expertise too thin.⁴⁶ From these perspectives, one might conclude that the post-9/11 institutional architecture — which relies heavily on a vast and fragmented network of autonomous state and local agencies — is poorly designed to combat terrorism.

Running counter to the argument that local police lack counterterrorism and national security intelligence expertise, however, is a view that local police are better suited than federal counterparts to perform certain intelligence functions because of their superior familiarity with their local communities — a deep familiarity that results from local police agencies' broad public service and community order mandate and from the fact that police forces and their leadership are generally drawn from the local area.⁴⁷ These factors were among those cited by a major post-9/11 RAND study in concluding that “[s]tate and local law enforcement agencies ... are valuable intelligence assets. They are the ‘eyes and ears’ in the war on terrorism.”⁴⁸

The informational challenges of preventing terrorism are not just about collecting, analyzing, and sharing more information but also about processing better information and avoiding problems of too much information — addressing the challenges of too many “dots.”⁴⁹ State and local agencies may play an important filtering role, sifting through vast quantities of data, including tips and reports of suspicious activities, and dismissing irrelevant reporting that could clog the system. Again, localized intelligence architecture may be an asset here, insofar as the general order-maintenance and service mission of state and local agencies is what creates neighborhood and regional familiarity necessary for sound judgment with respect to information gathering and filtering.

Community Engagement and Intelligence

Beside the previous points about knowledge and expertise, a growing chorus of voices argues that *relationships* of trust between communities (especially, when it comes to Islamist terrorism, Muslim communities) and government agencies and agents are important to acquiring information about potential threats.⁵⁰ With regard to immigrant or religious communities, for example, Stephen Schulhofer, Tom Tyler, and Aziz Huq have recently argued, based on their studies of policing models and responses to them, that “to the extent that terrorist groups seek either to recruit or hide within co-religionist communities, cooperation can provide information at lower cost and with fewer negative side effects than coercive or intrusive forms of intelligence gathering.”⁵¹ Looking to the British experience, Martin Innes similarly argues that relationships of trust between police and minority ethnic communities yields important intelligence benefits that might be lost to more aggressive intelligence efforts that would alienate those communities.⁵² If this is so, the question follows whether some localization of American counterterrorism architecture contributes to the building and maintenance of such cooperative relationships.

Whereas federal law enforcement agencies are mostly (though not exclusively) tasked with investigating specific federal crimes, and the FBI has some specific

intelligence and preventative responsibilities related to national security threats, local police functions include preventing and investigating general crime as well as maintaining order, patrolling, and providing services — and these are rarely distinct from their “national security” functions. Modern policing strategy trends, most notably community policing, call for broad and deep engagement within the community.⁵³ Outfitted with the resulting familiarity and networks of relationships with community actors and other local agencies and institutions, it is often argued that local police are naturally positioned to receive information and detect suspicious irregularities.⁵⁴ Local agencies responsible for counterterrorism intelligence and prevention can also benefit from networks of collaborative partnerships with other government and non-government actors — including other enforcement and public service agencies, civic and business organizations, etc. — that may be sources of information or assistance in investigation.⁵⁵

The federal government — through the FBI, DHS, and other agencies — has been expanding its Muslim community outreach in an effort to address concerns about its policies and to build networks of ties.⁵⁶ Meanwhile, some studies warn that counterterrorism training programs for local law enforcement and municipal police efforts to identify violently-extremist groups will likely backfire in areas where local agency personnel are ill-informed and harbor ethnic or religious biases, by alienating monitored communities.⁵⁷

Notwithstanding these efforts and concerns, there are reasons to expect that in some jurisdictions local police could be better than federal counterparts in building and maintaining relationships with community members, leaders, and actors that could yield important information or to mobilize responses needed to thwart terrorism.⁵⁸ First, some policing scholars posit that in many contexts local police are better able than federal law enforcement agencies like the FBI to cultivate and maintain relationships of trust and cooperation with minority communities and other local actors — and that this is significant in part because of their broader public service and law and order missions, their repeated and long-term interactions, and the mutual dependency of police and policed communities for problem-solving.⁵⁹

A closely related argument as to why intelligence localization therefore may be valuable, especially over the long term, is that it may serve as a break on natural tendencies of security agencies toward aggressive and invasive short-term measures that might alienate minority communities that view themselves as targeted. For example, sociologist David Thacher’s case study of the Justice Department’s early post-9/11 request that Dearborn, Michigan, police assist in interviewing large numbers of local immigrants revealed that concerns about community trust influenced the way city agencies participated in the interviews: local police declined to conduct the interviews themselves, worked hard to explain their participation in a qualified way, and they ultimately adopted a role representing community concerns in monitoring federal agents.⁶⁰ The role of local police in that case and many others was shaped by their interest in confining intelligence and information gathering efforts, which threatened

to undermine relationships with Arab community elements they had worked hard to develop, whereas federal agencies (with a much narrower mandate vis-à-vis local community) had less at stake in protecting those relationships.⁶¹ The general upshot, some argue, is that federal dependence on local agencies gives those local agencies leverage, and that they will use that leverage to restrain federal practices that would risk disrupting intelligence-generating relationships with community actors.⁶² As Samuel Rascoff argues, local police “are in significant respects well positioned to tap into their relationships with the local community to useful effect.... Not only do these long-term, multifaceted relationships have the effect of potentially restraining the impulses towards overly aggressive counterterrorism measures, they form the backbone of a robust intelligence network.”⁶³

Embedded in these optimistic claims about local policing and intelligence-yielding relationships are some critical assumptions about constraints on police behavior — assumptions, the validity of which, will vary significantly from locale to locale. The areas of Michigan Thatcher studied, for example, contain a high concentration of Arab-Americans, so one might expect police to be especially attuned to their concerns.⁶⁴ The relative effectiveness of local police as elements of a nationwide counterterrorism architecture will likely vary considerably across locales based on such factors as how well politically organized minority communities are, the relationship between the police and other local government institutions, and on the effectiveness of oversight mechanisms, including transparency and the ability of minority community organizations and other advocacy organizations to meaningfully engage and influence police agencies.⁶⁵

Uncertainties and Opportunities

It is unsurprising that post-9/11 institutional reconfigurations pushing counterterrorism responsibilities to local police agencies would raise concerns that local capabilities, refined over a long time to deal with other crime and public policy issues, match poorly with the national security imperatives of combating terrorism, or that saddling local police agencies with these responsibilities would distort and degrade their regular functions.⁶⁶ Studies show, however, that post-9/11 counterterrorism responsibilities have not resulted in radical changes to internal police agency structure or the way they manage their core, local public policy functions,⁶⁷ and the above analysis suggests that some comparative counterterrorism advantages derive from the very broad public service and order-protecting mandate of local police. In Daniel Richman’s words: “The contribution that local police forces can make to domestic intelligence policy making and collection is thus related to the nature of their ‘beat.’”⁶⁸

This still raises long-term questions about cost-effectiveness, though, including whether alternative institutional designs would more efficiently target resources. To a large degree the strategic wager to invest in local police intelligence architecture

versus centrally-managed capabilities is related to the architecture of the terrorism threat it is build to combat. The Al Qaeda network that perpetrated the 9/11 attacks has been weakened and is splintering into regional franchises abroad, but it remains hotly contested and highly uncertain to what degree the terrorism threat facing the United States will include a significant domestic or “home-grown” component.⁶⁹ International terrorist networks — especially those that Al Qaeda controlled or are supported by a central core — are often detectable through technological and institutional capabilities that only reside at the federal level, including large-scale and global programs to monitor communications, significant intelligence sharing and cooperation efforts with foreign government agencies, and centralized analysis of seemingly disparate bits of information.⁷⁰ By contrast, the more that terrorism threats include domestic, and perhaps homegrown, dangers, the more dependent the government will be on tips and observations generated locally.⁷¹ As a National Research Council report on counterterrorism and domestic intelligence put it, “The ability to detect broader and more diverse terrorist plotting in this environment will challenge ... the tools we use to detect and disrupt plots. It will also require greater understanding of how suspect activities at the local level relate to strategic threat information and how best to identify indicators of terrorist activity in the midst of legitimate interactions.”⁷² Those types of dispersed and decentralized threats will sometimes be more detectable at the local level, where terrorist plotters are operating or organizing.

In the classic sense of “laboratories of democracy,”⁷³ some long-term advantages of localism of American counterterrorism intelligence may also ultimately emerge through experimentation and resulting adaptation as best practices spread.⁷⁴ Schulhofer and his colleagues explain, for example, that law enforcement agencies will take varying strategic choices, including whether to focus on intrusive enforcement and intelligence gathering that promise immediate and instrumental benefits or to focus on efforts to build community trust and perceived legitimacy over the long-term, and varying tactical choices, including building ties to community leaders or through interaction with individuals in ordinary street-level encounters.⁷⁵

This sort of bottom-up learning through local innovation may be especially important in developing new policy tools for combating terrorism.⁷⁶ One possible example is processes for information sharing and analysis, and the federal government has in that regard been working with select state and local intelligence fusion centers (which have lately come under intense scrutiny and criticism)⁷⁷ to develop and refine policies and practices for recording, filtering, and sharing suspicious activity reports possibly indicative of terrorist activity. This particular program involves giving state and local partners significant discretion to design programs within federal information processing and privacy requirements, as well as feedback processes to build on successful initiatives and to continually refine those federal guidelines based on experience.⁷⁸

Some major cities are also experimenting with sophisticated data analytics technology to combat threats. As I have argued elsewhere:

“Given that it is highly unlikely that comprehensive federal legislation in this area will be enacted anytime soon, we will not have uniform rules to govern these growing capabilities. That is a good thing, because different locales face such different threats. Moreover, experimentation and adaptation, along with the public debate that accompanies them, can help cultivate and extend best-practices as these powerful analytic technologies continue to advance and spread.”⁷⁹

Learning from localized experimentation and adaptation might also be well-suited to the policy problem of countering violent extremist recruitment and radicalization — a problem that overlaps significantly with intelligence policy and practice but is also sometimes in tension with it.⁸⁰ Lessons from European countries more experienced in dealing with domestic terrorism threats and pockets of violent extremism among certain minority communities suggest that local governments are often better positioned than national ones to design and implement strategies for countering violent-extremist ideology and recruitment, but that counter-radicalization and national security intelligence efforts are difficult to meld because the latter may erode trust among communities perceived to be targeted for surveillance.⁸¹ Given their broader community protection and service mandate, local police and/or local non-law enforcement agencies may serve as a better bridge between those activities than could their federal counterparts, and may be better positioned to leverage the influence and capabilities of other local government and non-government actors. In such contexts, the federal government appears to be recognizing quite openly that its most effective role may be in funding local initiatives to combat violent extremism, facilitating the spread of programs bred from local experience, and sharing information about best practices developed by state and municipal governments for building relationships with community actors (educational, religious, and others) necessary to yield information about threats while also addressing their incipient formation.⁸²

CONCLUSION: STRATEGY AND ARCHITECTURAL COMPROMISES

Much more empirical study of post-9/11 U.S. domestic counterterrorism intelligence is needed, and this mapping exercise of advantages and disadvantages of localization vastly oversimplified the choices involved. The architectural reality is very messy because there is so much heterogeneity among local jurisdictions and their governing institutions, and because there is so much variation across jurisdictions in the mix of federally-driven centralization and bottom-up localization. Moreover, sometimes that mix is intentional and well-coordinated, sometimes it is neither, and it is always in some flux.⁸³

Returning to Friedberg's thesis about the interior dimension of grand strategy, one is struck in reading his Cold War history that, although generally effective, the institutional macro-structures and arrangements through which the United States waged it were very far from perfect. Moreover, their composition and configuration often resulted as much from political compromise as from rational design. In a similar way, localization of American domestic counterterrorism architecture should not be viewed simply as a carefully reasoned set of strategic choices drawn on a clean slate, but as also reflecting strong inertial pull of very long-standing and deeply embedded allocations of political power and constitutional federalism compromises. Continued localization of some counterterrorist intelligence policy and functions is not inevitable over the long-term, but it will remain a strong default position.

The practical value of studying and understanding the merits and drawbacks of localized counterterrorism functions will therefore not likely accrue much with respect to first-order questions, like whether instead of dividing counterterrorism powers vertically between the federal and state/local levels we should instead centralize them in the federal government. Although it has shown resilience so far, no doubt the localization of some features of American counterterrorism architecture could face renewed centralization pressures in the future if the frequency of terrorist attacks within the United States increases, especially if future terrorist attacks were to expose major breakdowns in cooperation, communication, or information sharing between the federal and local governments or between local governments.⁸⁴ Even then, though, there are limits to how far counterterrorism functions can be centralized, given that they cannot be neatly separated from policing and other core state and local responsibilities.

More likely the value of further study and improved understanding in this area will accrue with respect to second-order questions, like how best to design, arrange, manage, and oversee counterterrorism powers and functions shared vertically among federal, state, and local levels of government and within the constitutional structure we have inherited. The details of domestic counterterrorism architecture are still very much a work in progress, even if the major post-9/11 structural elements — federal bureaucratic reorganization, collaborative arrangements and grant programs linking federal agencies with state and local partners, etc. — are now in place. Better empirical understanding of their effectiveness will help refine the inner features of this structure and help extract the most value out of the localized aspects of our national security system.

AN HISTORIC PERSPECTIVE OF INTELLIGENCE GATHERING

TRANSCRIPT OF REMARKS

Frederick A.O. Schwarz, Jr.
Chief Counsel, Brennan Center for Justice

*Former Chief Counsel for the Senate Select Committee to Study Governmental
Operations with Respect to Intelligence Activities*

We all start with the understanding that there is an important need to address the terrorist threat. Those on the frontlines protecting us from terrorism are doing extremely important work for our country, for our state, and for our city. Vigilance is required to protect the country.

However, history teaches us that there are plenty of risks of excess and resulting harm in such endeavors. I will discuss the risks of harm and then discuss oversight.

Three elements create risks of harm. One is excessive secrecy. Another is lack of oversight. A third is vague language used to empower authorities to conduct surveillance.

There is a long history of vague language empowering the FBI to conduct activities that were harmful.

For example, in 1924, when J. Edgar Hoover took over what later became the FBI, he lied to the ACLU about his connection to the notorious Palmer raids at the end of World War I. Hoover told the ACLU he had barely anything to do with them. As we later found out on the Church Committee in the mid-1970s, Hoover was instrumental in rounding up politically active immigrants, denying them counsel, and deporting them. Yet, the ACLU's consent was very important in having him approved.

The attorney general who appointed Hoover, Harlan Fiske Stone, was a former dean of the Columbia Law School. (He later became Chief Justice of the U.S. Supreme Court.) He told Hoover he did not want the FBI investigating people's opinions; only their actions. The standard, he directed, should be criminal law. And that benchmark was followed from 1924 until 1938. Then President Franklin Roosevelt, jumped in. We regard FDR as a hero — in many ways correctly. But, he was not a hero on this subject.

Hoover was appointed the FBI's first director in 1935. In the run-up to World War II, Franklin Roosevelt instructed Hoover to investigate espionage and sabotage. Both were crimes. FDR also told him to go after "subversion." The trouble with that word is that it lacks precision. It became the enabling directive permitting the FBI to engage in a vast array of illegal and improper activities. Fighting "subversion" is what opened the door to all of the horrors later revealed by the Church Committee.

In the wake of two 1939 Supreme Court decisions limiting use of wiretaps,¹ Attorney General Robert Jackson ordered an end to FBI wiretapping. But Roosevelt sent a little handwritten note to his Attorney General effectively reversing him. FDR wrote, "I'm sure that that opinion was not meant to apply to the matters of national interest that you work on."

About fifteen years later, there was another Supreme Court decision² condemning warrantless bugging. Authorities had put hidden microphones in the bedroom of a mafia associate. The Court was offended and said the police had "flagrantly, deliberately, and persistently violated" the Fourth Amendment protection against unreasonable search and seizure. Nonetheless, they upheld the bookmaker's conviction, saying that the defendant had remedies other than a wholesale reversal.

One of those remedies was criminal prosecution of law enforcement. In fact, the Supreme Court actually sent a note to Attorney General Herbert Brownell asking whether prosecutions were warranted because of the FBI's behavior.

What did Brownell do? He hid behind fuzzy language. He sent a note to Hoover saying that wiretapping was permissible as long as it was — on Hoover's sole authority — in the "national interest." That standard remained for nearly a quarter-century until the passage of the Foreign Intelligence Surveillance Act (or FISA) in 1978.

The FBI's abuse went far beyond wiretapping. Hundreds of thousands of Americans had their mail opened. Nixon had his mail opened. Senator Church had his mail opened. The American Friends Service Committee had their mail opened.

This widening surveillance, in both number of targets and methods used, illustrates another problem of vague, indeterminate language: mission creep. Something starts as relatively narrow, and then, because of imprecision, secrecy and lack of oversight, goes beyond the narrow and proper to the broad and illegal.

For instance, the FBI's COINTELPRO program, or so-called Counter Intelligence Program, was launched because the Bureau was frustrated by Supreme Court decisions that made it difficult to lock up communists solely because of their beliefs. So, the Bureau decided to take the offensive. They set out to destroy and undermine organizations or people they deemed "subversive."

They started with the U.S. Communist Party, even though the majority of its members were, in fact, FBI agents. But, they moved on. Eventually, COINTELPRO targeted what they called "black nationalist hate groups."

One of these groups was the Black Panthers. Rhetorically at least, some Black Panthers were not exactly choirboys. It is not surprising the Black Panthers attracted law enforcement's attention. But the FBI went well beyond just paying attention. In

Chicago, the FBI sent a phony incendiary document to a black gang to incite them to kill the head of the Black Panthers in an act of reprisal. Surveillance is one thing. Sowing the seeds for murder is something else.

The FBI's choice of "black nationalist hate groups" was rather broad, to say the least. One of them was the non-violent, peaceful Southern Christian Leadership Conference, led by that notorious "hater," Martin Luther King.

Hoover, of course, was obsessed with King. His behavior toward King is a vivid demonstration of what can happen when there is a toxic mix of loose language, no oversight, and cavalier disregard for the law. Even Hoover realized he needed some sort of benediction from Attorney General Robert Kennedy to wiretap King. He even got a nod from the President, Robert's brother, Jack. Shrewdly understanding that anti-communism was a more powerful lever to justify surveillance than King's civil rights advocacy, the Bureau trained its sights on King's closest white adviser, Stanley Levison, a wealthy, Jewish, New York lawyer and business executive. I actually knew Levison when we worked together against South African apartheid. He did not look like a communist to me.

But, that's not how the Bureau spun it. They told Robert Kennedy that Levison belonged to the Communist Party. Yet, the Bureau did not tell Kennedy the full story. Levison had left the Communist Party before he began conferring with King. They simply did not tell the whole truth.

One wonders why Robert Kennedy, no fan of Hoover's and acutely aware of King's rising prominence, did not press for a fuller explanation. When I was counsel to the Church Committee, I had information that perhaps provides an answer as to why the Attorney General and the President acquiesced so easily. Unfortunately, I did not see its implications at the time.

At the exact same time [as] Hoover was pressing for permission to wiretap King, Levison, and King's lawyer, Clarence Jones, the FBI Director sent a little missive to the Attorney General and the White House Chief of Staff.

The gist of the letter was the following: The FBI knows that there have been seventy-two phone calls between the White House and one Judith Campbell, now better known as Judith Campbell Exner. Hoover explained that Campbell was the mistress of Chicago Mafia chief Sam "Momo" Giancana. He then attached a lengthy description of Giancana's criminal record. Always willing to serve, Hoover requested a meeting with the President to discuss this troubling matter.

Hoover did not need to say much else. Hoover knew, and Hoover knew the Kennedys knew he knew, of the President's dalliances with Judith Campbell. One leak to any one of Hoover's favored journalists, and the Kennedy brothers' careers were over. They were not exactly in a position to deny Hoover's request.

It is also worth noting that Giancana had recently worked with the CIA in futile attempts to assassinate Fidel Castro.

In a sense, Sam Giancana, a mobster, became the living embodiment of all the adverse consequences of unrestrained, hidden intelligence operations. The CIA set

out to kill Castro. They opted to recruit a crook to do the job. Meanwhile, at more or less the same time, the FBI was wiretapping the phones of the mobster's mistress, who just happened to be having an affair with the President of the United States. In the person of Sam Giancana, unrestrained appetites converged — those of the FBI, the CIA, and last, but not least, the President.

The combination of vagueness, secrecy, and its cousin, lack of oversight, is a surefire recipe for abuse.

Another example of mission creep in the absence of oversight involves the National Security Agency. In 1946, with the cooperation of the nation's three largest telegraph companies — this was in the days before email or even reliable international telephone connections — the NSA received a copy, every day, of all telegrams sent from the U.S. overseas. The initial rationale had a reasonable national security purpose: to review encrypted communications foreign embassies in the U.S. sent home. That was the NSA's job: to crack codes. But it was easier for the telegraph companies to hand over everything and let the NSA sort it out.

Of course, that is not what happened. Instead, the NSA began snooping on cables sent by civil rights activists, opponents of the Vietnam War, and others deemed a "threat." This lawless, comprehensive data collection lasted nearly thirty years. It was not until 1975, when the Church Committee uncovered it, that U.S. Attorney General Edward Levi told the NSA that its actions were unlawful and had to stop.

Today, intelligence collection faces an additional challenge. We do not live in a national police state. Federalism is a cherished and enduring tradition in this large country. Local law enforcement is critical to fighting terrorism. But, so is local oversight. Congressional review of federal intelligence activities is far from perfect, but it is infinitely superior to what it once was. But most local officials are extremely reluctant to question their police force. Additionally, many police chiefs, who do not have to resort to Hoover's blackmail, are highly effective at bullying local lawmakers to bend to their will.

This state of affairs is a genuine problem, a genuine dilemma. It is something we have to wrestle with. But, of one thing I am certain: secret, unconstrained law enforcement will lead to abuse. Without adherence to the law and meaningful, effective, independent oversight, we will back where the Church Committee was in 1975 and 1976: highly embarrassed by law enforcement's illegality and unfairness to all Americans.

PART TWO

**THE FIRST AMENDMENT AND DOMESTIC
INTELLIGENCE GATHERING**

INTRODUCTION

Elizabeth Goitein
*Co-Director, Liberty & National Security Program
 Brennan Center for Justice*

In 2006, a newcomer began attending services at the Islamic Center of Irvine in Southern California. The other mosque attendants welcomed him into their midst. They opened their homes to him and shared their beliefs about Islam. But then he began to talk about violence and weapons. The community grew alarmed, reported his statements to the FBI, and obtained a restraining order against him. It subsequently emerged that the individual was an FBI plant, sent into the mosque with hidden video and recording devices to capture everything that was being said. When the community learned what had happened, some stopped attending the mosque. Others reported that the good will that once permeated their tight-knit religious community was replaced by distrust.¹

This anecdote does not represent an isolated incident. The FBI has acknowledged using informants in mosques across the country.² Why is the FBI employing this particular method of intelligence collection, given the potential disruption to First Amendment-protected religious activity?

The answer likely lies in a peculiar narrative about Islam that has unfolded in the wake of September 11. Al Qaeda uses Islam to justify terrorism, as do some others who would follow in Al Qaeda's footsteps. But most Americans understand that only a minute fraction of the several million Muslims in this country pose any kind of threat. Accordingly, many Americans — including a number of our leaders — have posited that there are two kinds of Islam: the “true” Islam, which is practiced by the vast majority of Muslims in this country and the twisted perversion of the religion that Al Qaeda and other terrorist groups cite as a justification for their actions. The first kind is sometimes labeled “moderate” Islam, while the second kind is known as “Islamic extremism.”³ If we can identify people who subscribe to the “extremist” version of Islam, the narrative goes, we may be able to intervene in some way to prevent terrorist attacks.⁴

This narrative has been widely embraced by the public, and its emphasis on ideology drives the way we think and talk about terrorism. The process of becoming a terrorist, for example, is known as “radicalization.” “Radical” is almost certainly intended to describe the underlying philosophy, as it would seem an odd choice to describe the act of flying a plane into a building (or detonating a car bomb or planting an improvised explosive device (IED)). The term “radicalization” thus suggests that becoming a terrorist is a journey of ideology.

A focus on ideology is also evident in the response of law enforcement. In describing the process of radicalization, law enforcement agencies such as the New York City Police Department and the FBI have emphasized the importance of ideological indicators, which, according to them, include wearing traditional Islamic dress, receiving religious education overseas, and other religious behaviors.⁵ Intelligence gathering practices are then designed around these ideological indicators. For example, the Justice Department has relaxed the rules governing FBI investigations to allow the placement of informants in mosques even if the FBI has no reason to suspect any criminal or terrorist activity.⁶ Law enforcement agencies are urging Muslim community leaders to report anyone who exhibits “extremist” beliefs or behaviors.⁷ And, as Nura Maznavi’s article in this chapter illustrates, American Muslims re-entering the country after travel abroad face questions from customs officials about their religious beliefs and practices.

This operational response raises threshold empirical questions. First, despite its widespread usage, the term “Islamic extremism” is rarely defined. Is it true that Islamic terrorists are motivated by a particular religious ideology that we can identify and that distinguishes them from other practitioners of the faith? Second, and closely related, are there particular ideological indicators that can be used to spot terrorists before they act? These questions arose during the question and answer session of the symposium, when Maznavi was challenged to explain why the costs of techniques like mosque infiltration are not justified by the benefits. Maznavi responded by citing the work of Marc Sageman, who has conducted rigorous empirical studies of Islamic terrorists (including several hundred interviews) and has reached the surprising conclusion that they are not particularly religious — thus suggesting that a focus on religious ideology is likely to be ineffective in identifying would-be terrorists.⁸

Beyond these empirical questions, current intelligence gathering practices raise a host of First Amendment questions. University of Chicago Law School Professor Geoffrey Stone, whose remarks at the symposium were transcribed for this publication, began the discussion by addressing the infiltration by law enforcement of houses of worship. If agents infiltrated a church, temple, or mosque for the purpose of monitoring the ideas being expressed by religious leaders or congregants, the First Amendment would be “in play.” Nonetheless, Stone opined that the First Amendment would offer little protection in practice. A plaintiff would face a high hurdle in establishing standing to challenge the infiltration; the Supreme Court has held that a subjective “chill” of First Amendment rights is insufficient to open the

courthouse doors.⁹ If a litigant did have standing to raise the claim (for example, if it were raised as a defense in a criminal proceeding¹⁰), there would be no definitive precedent to guide the court¹¹ — and Stone suggested that courts would be reluctant to create any new doctrine because it would be exceedingly difficult to create principled, workable limits. Accordingly, Stone concluded, a more fruitful approach might be to focus on non-judicial constraints on intelligence gathering, such as the internal guidelines of the Justice Department and FBI.

While Stone focused on the legality of mosque infiltration, Kate Martin of the Center for National Security Studies broadened the inquiry, addressing the general question: Are expressions of “radical” or “extremist” beliefs, which could not themselves be criminally punished, a legitimate subject of law enforcement scrutiny at the intelligence-gathering phase? She recalled that civil liberties groups before 9/11 had urged a rule under which the government could not investigate mere advocacy of violence (which, under *Brandenburg v. Ohio*,¹² cannot be criminalized) unless it was accompanied by a concrete step toward violence, such as the purchase of a weapon. By contrast, she noted that today’s statutory prohibitions on “material support” for terrorism arguably provide, not only for investigation, but for actual criminalization of the advocacy of violence. This observation and its ramifications are further explored in her article.

Stone weighed in on the question raised by Martin, arguing that law enforcement officers should not be expected to ignore advocacy of violence any more than they should be expected to ignore the purchase of a gun, despite the fact that such purchase may be protected under the Second Amendment. He nonetheless emphasized that the *means* of investigation could be more or less intrusive, and that the infiltration of religious spaces, based on mere speech, might be considered a disproportionate step given its potential to chill religious exercise.

Mazvani moved the conversation from theory to unflinching reality, focusing on the effect current intelligence gathering practices have on the daily lives of American Muslims. As expounded in her article, many American Muslims today live in fear — a fear that stems from three sources: possible retaliation by federal agents if they or others in their community protest surveillance abuses; anti-Muslim sentiment among their neighbors and co-workers; and the potential for inviting law enforcement scrutiny by exercising their constitutional rights to free speech and religious exercise. To underscore that these fears are grounded in reality, she recounted stories that American Muslims had told her when seeking the help of her organization, Muslim Advocates. These stories — examples of ordinary American Muslims who were subjected to highly intrusive (and unpleasant) scrutiny by law enforcement agents — had a powerful effect on fellow panelists and audience members alike. They appear in her article.

Chuck Rosenberg,¹³ former U.S. Attorney for the Eastern District of Virginia, brought a different perspective to the discussion: that of someone with a long and distinguished career in law enforcement. He began with some observations about

process, noting that the purpose in revising the Attorney General's guidelines after 9/11 was simply to consolidate and streamline the several different sets of rules for different types of FBI investigations, and that the changes were vetted with members of Congress and their staff. He also suggested that one's view of the guidelines depends largely on one's view of the FBI: those who trust the organization (Rosenberg counted himself among these) find the guidelines to be balanced, sensible, and principled, while those who do not trust the organization find the opposite.

Responding to Maznavi's remarks, Rosenberg expressed regret over the stories of American Muslims whose religious worship was now tainted by fear but cautioned against basing policy judgments on anecdotes. He also opined that, regardless of whether a particular limitation on investigative activity (such as a restriction on infiltrating religious spaces) might be desirable in theory, it was dangerous, in practice, to signal that law enforcement would never cross a particular line when investigating a case, because that would help would-be terrorists to determine how and where they could plan their crimes without detection. Finally, he noted that any potential for abuse of the guidelines was greatly diminished by oversight from several quarters: the press, Congress, advocacy groups, presidential advisory and oversight boards, the Justice Department's Inspector General, officials at the FBI charged with implementing internal oversight, and whistleblowers.

Finally, another First Amendment question arose because of law enforcement's focus on "moderate" versus "extremist" Islam: Assuming *arguendo* that there is an identifiable "extremist" ideology at work — and assuming that the government can accurately differentiate between this ideology and religious views that are merely conservative or passionately held — does it nonetheless raise Establishment Clause problems for the government to praise one model of Islam and condemn another? Stone believed that this might rise to the level of viewpoint discrimination, thus triggering a heavy burden of justification on the government, but that it likely would not offend the Establishment Clause. However, when asked to comment on the recommendation put forward by the Chair and Ranking Member of the Senate Homeland Security and Governmental Affairs Committee that the Department of Defense amend its anti-discrimination policies to differentiate so-called "violent Islamic extremism" from "the legitimate practice of Islam,"¹⁴ Stone agreed that such an amendment would violate the Establishment Clause.

While it was clear that the panelists approached the issue of domestic intelligence gathering from different perspectives, at least one point of agreement emerged during the course of the discussion: under existing jurisprudence, and given the current configuration of this Supreme Court, individuals who wished to challenge intelligence-gathering practices on First Amendment grounds would face an uphill battle. In the question and answer session, however, University of Chicago Law School Professor Aziz Huq questioned whether the unavailability of judicial remedies implies that the conduct in question is indeed permissible under

the First Amendment, or whether it is simply an example of the Constitution being “underenforced.”¹⁵ Stone agreed that the Constitution may place demands on government even in the absence of a judicial remedy, but cautioned that those demands must be shored up by policy to be effective.

“TO THINK CLEARLY ABOUT THE FIRST
AMENDMENT, IT IS USEFUL TO IDENTIFY
BASIC PRINCIPLES BEFORE TRYING TO RESOLVE
PARTICULARLY DIFFICULT OR VEXING ISSUES...”

TRANSCRIPT OF REMARKS

Geoffrey R. Stone
Edward H. Levi Distinguished Service Professor
University of Chicago Law School

I want to begin by examining the relevant First Amendment principles outside the context of this particular issue. To think clearly about the First Amendment, it is useful to identify basic principles before trying to resolve particularly difficult or vexing issues.

To begin, then, suppose the police have probable cause to believe that a priest is engaging in child sexual abuse. They also have probable cause to believe that there is evidence of the priest’s illegal behavior in his desk in the church. They obtain a warrant, search the desk in the church, and find the evidence they need to prosecute the priest. Did this search violate the First Amendment because of its intrusion into the autonomy and independence of the church? I assume most of us would say that the standards required by the Fourth Amendment, which protects against unreasonable searches and seizures, would be sufficient to satisfy anything the First Amendment might itself require in this sort of situation, and that, indeed, seems to be the current state of the law.

Now, suppose that the police do not have probable cause. They have only a hunch that the priest might be involved in child sexual abuse. They therefore cannot constitutionally obtain a warrant and cannot search the church or the desk consistent with the Fourth Amendment. So, instead, they infiltrate the church by authorizing a police undercover agent to attend church services and get to know the congregation in order to get more information about the conduct of the priest. The undercover agent obtains evidence in this manner that corroborates the hunch that the priest is engaged in child sexual abuse, and the priest is thereafter prosecuted. Does the use of the secret agent in these circumstances violate either the First or Fourth Amendment?

Under well-established precedent, there is no violation of the Fourth Amendment

in this situation. The Supreme Court has held that individuals have no “reasonable expectation of privacy” that the people with whom they deal are in fact who they say they are. Thus, if you are deceived by someone into revealing information about yourself, there is no Fourth Amendment “search” and hence no Fourth Amendment violation. Personally, I think this doctrine is profoundly wrong-headed, but it is nonetheless well-settled.

The next question is whether the First Amendment prohibits the police from surreptitiously attending the church services and infiltrating the church community in an effort to determine whether the priest is engaged in child sexual abuse, when the police do not have probable cause to believe that the priest is engaged in such conduct. Does the First Amendment, wholly apart from the Fourth Amendment, prohibit the police from attending the church services because their purpose in doing so is not to participate in the religious activity but to gather information about possibly illegal activity? Are the police constitutionally prohibited from attending the church services for this reason, even though those services are generally open to anyone who wants to attend?

In most infiltration situations no First Amendment issue would arise. For example, if the police used an undercover summer camp counselor in order to investigate a counselor suspected of child sexual abuse, no First Amendment issue would arise, because the summer camp is not itself engaged in First Amendment activity. But when we are dealing with the infiltration of a church or a political organization, First Amendment activity is clearly at issue. Does that change the result from the camp counselor situation?

Under established First Amendment doctrine, if the government engages in activity that has only an incidental effect on First Amendment activity, there is a strong presumption that there is no constitutional violation. In my church hypothetical, the government’s interest in ferreting out child sexual abuse has nothing to do with the fact that in this case it happens to be investigating a priest in a church. The government’s interest would presumably be the same, and its investigation presumably would be the same, if the suspected child abuser were a counselor in a summer camp. The fact that a priest, a church and religion are involved in this particular investigation is wholly incidental to the government’s decision to investigate. The Supreme Court has long held that, absent extraordinary circumstances, such government action does not violate the First Amendment, even if it incidentally impinges on otherwise protected First Amendment activity.

What, though, are “extraordinary circumstances”? A good example is the Supreme Court’s decision in *NAACP v. Alabama*, in which the Court considered the constitutionality of an Alabama law that required all out-of-state organizations doing business in Alabama to disclose their membership lists. The NAACP objected that even though this law applied to all out-of-state organizations and therefore had only an incidental effect on the NAACP, the application of the law to the NAACP in Alabama at the very height of the civil rights movement would have a severe

chilling effect on the willingness of individuals to join or support the organization. In this situation, where the incidental effect of the government action would clearly have a severe impact on protected First Amendment activity, the Court held the application of the law to the NAACP unconstitutional. But the Court has applied that exception narrowly over the years, and it presumably would not apply in the church hypothetical, because such investigations are relatively rare and they do not have a demonstrably severe chilling effect on the willingness of individuals to attend church services generally. Thus, if the government is investigating ordinary criminal conduct and is not investigating First Amendment activity because it is First Amendment activity, then an investigation that intrudes upon a church, a mosque, or a synagogue ordinarily will not violate the First Amendment.

A potentially different situation arises if the government investigates an organization *because* its speech or religion is itself thought to be harmful, damaging, or dangerous. In this situation, we are no longer dealing with an incidental effects problem, but with a direct regulation of First Amendment activity. Thus, if a cleric gives radical speeches in a mosque, and the government employs undercover agents to infiltrate the mosque in order to record the cleric's speeches and to keep track of the people who attend them, we are clearly outside the scope of the incidental effects doctrine. Does such an investigation violate the First Amendment?

The first obstacle to invoking the First Amendment in this situation is that the Court has been quite reluctant to grant anyone standing to challenge this type of activity if the only harm they can allege is that they are chilled in the exercise of their rights. The Court has held that the mere fact of being chilled, in and of itself, is insufficient to establish standing to challenge the constitutionality of the government's action. As a result, it would be difficult under existing law for anyone in the mosque to establish standing to challenge the constitutionality of the government's infiltration of the mosque, even if the investigation was triggered by the content of the cleric's speech. This, too, is a wrong-headed doctrine, but it is what it is.

Assume now that someone in the mosque does have standing. This would be true, for example, if an individual is later arrested on a charge that he participated in a terrorist act, and the evidence offered against him includes his presence in the mosque during the cleric's radical speeches. In this situation, the individual might have standing to challenge the constitutionality of the government's infiltration of the mosque on the theory that it violated his First Amendment rights. The question then is whether the government in fact violated the First Amendment when it sent its agents into the mosque for the purpose of surveillance. At present, there is no definitive, or even close to definitive, precedent on this question.

The difficulty with articulating any straightforward doctrine to govern this issue is that the number of situations in which the problem arises is virtually limitless. Is it constitutional, for example, for the police to attend an anti-war demonstration? Does it matter if they are there to keep the peace, to take names, to deter people from protesting, to make it safer for people to protest? The mixed/elusive motive

problem arises in endless situations, and the Court has generally been reluctant to ask lower courts to determine whether any particular law or other government action is constitutional based on an inquiry into actual, subjective motive.

In light of all these obstacles, and with the Supreme Court constituted as it currently is, any effort to challenge the constitutionality of government surveillance of First Amendment activity is likely to meet stiff resistance from the Court. It seems safe to say that, as a practical matter, a lot more work needs to be done to articulate a clear and coherent theory that would persuade the current majority of the Supreme Court to hold that the “mere” government investigation of First Amendment activity violates the Constitution.

What all this suggests to me is that much more attention should be paid to possible nonconstitutional restraints on government that could help rein in such investigations. The FBI Guidelines for the investigation of political and religious organizations are a good example. After all, even if the Constitution does not prohibit the government from doing something, that doesn't mean the government should do it. The government can exercise restraint itself and place restrictions on its own behavior.

This is exactly what happened when Attorney General Edward Levi initially put the FBI Guidelines in place under President Gerald Ford after COINTELPRO came to light in the Church Committee hearings. Levi voluntarily promulgated guidelines that prohibited federal agents from investigating religious or political organizations in the absence of a specific and articulable reason to believe that illegal conduct was afoot. This was a major step forward. Unfortunately, subsequent Attorneys General have watered down the Levi guidelines over the past thirty-five years. At least in the short run, though, and until there is a change in the makeup of the Court, I think this may be a more fruitful way to proceed, particularly with the current Administration. Putting pressure on the Attorney General to adopt those sorts of self-imposed restraints could go a long way towards limiting this problem, at least at the federal level.

FBI SURVEILLANCE AND CUSTOMS AND BORDER PATROL QUESTIONING: IMPACT ON THE FIRST AMENDMENT RIGHTS OF THE AMERICAN MUSLIM COMMUNITY

Nura Maznavi
Former Staff Attorney
Project to End Racial and Religious Profiling
Muslim Advocates
 &
 Jawziya Zaman
Former Legal Fellow
Muslim Advocates

INTRODUCTION

Today, almost ten years after the tragic events of 9/11, there is immense fear and apprehension in the American Muslim community. This fear is three-fold. There is the fear of possible retaliation by federal agents if one speaks out against surveillance abuses. There is also the fear of hate crimes, discrimination, and harassment from fellow Americans as increasing levels of anti-Muslim sentiment sweep the country. And finally, there is the fear of exercising constitutionally protected rights — going to the mosque, donating to a religious charity, welcoming new Muslims into the community, or speaking one’s mind about religion, politics or foreign policy.

American Muslims care deeply about the safety and security of their country and do their part to protect it. They also demand the same rights and protections guaranteed to all Americans. The organization for which I work, Muslim Advocates — a national legal advocacy and education organization whose mission is to promote and protect freedom, justice, and equality for all, regardless of faith — has direct contact with American Muslims across the country on a daily basis (through “Know Your Rights” presentations, seminars, trainings, and other outreach) and hears and documents stories of American Muslims who are experiencing, at a deeply personal level, the stark reality of domestic intelligence gathering.

How did our nation get to the point where Americans are nervous about openly practicing their faith or speaking freely about political or religious affairs — core constitutional rights — because they might be monitored or questioned by federal

agents who could misinterpret their actions or speech? It is because over the past ten years, Americans have witnessed an alarming expansion of government powers — in particular, the intelligence collection powers of federal agencies such as the Federal Bureau of Investigation (FBI) or the Department of Homeland Security’s Customs and Border Protection (CBP) — without any transparency or accountability? While this expansion poses a risk to the civil rights and civil liberties of all Americans, this article will focus on how it impacts the lives and First Amendment rights of American Muslims.

FBI SURVEILLANCE OF AMERICAN MUSLIMS

Shortly after 9/11, FBI Director Robert Mueller made counterterrorism the Bureau’s top priority and directed agents in field offices around the country to gather data on Muslim and Arab communities in their regions.¹ Individuals in these communities were targeted for questioning and surveillance despite the absence of any individualized suspicion of wrongdoing. The targeting was based solely on a perception that — by virtue of their religion, ethnicity, race, or national origin — Muslim and Arab citizens and residents either might be engaged in, or might be able to provide information about, terrorist activity.

In late 2008, during the waning days of the George W. Bush administration, the Justice Department codified these new surveillance rules. Specifically, the Attorney General’s Guidelines for Domestic FBI Operations (Guidelines) were revised to consolidate previously separate guidelines for criminal, foreign intelligence, and counter-intelligence information. The Guidelines, issued by Attorney General Michael Mukasey, expanded the scope of the FBI’s domestic intelligence gathering, defining the agency’s functions as “extend[ing] beyond limited investigations of discrete matters.”²

While the revised Guidelines are problematic in many respects, particularly noteworthy is the procedure laid out for “assessments,” which are distinct from, and often precede, preliminary or full investigations. Assessments are a way of “obtaining information[,] ... detect[ing] ... threats to the national security[,] ... [and] prevent[ing] ... federal crimes.”³ Assessments conducted under the revised Guidelines require only an “authorized purpose,”⁴ and no factual basis for suspicion of wrongdoing is necessary — a far more lenient standard than was previously used.⁵ Indeed, in the absence of any factual basis for suspicion, it is unclear what circumstances warrant undertaking an assessment.⁶ The Guidelines also state that the “conduct of assessments is subject to *any* supervisory approval requirements prescribed by the FBI”⁷ (emphasis added) but contain no indication of these requirements.⁸

The FBI is free to use intrusive information collecting techniques during the assessment stage. Under previous Guidelines (issued by Attorney General John Ashcroft in 2002), during the “checking out of leads” phase, the FBI was allowed only to engage in “limited activity” to determine the need for further investigation.⁹

Agents were prohibited from using intrusive methods authorized during the later investigatory stages.¹⁰ Under the current Guidelines, however, even at the assessment stage, agents and informants are allowed to secretly attend meetings and events; to conduct so-called “pretext interviews,” in which agents hide their true identity; and to engage in indefinite physical surveillance of homes, offices, and individuals.¹¹ These invasive techniques disregard Americans’ right to be free from government intrusion into their daily lives in the absence of objective evidence to suspect illegal activity or wrongdoing.¹²

The Guidelines’ broad framework is implemented by the FBI’s Domestic Investigations and Operations Guide (DIOG),¹³ which not only mirrors many of the problems apparent in the Guidelines, but also expands the scope of permitted FBI actions. On September 16, 2009, Muslim Advocates filed suit seeking the public release of the DIOG.¹⁴ A heavily redacted version of the DIOG was released to the public shortly after the suit was filed.

Pursuant to the DIOG, FBI agents may engage in initial assessments without any particular “factual predication.”¹⁵ All that is required is an “authorized purpose,” which is vaguely defined as “less than ‘information or allegation’ as required for the initiation of a preliminary investigation.”¹⁶ Agents need not obtain approval before commencing an assessment, unless it pertains to a “sensitive investigative matter” involving “a religious or political organization, an individual prominent in such an organization, or a member of the news media.”¹⁷

The DIOG authorizes massive data gathering based on troubling assumptions and stereotypes about minority and ethnic communities. While it bars investigative activities based “solely on the exercise of First Amendment rights or on the race, ethnicity, national origin, or religion”¹⁸ (emphasis added), it allows investigative activities based partially on these factors.¹⁹ The DIOG authorizes the FBI to “identify locations of concentrated ethnic communities in the field office’s domain, if these locations will reasonably aid in the analysis of potential threats and vulnerabilities ... Similarly, the locations of ethnically-oriented businesses and other facilities may be collected ...” It further allows the “geo-mapping” of “ethnic/racial demographics.”²⁰

The DIOG authorizes the collection of behavioral data associated with certain minority communities, which can only be classified as ethnic, racial, and religious profiling. Such collection is permitted if the information is “reasonably believed to be associated with a particular criminal or terrorist element of an ethnic community.”²¹ For example, FBI agents are authorized to conduct surveillance of behavior such as the “cultural tradition of collecting funds from members within the community to fund charitable causes in their homeland at a certain time of the year.”²² This discussion of charity likely references the Muslim requirement of *zakat*, or alms giving. In other words, if all members of a terrorist group share a particular religious practice or characteristic, then anyone else who shares it is a fair target of government suspicion.²³ Additionally, the DIOG authorizes the collection and retention of data as they relate to other “ethnic” behaviors, including “finances by certain methods,

travel in a certain manner, work in certain jobs, or [coming] from a certain part of their home country that has established links to terrorism.”²⁴

The DIOG also authorizes the FBI to use informants and undercover agents in First Amendment-protected spaces, such as religious and political gatherings and organizations, without any evidence of wrongdoing. Specifically, Chapter 16 of the DIOG, “Undisclosed Participation,” permits agents to send undisclosed participants and undercover agents into organizations with no factual predicate that criminal conduct is underway.²⁵ FBI Director Robert Mueller described this power in testimony before the Senate Judiciary Committee: “The FBI must have a proper purpose before conducting surveillance, but suspicion of wrongdoing is not required.”²⁶ In other words, Chapter 16 allows the FBI to send undisclosed participants — informants or undercover agents — into religious, political, academic and other organizations where First Amendment rights of congregants or attendees are implicated. The conditions under which these powers may be used are not known because parts of this chapter remain undisclosed to the public.

The DIOG reveals a federal intelligence gathering framework that targets social, cultural, and religious behavior as an indicator of future criminal activity. Over the years this approach has resulted in unfair scrutiny and overbroad surveillance of the American Muslim community. Through Muslim Advocates’ contact with the community, it is clear that the FBI’s activities are causing fear and uncertainty among religious organizations. Muslim Advocates hears regularly from individuals who feel constrained from speaking and worshipping freely because they are afraid that their mosques are under surveillance and that their speech or religious practices may be the basis for government scrutiny.

The following are just two examples of how the FBI’s surveillance tactics are having an impact on the First Amendment rights of everyday Americans and their religious communities.

The first example is that of a young Muslim college student — by all accounts, an upstanding individual who was on the honor roll and involved in campus activities, as well as those of his local mosque. He had been in the United States since he was a child, but was out of status, something that the authorities knew for more than a decade. However, it was not until federal agents started investigating his local mosque that he was detained and questioned. He was threatened with deportation, then told that maybe he and the agents could help each other out: they would clear up his immigration issues if he agreed to report on the political and religious activities of members of his mosque.

In another instance, a community leader who is active in his local mosque met regularly with the FBI as part of the Bureau’s “community outreach.” One day the tenor of these meetings changed, and agents started asking him about the political and religious beliefs of other congregants, including their views on the Iraq war and the Palestine/Israel conflict. When he refused to answer — saying that he thought sharing such information would be inappropriate — they threatened him by suggesting they

would tamper with his mother-in-law's immigration status, commenting that "it would be a shame if her paperwork was somehow misplaced."

Muslim Advocates also often hears from American Muslims who are approached by authorities in their homes and offices because of political or religious postings on Facebook or involvement in their local mosque. American Muslim leaders are being asked by federal agents to report not just suspicious criminal behavior but also protected religious and political beliefs and activities. During one presentation in Houston last year, FBI agents asked community leaders to inform them of any Muslims expressing conservative views or adopting conservative religious practices.²⁷

These tactics chill free speech, practice, and association. They erode not only the rights of American Muslims but also the trust between many members of the community and law enforcement, as well as between community members and community organizations.

CUSTOMS AND BORDER PROTECTION QUESTIONING OF FIRST AMENDMENT PROTECTED BELIEFS AND ACTIVITIES

Muslim Advocates and other civil rights and civil liberties organizations increasingly are hearing complaints about disturbing questions that Customs and Border Protection (CBP) officers have asked American Muslims (or those perceived as such) returning to the United States after overseas travel. CBP officers are questioning such travelers about their religious and political beliefs and their religious associations, practices, and charitable activities, all of which are protected by the First Amendment. Some of the questions include the following:²⁸

- What is your religion?
- What mosque do you attend?
- Do you pray?
- Why did you convert to Islam?
- Why do you send your children to an Islamic school?
- What charities do you contribute to?
- What do you think about the war in Iraq and Afghanistan?
- What is your opinion of the Israel/Palestinian conflict?

While the government has a legitimate interest in verifying the identity of those entering the country and ensuring they do not intend to harm our nation, questions about religious and political beliefs and activities bear absolutely no relevance to these legitimate concerns. The practice of targeting a religious minority for such scrutiny damages the country's national security interests by wasting scarce government resources, generating false leads, and destabilizing the relationship between religious/ethnic communities and law enforcement.²⁹ Questions by federal law enforcement

officials about religious and political ideology also send the message that certain beliefs are not welcome here.

Muslims, and those perceived to be Muslim, who are questioned about their First Amendment-protected beliefs, activities, practices, and associations at the border fear that their responses will be used to unjustly target them for future law enforcement attention. They also worry that they may be subject to invasive and illegal questioning or investigative activities about their protected beliefs, associations, and activities, and they consequently feel reluctant to exercise their core freedom of speech and association rights as well as their right to freely practice their religion. By stigmatizing the religious and cultural beliefs and practices of an entire faith community, it is likely that this type of law enforcement scrutiny will “pervasively chill other community members’ willingness to engage in conduct that defines them.”³⁰

Unfortunately, CBP’s official policy on questioning about First Amendment-protected activities is unclear. The agency has not released any information about the scope of authorized questioning and whether there are any internal constraints or accountability mechanisms concerning queries that infringe on the First Amendment. All that is known is that CBP officers may inquire into “any matter which is material and relevant to the enforcement of immigration laws.”³¹ A CBP training manual also suggests that reasonable suspicion is not necessary to conduct a “routine” interview.³²

Courts have ruled that the government’s interest in screening individuals at the border is “paramount,”³³ such that Fourth Amendment requirements of probable cause and the issuance of warrants do not apply.³⁴ Routine border searches are presumed “reasonable” by virtue of the fact that they occur at the border.³⁵ Similarly, courts have refused to recognize a First Amendment exception to CBP’s broad authority to conduct searches of “expressive” materials,³⁶ and CBP officials are empowered to question individuals about the length and purpose of their travel³⁷ and the nature of their trip.³⁸

The case law does not, however, address the type of extremely intrusive questioning that is now taking place.³⁹ Complaints from Muslims returning to the United States suggest that their border searches and interrogations are far from “routine.” They take place in a coercive setting, with CBP agents sometimes intimidating innocent citizens by displaying their weapons or physically preventing them from leaving.⁴⁰ Unlike someone who is interviewed by law enforcement officials within the country, an interviewee at the border believes that he or she is not free to walk out of the interview, since he or she believes that entry into the country is contingent upon satisfying his or her interviewer.⁴¹ This point is starkly illustrated by one U.S. citizen’s interaction with a CBP officer who told her, “This is the border and you have no rights.”⁴² Some interviews have lasted as long as four hours, and in at least one case, CBP agents threatened that they would deny entry to a U.S. citizen if he did not comply with their demands.⁴³ This last incident is particularly disturbing, since the Supreme Court has long held that citizens have the constitutional right to

re-enter the country.⁴⁴ It also represents a dangerous breach of longstanding limits on executive power.⁴⁵

Since CBP's policies governing these interviews are largely unknown, various organizations have mounted efforts to have them disclosed. In 2007, for instance, the Asian Law Caucus and the Electronic Frontier Foundation filed a Freedom of Information Act (FOIA) request with the Department of Homeland Security (DHS) seeking release of agency records, including any policies or procedures, about border questioning.⁴⁶ Despite turning over 600 pages of records, the agency provided no documents that revealed any constraints on such questioning.⁴⁷ More recently, in 2010, Muslim Advocates and the American Civil Liberties Union (ACLU) sent a formal complaint to the Inspector General of the Department of Homeland Security (DHS), asking for an investigation into whether DHS and/or CBP has a codified policy that allows First Amendment-targeted questions, and if so, whether there are any safeguards to ensure that the queries comply with constitutional requirements.⁴⁸ In addition, Muslim Advocates and the ACLU filed FOIA requests on behalf of seven people who have been targeted repeatedly for prolonged interrogations about their First Amendment-protected beliefs and activities.⁴⁹ In response to the FOIA requests, DHS and CBP released limited documents that revealed no information about the existence of, or constraints on, any policies or procedures governing First Amendment-related questioning. Furthermore, the IG declined to open an investigation into CBP's practice of questioning travelers.

In 2009, Muslim Advocates published a report, *Unreasonable Intrusions: Investigating the Politics, Faith & Finances of Americans Returning Home*, which profiled dozens of people who have been detained and interrogated at the border. One of the stories in the report aptly illustrates the profound impact these federal practices and policies have on the daily lives of Muslims. An American citizen traveled to India on business and stopped in Pakistan to visit his ailing mother. Upon returning to the United States, he was detained, searched, and interrogated for more than three hours. He was asked about donations to his place of worship in the United States; the agent went so far as to tell him that he should not have made the contributions. He was asked why he enrolled his children in an Islamic school. He was questioned about the identities of people in photos he had in his wallet. His computer was seized and copied, and his cell phone was confiscated and mailed back one month later, broken and unusable. But the search and interrogation did not stop there. A few weeks after his border interrogations, FBI agents came to his home. They subjected him to a lengthy interrogation about information he had provided to CBP agents at the border.

This incident is significant, not because it is the most outrageous episode of its kind, but because it illustrates the chilling effect this type of questioning has on innocent U.S. citizens. "I took a business trip and visited my sick mother, and, because of that, I am treated like a criminal — I was questioned about my faith and family when I was coming home to my country and then in my own home," the

traveler said, in seeking the advice of Muslim Advocates. “I have a trip scheduled to go to Mecca for the pilgrimage — I’m nervous about my trip back, and my family doesn’t want me to go because they are worried about what will happen to me at the airport when I come home. We don’t want any more trouble. Should I cancel my pilgrimage?” This is but one story of one American Muslim. Other such stories, sadly, abound. In our country today, interrogations, harassment at the border, and surveillance of religious spaces are the daily reality for many American Muslims.

RECOMMENDATIONS

To address federal domestic intelligence gathering policies that violate the First Amendment rights of Americans, Muslim Advocates makes the following recommendations:

- The U.S. Attorney General should strengthen the Department of Justice’s 2003 Guidance Regarding the Use of Race by Federal Law Enforcement Agencies (“Guidance”) to include religion and national origin as protected classes; remove the national security and border integrity exception to the prohibition on profiling; and explicitly state that the ban on profiling applies to intelligence activities carried out by law enforcement agencies subject to the Guidance.
- The Justice Department and FBI should revise the Attorney General’s Guidelines and the FBI’s Domestic Investigations and Operations Guide to require a factual predicate before commencement of an assessment and before racial and ethnic information gathering, and to require heightened levels of supervisory approval and factual predicates for investigations that implicate First Amendment-protected activity.
- Congress should enact legislation, such as the End Racial Profiling Act, which bans racial, ethnic, religious and national origin profiling by federal, state and local law enforcement. Such legislation should contain language that explicitly prohibits profiling in the types of law enforcement activities described above, including FBI interviews and those by CBP agents at the border; searches of persons and/or property; and data collection and analysis/assessment of racial, ethnic and faith communities.

- Congress should enact legislation to place subject matter limits on CBP interrogations, making clear that questions about religious beliefs, political views, and associations with lawful persons and organizations are neither legitimate subjects for scrutiny, nor related to security concerns. The legislation should prohibit the use of race, ethnicity, national origin, or religion in deciding upon the scope and substance of investigatory or other law enforcement activity, except when there is reliable information, relevant to the locality and period of time, that links a person of a particular race, ethnicity, national origin, or religion to an identified criminal incident or scheme, and where reasonable suspicion, based on factors unrelated to race, ethnicity, national origin, or religion, is present.
- The Department of Homeland Security and/or Customs and Border Protection should issue a policy directive that prohibits officers from questioning travelers about their religious and political beliefs, associations, religious practices, charitable activities, and other First Amendment-protected activity during the course of border inspections and interrogations.

PROTECTIONS FOR FIRST AMENDMENT-PROTECTED SPEECH AND RELIGION WHEN INVESTIGATING TERRORISM

Kate Martin

Director

Center for National Security Studies

My purpose is to outline some of the general questions raised by FBI investigations that concern religious, political, or other speech activities and beliefs protected by the First Amendment.

This phenomenon is not limited to investigations targeting American Muslim communities. The first comprehensive critique of FBI targeting of groups for their political activities was in the 1976 Church Committee reports, which outlined the illegal surveillance and even “dirty tricks” used by the FBI for decades to target the civil rights movement and the anti-war movement.¹ Even after the reforms prompted by those revelations, including the Attorney General’s Guidelines for Domestic FBI Operations, the FBI targeted groups opposed to the administration’s policies in Central America in the 1980s.² As recently as September 2010, the Inspector General of the Justice Department documented FBI investigations of Quaker groups, anti-war groups, and others.³

FBI investigation of groups involved in First Amendment-protected activities is in some ways an intellectually and practically difficult problem when the FBI is indeed attempting to investigate criminal activity. (Of course, if the nexus between investigating groups and preventing criminal activity is missing, then the problem is a much simpler and more basic one: political spying by the government.) I realized the difficulty involved when I worked on this issue for the first time in connection with the FBI’s investigation of the murders of doctors who performed abortions. There were religious and advocacy groups who preached and advocated that abortion was murder and that one was morally justified — maybe even morally compelled — to stop the “murder of innocents”; some preached that violence to stop abortions could be justified. The issue for those of us in the civil liberties community was whether the FBI, in trying to find the killers of abortion doctors, could properly investigate such anti-abortion groups based solely on their rhetoric. Is it enough to justify an investigation that a group has embraced the position that killing doctors is morally

defensible or morally compelled? Our answer at the time was no — such speech is not enough to justify an FBI investigation of either the group or its members.

The question then arose, what additional facts should be necessary to authorize the FBI to open an investigation? At that time, in the mid 1990s, we hypothesized that it might be sufficient to open an investigation of an abortion protester who engaged in this type of rhetoric if the person also purchased a gun. We did not realize at the time that buying a gun is a constitutionally protected individual right⁴ — which means that this answer may no longer apply in the same way.

There is another hard problem in this field: we once believed that we could easily articulate the legal distinction between criminal conduct and protected speech. On the one hand, the government may properly criminalize the planning of violent acts. On the other hand, as spelled out in the seminal case of *Brandenburg v. Ohio*, defense or even advocacy of violence is protected by the First Amendment and may not be made a crime, except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action.⁵ But the constitutional line between activity that can be criminalized and that which may not be criminalized because it is protected by the First Amendment, has become blurred with the post-9/11 expansion of material support laws to cover speech-related activities as upheld by the Supreme Court in *Holder v. Humanitarian Law Project*.⁶

If we, as a society, have a rule that says law enforcement has to focus on criminal conduct as its objective — a rule that used to hold sway more than it does now — then how far afield from criminal conduct may law enforcement go in conducting investigations intended to prevent criminal conduct before it happens? That is the hard question before us today. Throughout our history, we have confronted violence carried out for political, ideological, or religious reasons. There is obviously a strong national interest in stopping such violence before it occurs. At the same time, the Bill of Rights is properly understood as recognizing that government surveillance and investigation of religious or political views is likely to chill the exercise of constitutionally protected rights.

Since the changes in the law made after 9/11, we must also worry that the chilling of speech may not be the only result of government surveillance. In his remarks earlier in this symposium, Fritz Schwarz described efforts by the FBI during the COINTELPRO days to disrupt organizations, and to harass or even destroy people, who held disfavored views — which it did using illegal methods including wiretaps and “black bag jobs.”⁷ Fortunately, the FBI no longer operates like that. In a sense, though, it may be because the FBI no longer has to. There has been such a major expansion of the criminal law that the government has a much larger number of *legal* tools to use against people they identify in the investigative process as engaging in disfavored speech (or being members of a disfavored political or religious group).

One such tool is to selectively enforce certain laws against the individuals in question. A case in point is the use of immigration law after 9/11. Immigration law, like the law prohibiting underage drinking, is an area of law where there exists what

some have labeled an “enforcement deficit” — i.e., many more violate the law than are prosecuted. In the first three months after 9/11, 1,100 people who were suspected of being Arab or Muslim were rounded up and jailed. Their perceived religion or ethnicity was the deciding factor in who was imprisoned. The majority, not being citizens, were charged eventually with being out of status under the immigration laws — charges that almost certainly would not have been brought if the terrorist attacks of 9/11 had not occurred and they were not Arab or Muslim. Some voluntarily left the country, even though they may well have had the legal right to stay, and many were forcibly deported.⁸

In a conversation with a high-ranking Justice Department official, I raised the objection that this was religious and racial discrimination. We are a country with 11 million people out of status; when the government decides to target a major part of its immigration enforcement efforts against Muslims and Arabs, that is discrimination. The official adamantly denied the charge. He defended the practice as a reasonable allocation of resources, given that the government cannot deport all 11 million undocumented persons. That, indeed, was the primary counter-argument in the debate over the post-9/11 round up of Muslims: there are so many people who are out of status that enforcement resources have to be targeted in some way, and it is appropriate to do so on the basis of the religion or ethnicity common to many Al Qaeda terrorists. This problem of discriminatory enforcement in areas of the law where there is an enforcement deficit needs to be understood as linked to the problem of surveillance of First Amendment-protected activities.

I also want to address briefly Prof. Geoffrey Stone’s point that the chance of successfully challenging this type of surveillance in the Supreme Court is quite small. That leaves us with two possible fixes: congressional action and/or the administration changing the Attorney General’s Guidelines for Domestic FBI Operations. One of the purposes of the Guidelines, when they were first adopted, was to protect First Amendment activities from untoward surveillance. In part, the Guidelines accomplished this by prescribing the rules for when the FBI could open investigations; when specific investigative techniques could be used; when FBI agents could ask questions, having identified themselves as FBI; and when they could use the more intrusive technique of not identifying themselves as an FBI agent, or even recruiting someone who was not an FBI agent to act as a covert informant inside a place of worship. The Guidelines contained a series of rules intended to limit the use of such techniques and to require a factual predicate — i.e., the existence of some evidence or basis for suspicion that a crime has been committed or is being planned. Since their adoption more than thirty years ago, those rules have been watered down significantly, especially during the past administration.⁹

One of the key aspects of the Guidelines, however, is that historically they have gone beyond simply authorizing or prohibiting different investigative techniques. They also have had provisions specifically intended to protect against the unwarranted investigation of First Amendment-protected activity. Accordingly, before 2002, the

Guidelines provided that if the FBI planned to investigate political or religious speech or activity — to use Geoffrey Stone's example, if it wished to send someone into a mosque for the purpose of listening to a sermon — it needed to meet a heightened standard because of the potential chilling effect of such investigation on First Amendment-protected activities.¹⁰

Former Attorney General John Ashcroft rejected that principle as absurd. He argued that if a member of the public can go into a mosque, why should there be any limitation whatsoever on the FBI attending a service? That view was reflected in the changes made to the Guidelines eroding the protections for speech and religion in such circumstances.¹¹

The erosion of protections in the Guidelines happened at the same time that other significant changes were made in FBI operations. Since 9/11, the mission of the FBI has changed. Indeed, both the FBI and local law enforcement are now focused on the idea that religiously motivated violence is somehow the major domestic threat to the United States. At the same time, there has been a vast increase in technological capabilities for surveillance, making it much simpler and cheaper to surveil many more people than before. And there has been a vast increase in government resources put into law enforcement. I am afraid I am less sanguine than Matthew Waxman¹² that the future architecture of law enforcement and intelligence will be driven by the nature of the threat. What we have seen, in my view, is that the architecture is based on a number of factors — including partisan debates, an unfortunate influence that is not likely to lead to the best possible answers in terms of mission and effectiveness.

Finally, this is not a problem just for the FBI or just for this particular moment in our history. How to enforce the laws against terrorism effectively without chilling constitutionally protected speech or religion is a perennial problem. After all, it is very hard to find an actual terrorist, who is presumably trying to hide; it is much easier to focus on people who may share or appear to share some of the same ideas that are presumed to motivate the terrorist. And there is always a strong bureaucratic incentive to do *something*.

What perhaps adds a new dimension is the fact of increased criminalization, with more individual activities having been outlawed by the state.¹³ I do not believe we have really examined or understood the full implications of that development, not just for prosecutions, but also for investigations. I tend to think of this as the Raskolnikov problem, insofar as Raskolnikov deliberates until the very moment of the crime whether he should or will murder the old woman.¹⁴ The FBI's mission is to prevent the next crime or terrorist attack before it happens, a mission I wholeheartedly endorse. But what I take from the story of *Crime and Punishment* is that human beings decide at different points whether they are in fact going to go forward and murder the old lady; that having free will means that a person may decide not to commit the crime they have been considering. The criminal law used to be more attuned to this problem. As a society committed to individual responsibility and freedom, we do not criminalize thoughts of violence, unlike totalitarian countries.

Historically at least, we understood that the law could only outlaw some actual step taken along the path to violence, not mere thoughts or speech. Recent changes challenge that fundamental notion. That challenge is not well-understood or debated — perhaps because the original understanding about the relation between free will and government punishment is insufficiently respected in the current climate in which we try to prevent the next terrorist attack.

PART THREE

**REGULATION OF DOMESTIC INTELLIGENCE
GATHERING AND POTENTIAL FOR REFORM**

INTRODUCTION

Emily Berman
Visiting Assistant Professor
Brooklyn Law School

The third part of the symposium took up the issue of regulating domestic intelligence-collection efforts by law enforcement. It explored the sufficiency of current regulations and contemplated some possible reforms of those regulations.

The rules governing domestic intelligence collection by law enforcement derive from several sources. First there is, of course, the Constitution and in particular the Fourth Amendment,¹ which bars unreasonable searches and seizures. The First² and the Fourteenth Amendments³ can also come into play if, for example, intelligence collection affects expressive, religious, or associational rights, or if it is carried out in a way that runs afoul of the Equal Protection Clause.

But as Professor Aziz Huq illustrated in his remarks,⁴ these constitutional limits are often relatively toothless in the modern intelligence collection context. Consequently, both Congress and the states have enacted statutes, such as the USA PATRIOT Act, the Foreign Intelligence Surveillance Act, and Title III of the criminal code, that create limits on domestic intelligence gathering over and above the constitutional minimums.

In addition to these relatively familiar sources, there are others that are less known. Internal executive branch guidelines and presidential directives, implemented in agencies like the Department of Homeland Security and the Department of Justice, make up a large portion of the body of rules that actually shape how law enforcement agencies collect intelligence in the United States. These are guidelines like the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources or the Attorney General's Guidelines on FBI Undercover Operations. Of particular relevance to this symposium are the Attorney General's Guidelines for Domestic FBI Operations.

Guidelines limiting the FBI's domestic intelligence collection activities were originally implemented in 1976 in the wake of revelations of widespread inappropriate — and often illegal — FBI intelligence collection on Americans in the 1960s. These

initial Guidelines limited the FBI's intelligence collection role by requiring that all the Bureau's investigative activities be closely linked to actual wrongdoing or violence. In so doing, the Levi Guidelines, as they were known, essentially removed the FBI from the domestic intelligence collection business.

Over time, the Guidelines have evolved. For nearly thirty years, the limits on FBI activity were incrementally and modestly expanded, permitting some intelligence collection but simultaneously requiring close oversight of those activities, placing strict limits on the means that could be used, and limiting the length of time an investigation could last if it did not yield indicia of criminal activity.

Since 9/11, the expansion of FBI powers has accelerated. In the wake of the terror attacks in New York, Washington, D.C., and Pennsylvania, the FBI shifted its focus from solving crimes and prosecuting perpetrators, to preventing crimes — particularly crimes of terrorism — before they could cause harm. The current Guidelines unequivocally state that “[t]he FBI is an intelligence agency as well as a law enforcement agency.”⁵

As the FBI's focus has returned to intelligence collection, the Guidelines' substance has come to reflect that focus. In addition to the FBI's traditional investigative role, in the post-9/11 era federal agents have taken on the responsibility of analyzing information to “identify and understand trends, causes, and potential indicia ... of threats ... that would not be apparent from the investigation of discrete matters alone.”⁶ To effectively carry out this portion of its mission, the FBI must collect, retain, and study vast amounts of information.

One of the most significant post-9/11 changes in this area came as part of the Attorney General's Guidelines for Domestic FBI Operations implemented in 2008 by Attorney General Michael Mukasey. In order to facilitate intelligence collection and analysis, these Guidelines created a new investigative phase called an “assessment.” An assessment is an investigative stage that may be initiated without any concrete indication of wrongdoing or threat to national security. This means that, for the first time since the Guidelines were initially implemented in 1976, an investigation can begin in the absence of any factual basis for suspicion.

Not only do assessments permit investigations in the absence of suspicion, but investigators are also empowered to employ highly intrusive investigative techniques in carrying out assessments. For example, government agents can send informants to collect information at political meetings or religious services; can hide their status as federal officials in interviews with a target's family, neighbors, or business associates; can station agents outside a target's home or office — and even have them followed (perhaps even electronically) — so that their movements are tracked day and night.

Granting these sorts of powerful authorities to the FBI may seem the logical response to the threats that we face and the potentially calamitous consequences of failed prevention. But when designing regulation to govern FBI activities, it is important to keep two things in mind. First, there is the Bureau's history. In addition to the excesses of wiretapping, infiltration, and harassment exposed in the 1960s,

there has been ample evidence of post-9/11 excess as well. A seemingly never-ending series of reports from the Justice Department's Office of the Inspector General has documented departures from rules governing the use of national security letters, the acquisition of telephone records, investigation of First Amendment-protected activity, and even the rules about learning the rules.⁷ Second, no set of regulations or investigative practices can guarantee that there will not be another catastrophic terrorist attack. At some point — a point that different policymakers would locate in different places — the security benefit of increased government power is outweighed by the risks to civil liberties posed by government actions.

Given the FBI's track record, the changes implemented by the 2008 Guidelines proved quite controversial and remain subject to heated debate. Some argue that the powers granted by the Guidelines are necessary to protect the security of the homeland. Others argue that the authorities extended to the FBI are subject to insufficient oversight and create risks to civil liberties that are simply too great.⁸

It is not surprising that these rules spur controversy. Efforts to determine the appropriate contents of the rules governing domestic intelligence investigations raise important questions to which there are no easy answers. For example, what should a preventive focus mean for investigations? What, if any, public spaces or private information should be off-limits to intelligence collection activities? If potential terrorists might be lurking around every corner, how does the law enforcement community decide where to deploy limited resources? Does adding to law enforcement's intelligence collection power increase the likelihood of predicting violent activity? Does it increase the likelihood of widespread civil liberties violations? Are there other ways to achieve the law enforcement and intelligence benefits of intrusive investigations through less intrusive means?

During the symposium, former Deputy Director of the FBI National Security Branch Philip Mudd⁹ elaborated on some of the challenges posed by the intelligence community's preventive focus. As an initial matter, he pointed out, the decision to focus on prevention was not a choice made by the FBI. The Bureau was instructed, by Congress and by the Director of National Intelligence, to adopt a preventive counterterrorism policy. Preventive investigations, he argued, cannot be tethered to proof of criminal activity. Waiting for proof of criminal activity is — by definition — not preventive, it is reactive. And this means that agents are certain to drag innocent people into investigations. So preventive efforts cannot be coupled successfully with attempts to spare innocent Americans from FBI scrutiny.

But perhaps the greatest challenge Mudd saw in this area stems from the unreasonable expectation of 100 percent prevention success imposed on the intelligence and law enforcement communities. They are expected to avert any and all terrorist threats before they manifest in damage to life or property. These lofty expectations place enormous pressure on investigators to push the limits of the rules in order to collect potentially relevant information. This pressure is exacerbated by the threat of being blamed — in congressional hearings, in front of the C-SPAN

cameras, in a government report, or in the court of public opinion — for what went wrong if there is an attack. Fear of this public shaming not only incentivizes aggressive intelligence collection but also encourages ill-supported investigations and reluctance to close an investigation even if it has failed to yield actionable information.

To partially address some of these problems, Mudd advocated for a more effective mechanism for *ending* intelligence investigations. In his view, the FBI has too many cases open simultaneously, but agents are leery of closing any one investigation for fear of false negatives. Many reform proposals and expressions of opposition focus on the rules regarding the opening of investigations. But extending unfruitful investigations also risks collecting information on innocents unnecessarily and draining law enforcement resources. A process for ending investigations that would give agents a paper trail to point to, should the subject of the investigation later turn out to pose an actual danger, might go a long way in putting a halt to unnecessary investigative activity.

Former Assistant General Counsel of the Central Intelligence Agency Suzanne Spaulding¹⁰ enthusiastically agreed with Mudd's diagnosis of the problem as unreasonable expectations. In her view, counterterrorism is about risk *management*, not risk *elimination*. A successful terrorist attack does not necessarily mean that something went wrong or that someone failed to do their job. As a society, we need to internalize the reality that giving more power to government does not ensure perfect safety, and public officials need to articulate this fact as well.

In addition to the challenges that preventive policing poses, the panel explored some of the other risks that domestic intelligence collection regulation must work to prevent. These include privacy-related concerns and the risk of reliance on racial, ethnic, or religious profiling. The overriding question is how to design a regulatory scheme that is both effective in countering the serious threat we face, while simultaneously minimizing these varied concerns. Accepting the impossibility of 100 percent prevention as suggested by Philip Mudd and Suzanne Spaulding would be one step in the right direction. The chapter's contributors suggest that, given the current preventive stance of law enforcement, we should explore some possible alternative means of placing appropriate constraints on government activity. Shahid Buttar suggests increased focus on the sufficiency of state and local regulations, while Professor Huq contemplates a different way of thinking about what privacy rights the Fourth Amendment should protect. Their remarks on those topics follow this introduction.

While each panelist came to this issue from a different perspective, and each had unique concerns and emphases, there were important points of agreement. First, there was consensus that the expectation of absolute prevention is not only unrealistic but also unhelpful. It leads to inappropriate continuation of unproductive investigations, over-inclusion of names on watch-lists, and the use of tactics with insufficient safeguards. Second, there was enthusiastic agreement that regulations should prohibit religious profiling, which all the panelists decried

as ineffective and counterproductive. These points of consensus could form the basis of an effort to reintroduce some limits and accountability into domestic intelligence collection efforts by law enforcement.

NATIONAL SECURITY VS. DEMOCRACY IN AMERICA

Shahid Buttar
Executive Director
Bill of Rights Defense Committee

As we discuss the past decade's assault on constitutional rights, it is important to consider discrete events in the context of some broader themes.

BROAD SOURCES AND IMPACTS: NO ONE PARTY, NOR ONE VULNERABLE COMMUNITY

The sources of recent expansion in the FBI's powers have transcended presidential administrations, as well as political parties. Both Democrats and Republicans share responsibility for the Bureau's contemporary excesses.

The targets of the FBI's recent abuses have also transcended communities. Muslims, Arabs, and South Asians are hardly the only groups to endure rights violations unaddressed by courts. Environmental and peace activists have also suffered at the Bureau's hands.¹ Concerns about the return of COINTELPRO are not driven by the marginalization of a particular community, but rather by a disturbing pattern of expanding abuses that has grown to undermine the rights of Americans from all walks of life.

In the wake of House Homeland Security Chairman Rep. Peter King's (R-NY) thoughtless hearings about alleged radicalization in domestic Muslim communities, a debate has emerged about the impact of domestic intelligence collection on the American Muslim communities. But if you look at the federal prisons, you will not find only Muslims accused of terrorism there. You will find a lot of other Americans, too, including those with European ancestry accused of terror offenses relating to their environmental advocacy.²

At the moment, the FBI is pursuing terror investigations of dozens of peace activists, labor organizers, and Occupy participants across the country. Recently, in the summer of 2012, Occupy Cleveland activists were charged with terror offenses in connection with an alleged plot to bomb a bridge.³ In Chicago mere weeks later, five more were abducted and held without access to counsel before prosecutors explained

an alleged bomb-making plot based on the activists' possession of equipment for brewing beer at home, not unlike that used in the White House.⁴

Years before, in the months preceding the 2008 Republican National Convention in St. Paul, Minnesota, the FBI sent an agent posing as a single lesbian mother to infiltrate several groups of protesters.⁵ In the wake of the Supreme Court's spring 2010 decision in *Holder v. Humanitarian Law Project*, prosecutors and investigators seized on their new powers to assign associational guilt, raiding homes and offices in Minneapolis, Chicago, and Los Angeles, before dragging two dozen activists before secret grand juries to testify about their First Amendment-protected activities.⁶ Muslims, for better or worse, at least enjoy plenty of company.

When we consider the problem in terms of information sharing, in particular, the community that seems most at risk is the Latino community. Information sharing between local police departments and federal agencies, particularly Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP), has prompted a mounting humanitarian crisis.⁷ The FBI plays a curious (and widely overlooked) role in these immigration enforcement efforts, driven by DHS policy responses to cities and counties around the country trying to opt out of ICE coordinated programs in order to protect the rights of their residents.⁸

ICE has generated enormous controversy through its so-called "Secure Communities Initiative," (S-COMM) through which local police share fingerprint and arrest data with ICE which, in turn, detains and deports thousands even before conviction of any criminal offense. After Arlington County in Virginia and San Francisco and Santa Clara Counties in California voted not to participate in ICE's program, the terms of the initiative changed.⁹ Although S-COMM was initially described as a collaboration between local and federal law enforcement, ICE decided to gather biometric arrest data from the FBI instead. Now S-COMM is touted as *federal* inter-agency cooperation.¹⁰

Policymakers, journalists, and advocates should not artificially limit their treatment of the detrimental consequences of domestic intelligence gathering and information sharing. The consequences are much graver and impact many more (and different) people than observers tend to presume.

DRAGNET SURVEILLANCE: THREATENING INDIVIDUAL RIGHTS AND DEMOCRACY

Broad domestic intelligence gathering poses a danger not only to vulnerable groups (of almost any sort, whether ethnic, religious or political minorities) but also to democracy as a whole. In addition to facilitating profiling (and thus violating fundamental norms of equal protection), dragnet surveillance presents other dangers that ultimately undermine civil society.

One risk is over-inclusion: collecting information, particularly in an invasive way or about constitutionally protected activity like political speech, from individuals who are not genuine security threats. Of course, these tactics abuse the civil rights

of particular individuals and the communities they represent. But by systematically imposing a chilling effect on the voices and actions of dissidents, the increasingly aggressive intelligence collection regime deprives the rest of our society of their views.

When our government inhibits legitimate First Amendment-protected activity of the sort that the Bill of Rights was written to protect, it is not just the people whose speech (or assembly, or association, or redress of grievances) is constrained who suffer, nor even others who censor themselves (what courts have long recognized as “chilling effects”) as a result. Everyone suffers when our institutions make decisions without being informed by the ideas and perspectives of dissidents. Communities advocating policy changes with respect to foreign military intervention, environmental degradation (relating to climate change, as well as shale gas extraction through hydraulic fracking), federal banking policies, the role of corporations in our society, the student loan crisis, or any number of other issues have endured suppression of their expression by national security agencies.

Various and sundry policies adopted by Congress, presidential administrations, private corporations, and even courts, may well have proven different had we prioritized a robust free market for ideas above the self-serving backroom demands of our national security establishment.

The inflated position of that establishment in setting its own rules appears even more bizarre when viewed in light of the agencies’ failure to secure the success of their own missions.

NATIONAL SECURITY RISKS

From a national security perspective, law enforcement assumptions about the sources of terrorism undermine efforts to prevent violence. For instance, neither the 2010 suicide attack in Austin, Texas, by a man who flew a plane into a government building,¹¹ nor the 2009 assassination of a doctor during a church service in Kansas City, Missouri,¹² nor the 2012 massacre of Sikhs in Oak Creek, Wisconsin,¹³ were committed by individuals from groups commonly subjected to counter-terror scrutiny. These threats escape the aggressive tactics often employed by counterterrorism and intelligence agencies because they do not fit the faulty race, faith, or political models profile driving counterterrorism surveillance.

There are other dangers beyond missing potential threats. Among the most demonstrable are the risks of eroding communities’ trust in law enforcement institutions and thereby diminishing access to human intelligence. Ironically, this consequence of heedless domestic intelligence collection may produce precisely the sort of radicalization about which Representative King and others are so concerned. The genius of the First Amendment is that it brings into the public sphere grievances that might otherwise be expressed through violence. Yet, by profiling particular communities or presuming guilt by association, authorities risk alienating communities susceptible to militant recruitment and creating opportunities for violent individuals

within their midst to recruit others frustrated by their own marginalization.

Data mining is another technique of questionable efficacy. Data mining is predicated on two faulty assumptions. The first is that particular precursors can be identified that lead to violent extremism. Precursors to violence were the principal subject of an NYPD report in 2007¹⁴ later discredited by the Brennan Center.¹⁵ While that particular report was ridden with fallacies and faulty reasoning, other efforts since have aimed to identify specific behaviors that presage later violence.

This theory presumes that all terrorists follow a predictable course of behaviors that transforms them from law-abiding citizens to mass murderers. Unfortunately, human behavior is not that simple. Comprehensive studies of terrorist biographies show that there is no consistent pattern of transformation.¹⁶

Data mining also relies on having sufficient information to generate accurate predictions. In the commercial context, data mining is a powerful tool and this sort of predictive use of it works well. For instance, with enough data, we can predict the likelihood that customers who buy milk will also buy other products, because there are a sufficient number of data points to derive reliable predictions.

But terrorist attacks are too infrequent to enable any reliable determinations about recurring precursors.¹⁷ Without a dramatically higher number of attacks to analyze, generalizable conclusions about counterterrorism based on data mining will inevitably be inaccurate.

Unfortunately, the flawed approach employed by counterterrorism agencies is plagued by even worse problems. For instance, FBI informants have infiltrated faith institutions to bribe heroin addicts and schizophrenics to participate in plans that the informants initiate, leading to “terrorist plots” that are essentially contrived.¹⁸ Stories based on such facts are routinely trumpeted in the media as examples of institutional success. But prosecutions of defendants accused of joining plots hatched by FBI agents or informants focus on consumers, rather than producers or distributors, of terrorism. This distinction is well-understood by law enforcement professionals involved in drug prosecutions, or any other sort of contraband.

Consumers of illicit drugs or weapons are of course subject to prosecution, but investigators rarely focus their attention on them because they play a limited role in the “market” for those materials. In fact, if consumers draw the notice of law enforcement, they are often used as intelligence assets to identify their suppliers, and ideally, the original producers. Infiltrating mosques with informants and prosecuting people unsophisticated enough to take FBI bribes to join law enforcement-generated plots does not hold similar promise. Rather than targeting the “producers” or “distributors” of terrorism (weapon-makers and militant recruiters, respectively), the current model of artificial cases only ensnares potential consumers.

On the one hand, “consumers” of terror plots do present security risks, to the extent that they could hypothetically pose a threat to public safety were they recruited by real militants. On the other hand, by luring potential consumers of terrorism generated by others, rather than terrorists who actually initiate plots, the Bureau

abandons the goal of tracing terror networks to their sources. The FBI has resigned the legitimate counterterrorism mission of finding and destroying international terror networks in favor of the national security equivalent of busting junkies for sniffing glue.

Moreover, by contriving fake terror plots, law enforcement agencies stack the deck, skewing the database of information that could otherwise be used to discover actual terrorist threats. The result is the equivalent of an accountant cooking the books. The knowledge gained from these manufactured cases raises the troubling possibility of directing counterterrorism efforts away from genuine precursors of violent extremism, and toward other activities that have little utility.

The modus operandi of traditional counter-terror efforts thus undermines its own aims in two dimensions. In the near term, infiltration-driven investigations overlook producers and distributors of terror in favor of preying upon people merely susceptible to suggestion. Furthermore, efforts to contrive cases pollute the pool of potentially actionable intelligence over time.

SOLUTIONS: FEDERAL V. LOCAL

These problems are not insurmountable. There are solutions.

Before addressing those that are viable, it is worth first eliminating some that are not. Several symposium participants discussed the insufficiency of the First and Fourth Amendments as loci for protection. Prof. Aziz Huq mentioned that our constitutional laws are generally under-enforced. Prof. Geoffrey Stone noted the doctrine surrounding standing has emerged as an often insurmountable barrier impeding access to justice. The upshot is that Article III courts cannot protect constitutional rights in this context, whether due to standing barriers or other (jurisprudential or practical) limits on access to justice.

One possibility, which Prof. Stone hinted at, entails changing existing federal policy to address these shortcomings, either by enacting legislation or altering administrative regulations that would raise rights above the current constitutional baseline. Unfortunately, however, the particular federal policy at issue in the FBI abuses detailed here (the 2008 Mukasey Guidelines) is not seriously under review within the Justice Department.¹⁹ Nor has Congress shown much interest in enacting a statutory charter to constrain the FBI. Changes to federal policy, then, are unlikely to emerge as solutions to these ongoing abuses.

In contrast, state and local laws that impose institutional limits on law enforcement offer a great deal of promise.

As a practical matter, the number of agents employed by local agencies are an order of magnitude (and then some) greater than their federal counterparts. Around the country, state and local police employ more than 800,000 officers. In contrast, the primary federal investigative institution, the FBI, has 35,000 employees, only some of whom are operational investigative agents. In other words, state and local

reforms might offer many opportunities to raise rights above the federal floor, while important battles that remain to be won are waged in Washington.

Local reform initiatives are attractive not only because of the sheer volume of abuse potentially meted out by local and state law enforcement agencies, but also because municipal and state legislators are more accessible and more empowered than members of Congress.

Congress is notoriously inaccessible. Money, or a large number of motivated constituents, are required even to reach a member of Congress, let alone secure enough of her focus to enable serious consideration of an issue. While federal legislators' aides help them wade through complicated issues, they tend to have little relevant experience themselves, resulting in a predictable focus on whatever issues are set by the policy discourse, rather than ideas proposed by constituents.²⁰ The volume of legislation Congress considers is so overwhelming that many legislators never even read bills before they come up for a vote.²¹

Members of Congress are also relatively disempowered. Even if a constituent is able to attain the support of a federal legislator, that legislator must then convince hundreds of colleagues in order for a bill to become law. The committee structure also narrows access, since only Representatives or Senators with a committee assignment relevant to a particular issue (or a leadership position in their party) have the power to set the agenda.

None of these problems plague city councils. First, council members represent vastly fewer constituents, which makes it easier for those they represent to secure meetings with them. Second, local representatives often lack staff, and accordingly welcome the opportunity to hear substantive proposals from supporters. Finally, they have fewer colleagues to persuade in order to pass a proposal. New York, the largest city in the United States, has only fifty one council members, less than one-eighth of the members of the House of Representatives, let alone the full Congress.

Local and state legislatures are thus more viable targets for reform proposals. It is easier to reach individual officeholders, and relatively speaking, they have a greater ability to influence their respective institutions.

It may seem, at first glance, that local reforms would inevitably prove inadequate to constrain abuses by federal agencies. After all, only Congress or the Department of Justice can constrain the FBI. Yet, as a practical matter, the scale of resources available to federal agencies is vastly greater when collaborating with local counterparts than when acting alone.

Cooperation by local agencies is accordingly the Achilles' heel of the national security establishment. As more local jurisdictions reclaim control over their law enforcement agencies, the resources available for unrestrained federal initiatives will fade, at the same time as a normative shift will build that could ultimately alter the federal paradigm, as well.²²

SOLUTIONS: PARTICULAR PROVISIONS

One broad set of measures local legislatures could impose are provisions to detect and protect against potential profiling based on race, religion, national origin, faith, or political belief. Although there has been a consensus on the evils of profiling for a decade, Congress has yet to enact any reform.²³

The Department of Justice issued guidance for the use of race in law enforcement in 2003 that was dramatically under-inclusive.²⁴ Exemptions for national security and border integrity rendered the policy useless given how profiling occurs today.²⁵ Yet, federal legislative remedies have so far failed to find traction.

The place to start is transparency. The centerpiece of the proposed End Racial Profiling Act is the collection and analysis of data concerning the investigatory targets that are impacted by stops, searches, arrests, and uses of force. These provisions are designed to address executive secrecy and achieve long overdue transparency about who, exactly, is affected by law enforcement policies and practices.

Beyond transparency, the erosion of Fourth Amendment principles concerning illegal searches and seizures in the federal jurisprudence creates a compelling opportunity to restore them through local legislation. For instance, simply requiring individualized suspicion (as opposed to allowing associational suspicion) as a predicate for searches or surveillance can dramatically curtail unchecked domestic information collection.²⁶ Local jurisdictions can enact enforceable protections to reiterate this longstanding federal standard,²⁷ as Berkeley, California, did in September 2012.²⁸

Remedies drawn from other areas of the law also hint at potential reforms. In the criminal context, the exclusionary rule inhibits the use of inappropriately gained evidence. But there is no analog in the intelligence context.

There are more than 77 DHS-coordinated fusion centers, 103 FBI-coordinated Joint Terrorism Task Forces, plus the FBI's eGuardian Database and vast secret intelligence systems run by National Security Agency. The duplication and redundancy among these various networks not only is inefficient (to the point of being fraudulent) but also creates a one-way valve: once data is "in," there is no way to remove it. Even intelligence that is collected illegally — or is simply inaccurate — cannot be reliably removed from the information mosaic.

Finally, previous restrictions on intelligence gathering suggest several models. In 1976, investigations by congressional committees led by Senator Frank Church (D-ID) and Representative Otis Pike (D-NY) documented a "sophisticated vigilante operation" by the FBI, CIA, and other intelligence agencies known as COINTELPRO. Guidelines issued by U.S. Attorney General Edward Levi in the wake of the investigations aimed to curtail these illegitimate and unconstitutional activities.²⁹

The original Levi Guidelines included advisory controls, which can ensure that investigations burdening civil rights (such as those involving the use of undercover informants in groups pursuing First Amendment-protected political or religious

activities) are reviewed by headquarters and closed if unsupported by evidence suggesting guilt of a criminal offense. The factual predicate once required to initiate an investigation should be restored, so that law enforcement agents do not chase wild geese. These reforms serve as a model that local legislatures should adopt as legal restrictions to halt mounting abuses and enable both legislative and judicial oversight.

Our nation's counterterrorism efforts have undermined both civil rights and national security, placing the institutional interests of government agencies before communities vulnerable to law enforcement excesses, as well as the country as a whole. But these failures can be fixed by implementing measures to ensure transparency, supervisory controls, and requirements for individual suspicion as a predicate for collecting intelligence. Measures to enable inaccurate, or illegally obtained, data to be purged from intelligence databases are also crucial. Finally, the use of informants and infiltration as methods to ensnare unwitting potential participants in terror plots must be curtailed in order to wean law enforcement agencies from contrived cases and focus them on their unfulfilled mission of pursuing real terrorists.

“[O]UR DOMINANT NOTION OF
 PRIVACY IS TOO LIMITED TO DO THE WORK
 NECESSARY FOR EFFECTIVE REGULATION OF
 DOMESTIC INTELLIGENCE.”

TRANSCRIPT OF REMARKS

Aziz Huq
Assistant Professor of Law
University of Chicago School of Law

As an academic, I have no daily exposure to the practical problems of domestic intelligence and its consequences. The safe inference, therefore, is that I both know nothing and I excel at saying so in too many words.

If academics have a comparative advantage — and they may not — it is in their ability to reflect at more length on the implicit logic of regulatory structure, the ambient reasoning of the law. So my goal here is to suggest to you a new design principle to aid in our thinking about domestic intelligence institutions. It is a design principle that, I think, helps us understand the blind spots of the current architecture and points toward new concerns. The insight is not wholly new. I have drawn inspiration from my University of Chicago Law School colleague Professor Lior Strahilevitz’s work on privacy in tort law,¹ and from a new book by Professor Helen Nissenbaum of New York University.² But there’s some value, I think, to arbitrating the insight over into the security context.

The core intuition is this: our dominant notion of privacy is too limited to do the work necessary for effective regulation of domestic intelligence. That dominant conception is a liberal one, in a classical Millian sense.³ It is discrete and individual. Privacy is imagined, presumed, protected as, say, a zone of immediate, individual autonomy clinging close to us like the atmosphere clings to the earth.

This concept lies at the heart of the Fourth Amendment, which for almost 200 years was literally a protection of the close physical spaces of the person — one’s home, one’s pockets, perhaps one’s car.⁴ In a landmark 1967 case called *Katz*, the Supreme Court extended that right to protect against telephonic surveillance and all other “reasonable expectations of privacy.”⁵ Since expectations are endogenous to the content of the law, however, scholars and judges have struggled since with the

scope of that rule. Federal statutes echo the individual focus. The 1974 Privacy Act, most importantly, places constraints on discrete disclosures by federal agencies about individuals.⁶

The discrete and individual concept of privacy, however, is an insufficient response to the means through which government can predictably look inside an individual life in ways that inhibit decisions to participate in a robust array of political and social life choices.

Consider the government's options if it wished to build up a picture of my daily work life. Every day, I drive to work on a highway, passing through electronic tollbooths at the beginning and end of the road. I sit in an office with shockingly thin walls, where much of what I say can be overheard by the neighboring office dweller. And I do my research on a computer, an Internet server, and an email account created by my employer.

Under current law, the government can, with the nominal process associated with an administrative subpoena, secure the electronic tollbooth records and credit card records associated with my gas purchases to ascertain my travel patterns.⁷ Because I live in a state within the U.S. Court of Appeals for the Seventh Circuit, the government may attach a GPS device to my vehicle and monitor my movement.⁸ Regardless of where I live, the government may secure my neighbor's reports of all he has overheard from my office. The government can also seek out my correspondents in research, and secure information from them by enticement or threat. And because I am not a student covered by the Family Educational Rights and Privacy Act (FERPA),⁹ the government may easily secure from the University of Chicago records of my e-mail traffic that are more than 180 days old and perhaps also emails that are less than 180 days old but that have been opened or otherwise viewed.¹⁰ A search of my desktop or office would entail a warrant, but my employer, and not I, would be in a position to waive the warrant requirement.

There are two lessons here. First, privacy is often not an individual but a relational matter. In social and political life especially, no one is an island. We are "exposed" through friends, work colleagues, and — especially pertinent today — co-congregants. Sociologists since the 1970s have written about how "weak ties" with non-intimate friends provide important networks for social life. Law has not registered this fact; our dependence on wide networks of weak ties is consequently a privacy weakness. We are further exposed by our reliance on commercial third parties, such as credit providers and Internet service providers, which maintain historical records about us. Yet the Fourth Amendment draws a sharp line, protecting my interest in a fact that I hold, but not my interest in a fact I have disclosed to a third-party individual or business entity. Statutes offer only residual protection for the latter. The Fourth Amendment gives no protection to third-party records.¹¹ Nor does it protect us from disclosures of what we have shared with others.¹² Our privacy is in the hands of friends and strangers, vulnerable to whatever inducements, suggestions or threats the government may level against them.

Second, the relational aspect of privacy is magnified by technological and social practices that have expanded dramatically the “data trail” most people leave in their wake. This has created a new set of entities with information about us — our employers, our creditors, our business partners. It also means that there are new ways for the state to build up knowledge about us, ways that the law does not respond to. Specifically, changing technology means that we scatter a breadcrumb trail of data in our wake. Lone, discrete pieces of information that would have been of scant informational value before can be aggregated and analyzed to reveal new kinds of data. Think of how revelatory analysis of your aggregate bank records, credit card statements, or e-mail correspondence would be. It becomes cheaper almost by the day for government to find the processing power necessary to analyze the aggregate data yielded up. Yet constitutional law has barely begun to think about aggregation beyond a few hints in a 1970s opinion called *Whalen v. Roe*.¹³ And statutory law on “minimization” procedures remains too closed to public scrutiny to provide assurance of privacy.¹⁴

Combine the third party record doctrine and the potential of aggregation and you see that legal constraints on government information gathering are often unavailing because of the availability of commercial substitutes. Even if public pressure leads to cessation of efforts like the Defense Advanced Research Projects Agency’s Total Information Awareness,¹⁵ that is, the federal government, within financial constraints, can merely purchase the same data.

Combine the law’s failure to recognize the reasonable expectation of privacy when we disclose something to intimates, and you have to see that that the prevailing protection of associational freedoms, in cases such as *NAACP v. Button*,¹⁶ may equally be nugatory.

The law, in short, has not kept up with technological and social change relevant to the integrity of our private, political and social lives from state intrusion. Rather, the law remains entangled in a limited and limiting conception of privacy as granular and insular. To be sure, that older conception of privacy is not unimportant. It should be supplemented — not replaced, but supplemented — with a *relational* concept of privacy — a concept that takes account of how information is a function of its interpersonal context, and its relationship with other data, specifically with the possibility of aggregated data. Such a relational concept, I think, captures better the manner in which social and technological changes will interact with the evolving domestic security apparatus.

I should close by saying that I offer this idea knowing that the manner of its implementation is far from obvious. Constitutional precedent changes slowly. Statutes also evolve fitfully, and the process of legislative deliberation is surely not the republican ideal envisaged by Madison. It is nevertheless in discussions of this kind that inklings of intellectual change can be nurtured in ways that open possibilities on other fronts.

ENDNOTES

THOMPSON: INTRODUCTORY ADDRESS: “AN INQUIRY INTO EXTREME IDEOLOGY AND VIOLENT ACTION SHOULD BE A BROAD-BASED EXAMINATION...”

1 FAIZA PATEL, BRENNAN CTR. FOR JUSTICE, RETHINKING RADICALIZATION (2011), available at http://brennan.3cdn.net/f737600b433d98d25e_6pm6beukt.pdf.

2 In 2009, James Wenneker von Brunn was accused of shooting a guard at the U.S. Holocaust Museum; he died before trial. Liz Robbins, *J. W. von Brunn, Accused Museum Gunman, Dies at 89*, N.Y. Times, Jan. 7, 2010, at B19.

3 Jared Lee Loughner pleaded guilty in 2012 for shooting 20 people at an Arizona political event in 2009, killing 6 people, including Chief U.S. District Court Judge John Roll, and wounding 14, including U.S. Representative Gabrielle Giffords. Fernanda Santos, *Gunman in Giffords Shooting Sentenced to 7 Life Terms*, N.Y. Times, Nov. 9, 2012, at A16.

4 Nidal Hassan was an Army Major accused of fatally shooting 13 and wounding 29 at Fort Hood in 2009. Robert D. McFadden, *Army Doctor Held in Ft. Hood Rampage*, N.Y. Times, Nov. 6, 2009, at A1.

5 Colleen LaRose was a Pennsylvania resident accused of trying to recruit Islamic terrorists. The charges against her became public in March 2010.

6 Charlie Savage, *Pennsylvania Woman Tied to Plot on Cartoonist*, N.Y. TIMES (Mar. 9, 2010), available at <http://www.nytimes.com/2010/03/10/US/10pennsylvania.html>

PATEL: INTRODUCTION TO INTELLIGENCE COLLECTION BY STATE AND LOCAL LAW ENFORCEMENT

1 *Ten Years After 9/11: Are We Safer?: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 112th Cong. 25 (2011) (testimony of Janet A. Napolitano, Secretary, U.S. Dep’t of Homeland Sec.), available at <http://www.hsgac.senate.gov/hearings/ten-years-after-9/11-are-we-safer>.

2 KSHEMENDRA PAUL, INFO. SHARING ENVIRONMENT, ANNUAL REPORT TO THE CONGRESS: NATIONAL SECURITY THROUGH RESPONSIBLE INFORMATION SHARING 15 (2012), available at http://ise.gov/sites/default/files/ISE_Annual_

Report_to_Congress_2012.pdf.

3 *Id.*

4 *The Department of Homeland Security State and Local Fusion Center Program: Advancing Information Sharing While Safeguarding Civil Liberties: Hearing Before the Subcomm. on Intelligence, Info. Sharing, & Terrorism Risk Assessment of the H. Comm. on Homeland Sec.*, 110th Cong. 6 (2007) (written testimony of David W. Sutherland, Officer for Civil Rights and Civil Liberties, Dept. of Homeland Sec.), *available at* <http://chsdemocrats.house.gov/SiteDocuments/20070314172323-14515.pdf>.

5 *See* Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat 266; 6 U.S.C.A. § 124(h) (West 2011) (establishing the DHS Regional Fusion Center Initiative); 6 U.S.C.A. § 609(a)(7) (West 2011) (“establishing, enhancing, and staffing with appropriately qualified personnel State, local, and regional fusion centers”); 6 U.S.C.A. § 124(i) (West 2011) (establishing a Homeland Security Information Sharing Fellows Program).

6 A fusion center is defined by the federal government as a “collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity.” DEPT OF JUSTICE & DEPT OF HOMELAND SEC., FUSION CENTER GUIDELINES: DEVELOPING AND SHARING INFORMATION AND INTELLIGENCE IN A NEW ERA 2 (2006), *available at* http://it.ojp.gov/documents/fusion_center_guidelines.pdf.

7 INFO. SHARING ENVIRONMENT (ISE), FUNCTIONAL STANDARD (FS), SUSPICIOUS ACTIVITY REPORTING (SAR), VERSION 1.5 2 (2009), [hereinafter ISE SAR FUNCTIONAL STANDARD], *available at* <http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-dhswide-sar-ise-appendix.pdf> (defining SAR as “[o]fficial documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity”).

8 *Id.* at 9.

9 *See* Matt Apuzzo & Adam Goldman, *With CIA Help, NYPD Moves Covertly in Muslim Areas*, ASSOCIATED PRESS (Aug. 23, 2011), *available at* <http://www.ap.org/Content/AP-in-the-News/2011/With-CIA-help-NYPD-moves-covertly-in-Muslim-areas> (detailing an extensive NYPD program of intelligence gathering focusing largely on Muslims). Additional stories on the NYPD’s intelligence program can be found at <http://ap.org/media-center/nypd/investigation>.

10 As Professor Waxman also noted, the threat is likely a mix of the two types of terrorism. Nonetheless, the distinction is important in understanding how the allocation of law enforcement resources should be weighted.

11 *See* BRIAN MICHAEL JENKINS, RAND CORP., STRAY DOGS AND VIRTUAL ARMIES: RADICALIZATION AND RECRUITMENT TO JIHADIST TERRORISM IN THE UNITED STATES SINCE 9/11 (2011), *available at* http://www.rand.org/pubs/occasional_papers/OP343.html; DAVID SCHANZER, CHARLES KURZMAN & EBRAHIM

MOOSA, ANTI-TERROR LESSONS OF MUSLIM-AMERICANS (2010), *available at* http://www.sanford.duke.edu/news/Schanzer_Kurzman_Moosa_Anti-Terror_Lessons.pdf; PETER BERGEN & BRUCE HOFFMAN, BIPARTISAN POLICY CTR., ASSESSING THE TERRORIST THREAT: A REPORT OF THE BIPARTISAN POLICY CENTER'S NATIONAL SECURITY PREPAREDNESS GROUP (2010), *available at* <http://bipartisanpolicy.org/sites/default/files/NSPG%20Final%20Threat%20Assessment.pdf>; PETER NEUMANN, BIPARTISAN POLICY CTR., PREVENTING VIOLENT RADICALIZATION IN AMERICA (2011), *available at* <http://bipartisanpolicy.org/sites/default/files/NSPG.pdf>.

12 See, e.g., Peter King, Op-Ed, *King: What's Radicalizing Muslim Americans?*, NEWSDAY (Dec. 17, 2010), <http://www.newsday.com/opinion/oped/king-what-s-radicalizing-muslim-americans-1.2550488>.

13 Spencer Ackerman, *New Evidence of Anti-Islam Bias Underscores Deep Challenges for FBI's Reform Pledge*, WIRED (Sept. 23, 2011), <http://www.wired.com/dangerroom/2011/09/fbi-islam-domination/>.

14 See e.g., FAIZA PATEL, BRENNAN CTR. FOR JUSTICE, RETHINKING RADICALIZATION 15-16 (2011); MUSLIM AM. CIVIL LIBERTIES COAL., COUNTERTERRORISM POLICY: MACLC'S CRITIQUE OF THE NYPD'S REPORT ON HOMEGROWN RADICALISM (2010), *available at* http://brennan.3cdn.net/d10bbb4a9669213c31_bym6iivs1.pdf.

15 See, e.g., *The Role of Local Law Enforcement in Countering Violent Islamic Extremism: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 110th Cong. 3 (2007) (written testimony of Thomas Dailey, Major, Homeland Sec. Div., Kansas City, Missouri Police Dept'), *available at* <http://www.hsgac.senate.gov/hearings/the-role-of-local-law-enforcement-in-countering-violent-islamist-extremism> (describing how *Radicalization in the West* is used in the Kansas City, Missouri, Police Department "to stay abreast of threats").

16 See THOMAS CINCOTTA, POLITICAL RESEARCH ASSOCS., MANUFACTURING THE MUSLIM MENACE: PRIVATE FIRMS, PUBLIC SERVANTS, AND THE THREAT TO RIGHTS AND SECURITY 50 (2011), *available at* http://www.publiceye.org/liberty/training/Muslim_Menace_Complete.pdf; Michael Powell, *In Police Training, a Dark Film on U.S. Muslims*, N.Y. TIMES, Jan. 24, 2012, at A1; Michael Powell, *In Shift, Police Say Leader Helped With Anti-Muslim Film and Now Regrets It*, N.Y. TIMES, Jan. 25, 2012, at A22.

17 The view that the FBI is spying on Muslim communities, for example, has led Muslim, South Asian, and Arab groups to recommend that Muslims only speak to the police with an attorney present. While this is surely a constitutional right, the presence of an attorney will likely chill communications. PATEL, *supra* note 14, at 25, 52 n.188.

18 See Eileen Sullivan, *NY Muslims Feel Targeted Despite Alliance Promise*, YAHOO! NEWS (Aug. 25, 2011), news.yahoo.com/ny-muslims-feel-targeted-despite-alliance-promise-070319607.html.

19 See, e.g., Julia Preston, *Deportation Program Sows Mistrust, U.S. Is Told*, N.Y.

TIMES, Sept. 16, 2011, at A12 (“But many local police officials told the task force that the program had eroded trust between them and immigrant communities by leaving the impression that they were engaged in enforcing federal immigration laws. Some communities had become reluctant to report crimes.”).

20 See S.F. POLICE DEP’T, GENERAL ORDER 8.10, GUIDELINES FOR FIRST AMENDMENT ACTIVITIES (2008), *available at* <http://www.sf-police.org/modules/ShowDocument.aspx?documentid=24722>; Seattle Mun. Code §§ 14.12.010 et seq. (2011).

21 FED. BUREAU OF INVESTIGATION, JOINT TERRORISM TASK FORCE STANDARD MEMORANDUM OF UNDERSTANDING BETWEEN THE FEDERAL BUREAU OF INVESTIGATION AND THE SAN FRANCISCO POLICE DEPARTMENT 5 (2007), *available at* <http://www.scribd.com/doc/55829249/SFPD-JTTF-MOU-2011>.

22 Although we do not have a copy of the Bureau order, the full text is reprinted in the minutes of the joint meeting of the San Francisco Police Commission and the San Francisco Human Rights Commission held on May 18, 2011. Meeting minutes, Human Rights Commission and the Police Commission (May 18, 2011), *available at* <http://www.sf-police.org/Modules/ShowDocument.aspx?documentid=25397>.

23 *Id.*

24 See Dep’t of Justice, Office of the Inspector Gen., A Review of the FBI’s Investigation of Certain Domestic Advocacy Groups *passim* (2010), *available at* www.justice.gov/oig/special/s1009r.pdf (describing FBI activity relating to domestic advocacy groups); Jim Dwyer, *New York Police Covertly Join in at Protest Rallies*, N.Y. Times, Dec. 22, 2005, at A1 (reporting undercover police officers had surveilled Iraq war protests and other rallies); Frederick A.O. Schwarz, Jr. & Aziz Z. Huq, *Unchecked and Unbalanced: Presidential Power in a Time of Terror* 13-49 (2007) (describing how the FBI’s broad mandate led to targeting of minorities and anti-establishment groups in the mid-twentieth century).

GERMAN: THE EXPANDING STATE AND LOCAL INTELLIGENCE ENTERPRISE AND THE THREAT TO CIVIL LIBERTIES

1 For example, the Church Committee noted in its final report that the breadth of the FBI’s investigations into what it considered subversive activities led to the unfettered collection of a large amount of information on peaceful individuals and groups such as the NAACP. S. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, FINAL REPORT: INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS (BOOK II), S. REP. NO. 94-755 (1976), *available at* <http://www.archive.org/details/finalreportofsel02unit>; S. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, SUPPLEMENTARY DETAILED STAFF REPORTS ON

INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS (BOOK III), S. Rep. No. 94-755 (1976), *available at* <http://archive.org/details/finalreportofsel03unit>.

2 BOOK II, *supra* note 1, at 2-3.

3 See Michael Warner, *Wanted: A Definition of "Intelligence:" Understanding Our Craft*, CENT. INTELLIGENCE AGENCY, *available at* <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article02.html> (last updated June 27, 2008).

4 BOOK III, *supra* note 1, at 27.

5 *United States v. United States Dist. Court (Keith)*, 407 U.S. 297, 313-314 (Sup. Ct. 1972).

6 See FRANK DONNER, *PROTECTORS OF PRIVILEGE: RED SQUADS AND POLICE REPRESSION IN URBAN AMERICA* (1990).

7 28 C.F.R., §23.20(a) (2006).

8 28 C.F.R., §23.20(e) (2006).

9 For a discussion of these reforms, see DONNER, *supra* note 6, at 345-69.

10 See MARILYN PETERSON, *BUR. OF JUSTICE ASSISTANCE, DEP'T OF JUSTICE, INTELLIGENCE-LED POLICING: THE NEW INTELLIGENCE ARCHITECTURE* 5 (2005), *available at* <http://www.ncjrs.gov/pdffiles1/bja/210681.pdf>.

11 COMM. ON THE JUDICIARY, D.C. CITY COUNCIL, *REPORT ON INVESTIGATION OF THE METROPOLITAN POLICE DEPARTMENT'S POLICY AND PRACTICE IN HANDLING DEMONSTRATIONS IN THE DISTRICT OF COLUMBIA* (2004), *available at* <http://www.dcwatch.com/police/040324.htm>.

12 MIAMI CIVILIAN INVESTIGATIVE PANEL, *REPORT ON THE FREE TRADE AREA OF THE AMERICAS SUMMIT* (2006), *available at* <http://www.miamigov.com/cip/downloads/FTAAREport.pdf>.

13 N.Y. CIVIL LIBERTIES UNION, *RIGHTS AND WRONGS AT THE RNC: A SPECIAL REPORT ABOUT POLICE AND PROTEST AT THE REPUBLICAN NATIONAL CONVENTION* (2005), http://www.nyclu.org/files/publications/nyclu_pub_rights_wrongs_rnc.pdf.

14 *St. Paul Police Conduct Mass Preemptive Raids Ahead of Republican Convention*, DEMOCRACY NOW! (Sept. 1, 2008), *available at* http://www.democracynow.org/2008/9/1/st_paul_police_conduct_mass_pre.

15 PETERSON, *supra* note 10, at 9-11.

16 DEMOCRATIC STAFF OF THE H. COMM. ON HOMELAND SEC., *I 10th Cong., LEAP: A LAW ENFORCEMENT ASSISTANCE AND PARTNERSHIP STRATEGY* 5 (2006), <http://hsc-democrats.house.gov/SiteDocuments/20060927193035-23713.pdf>.

17 *Id.* at 5 (quoting Michael Downing, Commander, Los Angeles Police Department Counterterrorism/Criminal Intelligence Bureau).

18 See MIKE GERMAN & JAY STANLEY, AM. CIVIL LIBERTIES UNION, *WHAT'S WRONG WITH FUSION CENTERS* (2007), *available at* http://www.aclu.org/files/pdfs/privacy/fusioncenter_20071212.pdf.

19 TODD MASSE, SIOBHAN O'NEIL & JOHN ROLLINS, CONG. RESEARCH SERV.,

FUSION CENTERS: ISSUES AND OPTIONS FOR CONGRESS 1 (2007), *available at* http://epic.org/privacy/fusion/crs_fusionrpt.pdf.

20 Mike Chalmers & Lee Williams, *Intelligence Facility Casts a Wide Net*, THE NEWS JOURNAL (May 7, 2007), <http://www.delawareonline.com/apps/pbcs.dll/article?AID=/20070507/NEWS/705070333>.

21 MASSE, *supra* note 19, at 22 fn.60.

22 INFO. SHARING ENVIRONMENT (ISE), FUNCTIONAL STANDARD (FS), SUSPICIOUS ACTIVITY REPORTING (SAR), VERSION 1.0, ISE-FS-200 (2008) (on file with authors).

23 MARK A. RANDOL, CONGRESSIONAL RESEARCH SERV., TERRORISM INFORMATION SHARING AND THE NATIONWIDE SUSPICIOUS ACTIVITY REPORT INITIATIVE: BACKGROUND AND ISSUES FOR CONGRESS 4-6 (2009), *available at* http://assets.opencrs.com/rpts/R40901_20091105.pdf.

24 OFFICE OF THE CHIEF OF POLICE, L.A. POLICE DEP'T, SPECIAL ORDER NO. 11, REPORTING INCIDENTS POTENTIALLY RELATED TO FOREIGN OR DOMESTIC TERRORISM (2008) (on file with authors). A copy of the LAPD Special Order can be found here: SUSPICIOUS ACTIVITY REPORT (SAR) SUPPORT AND IMPLEMENTATION PROJECT, FINDINGS AND RECOMMENDATIONS OF THE SUSPICIOUS ACTIVITY REPORT (SAR) SUPPORT AND IMPLEMENTATION PROJECT 36 (2008), *available at* <http://online.wsj.com/public/resources/documents/mccarecommendation-06132008.pdf>.

25 *Id.*

26 See MIKE GERMAN & JAY STANLEY, AM. CIVIL LIBERTIES UNION, FUSION CENTER UPDATE (2008), *available at* http://www.aclu.org/pdfs/privacy/fusion_update_20080729.pdf.

27 CINCOTTA, *supra* note 16, at 14.

28 *Id.* at 32.

29 Meg Stalcup & Joshua Craze, *How We Train Our Cops to Fear Islam*, WASH. MONTHLY (March/April 2011), <http://www.washingtonmonthly.com/features/2011/1103.stalcup-craze.html>.

30 CINCOTTA, *supra* note 16, at 13.

31 Stalcup, *supra* note 29.

32 CINCOTTA, *supra* note 16, at 32.

33 MITCHELL SILBER & ARVIN BHATT, N.Y. POLICE DEP'T, RADICALIZATION IN THE WEST: THE HOMEGROWN THREAT 6 (2007), *available at* <http://publicintelligence.net/nypd-radicalization-in-the-west-the-homegrown-threat/>. This report was revised in 2009. See *infra* p. 32 and note 39. This report seems to draw heavily from an earlier FBI Intelligence Assessment. See COUNTERTERRORISM DIV., FED. BUREAU OF INVESTIGATION, THE RADICALIZATION PROCESS: FROM CONVERSION TO JIHAD (2006), *available at* <http://cryptome.org/fbi-jihad.pdf>. However, the FBI intelligence assessment is not cited.

34 Memorandum from Aziz Huq, Brennan Ctr. for Justice, Concerns with Mitchell D. Silber and Arvin Bhatt, N.Y. Police Dep't, Radicalization in the

West: The Homegrown Threat (Aug. 30, 2007), *available at* http://brennan.3cdn.net/436ea44ae969ab3c5_sbm6vtxgi.pdf. *See also* Memorandum from Am. Civil Liberties Union and Coalition to Members of the S. Comm. on Homeland Sec. and Governmental Affairs (May 7, 2008), *available at* <http://www.aclu.org/safefree/general/35209leg20080507.html>.

35 MUSLIM AM. CIVIL LIBERTIES COAL., COUNTERTERRORISM POLICY: MACLC'S CRITIQUE OF THE NYPD'S REPORT ON HOMEGROWN TERRORISM (2008).

36 *See, e.g., Hearing of the S. Homeland Sec. & Governmental Affairs Comm.: Violent Islamist Extremism: The European Experience*, 110th Cong. (2007) (testimony of Lidewijde Ongerling and Marc Sageman), *available at* <http://www.hsgac.senate.gov/hearings/violent-islamist-extremism-the-european-experience>.

37 Alan Travis, *MI5 Report Challenges Views on Terrorism in Britain*, THE GUARDIAN (Aug. 20, 2008), <http://www.guardian.co.uk/uk/2008/aug/20/uksecurity.terrorism1>; Alan Travis, *The Making of an Extremist*, THE GUARDIAN (Aug. 20, 2008), *available at* <http://www.cjgsu.net/initiatives/MI5-B.pdf>.

38 NAT'L COUNTERTERRORISM CTR., TOWARDS A DOMESTIC COUNTERRADICALIZATION STRATEGY (August 2008).

39 *See* MITCHELL SILBER & ARVIN BHATT, N.Y. POLICE DEP'T, RADICALIZATION IN THE WEST: THE HOMEGROWN THREAT 11-12 (2009), *available at* www.nyc.gov/html/nypd/downloads/pdf/public_information/NYPD_Report_Radicalization_in_the_West.pdf. This report was originally released in 2007 without the statement *see supra* note 33.

40 *Id.* at 12.

41 *See* Letter from Muslim Am. Civil Liberties Coal. to Police Comm'r Raymond Kelly (Sept. 2009), *available at* <http://maclcl1.wordpress.com/2009/09/08/maclcl-90809-letter-response-to-nypd-statement-of-clarification/>.

42 STAFF OF S. COMM. ON HOMELAND SEC. & GOVERNMENTAL AFFAIRS, 110th CONG., VIOLENT ISLAMIST EXTREMISM, THE INTERNET, AND THE HOMEGROWN THREAT (2008).

43 *Spying on First Amendment Activity—State-By-State*, AM. CIVIL LIBERTIES UNION, <http://www.aclu.org/spy-files/spying-first-amendment-activity-state-state> (last visited Oct. 3, 2012).

44 *See Stop Spying*, AM. CIVIL LIBERTIES UNION OF MD., <http://www.aclu-md.org/Index%20content/NoSpying/NoSpying.html> (last visited Apr. 15, 2011). *See also* STEPHEN H. SACHS, REVIEW OF MARYLAND STATE POLICE COVERT SURVEILLANCE OF ANTI-DEATH PENALTY AND ANTI-WAR GROUPS FROM MARCH 2005 TO MAY 2006 (2008), *available at* <http://cdm266901.cdmhost.com/cdm/singleitem/collection/p266901coll7/id/1891/rec/4>.

45 MSP submitted the information to the Washington-Baltimore High Intensity Drug Trafficking Area Task Force (HIDTA) database. HIDTA is a federal program that provides funding and support to participating law enforcement agencies to support regional counter-drug and counter-terrorism efforts. *See* 21

U.S.C. §1706 (2006).

46 Kirsten Atkins, *Statement for the American Civil Liberties Union on Illegal Spying*, AM. CIVIL LIBERTIES UNION (Feb. 22, 2006), <http://www.aclu.org/national-security/statement-kirsten-atkins-target-illegal-spying>.

47 Jessica Guynn & John Simerman, *Sheriff's Deputies Take Steps to Protect Safeway CEO*, CONTRA COSTA TIMES (Jan. 27, 2004).

48 Liliana Segura, *RNC Raids Have Been Targeting Video Activists*, ALTERNET (Aug. 31, 2008), http://www.alternet.org/rights/97110/rnc_raids_have_been_targeting_video_activists_/.

49 Matthew Rothschild, *VA Police Delete Photographs Taken by Muslim-American Journalism Student*, THE PROGRESSIVE (Sept. 17, 2007), available at http://www.progressive.org:80/mag_mc091707.

50 *ACLU of Washington Supports Professor Detained for Taking Photos on Public Property*, AM. CIVIL LIBERTIES UNION OF WASH. (Nov. 15, 2007), <http://www.aclu.org/technology-and-liberty/aclu-washington-supports-professor-detained-taking-photos-public-property>.

51 James Queally, *ACLU Lawsuit Accuses Two Newark Police Officers of Illegally Detaining, Threatening Honors Student*, THE STAR-LEDGER (Newark, N.J.) (Mar. 28, 2011), available at http://www.nj.com/news/index.ssf/2011/03/aclu_lawsuit_against_newark_po.html.

52 JOINT REG'L INTELLIGENCE CTR., INTELLIGENCE ASSESSMENT: GUARDIAN INCIDENT REVIEW: AUGUST 2009 (2009), available at <http://info.publicintelligence.net/LA-RTTACguardianincidents.pdf>.

53 Guy Lawson, *The Fear Factory*, ROLLING STONE, Feb. 7, 2008, at 61, 64, available at <http://guylawson.com/pdf/rollingstone/fearfactory.pdf>.

54 *Praying Passengers Spark Security Concerns at LAX*, CBS L.A. NEWS (Mar. 13, 2011), available at <http://losangeles.cbslocal.com/2011/03/13/2-arrested-after-alaska-airlines-jet-lands-at-lax/>.

55 *Stop and Frisk Campaign: About the Issue*, N.Y. CIVIL LIBERTIES UNION, <http://www.nyclu.org/issues/racial-justice/stop-and-frisk-practices> (last visited April 15, 2011).

56 *Terry v. Ohio*, 392 U.S. 1, 30 (1967).

57 *Stop and Frisk Facts*, N.Y. CIVIL LIBERTIES UNION, <http://www.nyclu.org/node/1598> (last visited April 15, 2011).

58 Al Baker, *Street Stops by the Police Hit a New High*, N.Y. TIMES, Feb. 23, 2011, at A17.

59 Bob Herbert, Op-Ed, *Watching Certain People*, N.Y. TIMES, Mar. 1, 2010, at A23.

60 *Prevention Awareness Bulletin*, NORTH CENT. TEX. FUSION SYSTEM (Feb. 19, 2009), http://www.privacylives.com/wp-content/uploads/2009/03/texasfusion_021909.pdf.

61 VA. FUSION CTR., DEPT OF STATE POLICE, 2009 VIRGINIA TERRORISM THREAT ASSESSMENT 9, 17 (2009), *available at* <http://www.infowars.com/media/vafusioncenterterrorassessment.pdf>.

62 MO. INFO. ANALYSIS CTR., STRATEGIC REPORT: THE MODERN MILITIA MOVEMENT (2009), *available at* <http://www.constitution.org/abus/le/miac-strategic-report.pdf>.

63 Ryan J. Foley, *Homeland Security Collected Information on Wisconsin Abortion, Pro-Life Activists*, CNS NEWS (Feb 8, 2010), <http://cnsnews.com/news/article/homeland-security-collected-information-wisconsin-abortion-pro-life-activists>.

64 Press Release, Am. Civil Liberties Union, Tennessee Law Enforcement Classifies Protected Free Speech as “Suspicious Activity” (Dec. 10, 2010), *available at* <http://www.aclu.org/free-speech/tennessee-law-enforcement-classifies-protected-free-speech-suspicious-activity>.

65 Glen Johnson, *Audit Finds Celebrity Records Improperly Checked*, SEATTLE TIMES (May 6, 2009), http://seattletimes.com/html/nationworld/2009184821_apuscelebritysearches.html.

66 Jay Stanley, *Drilling Opponents Spied On Like Terrorists*, HUFFINGTON POST (Sept. 16, 2010), http://www.huffingtonpost.com/jay-stanley/drilling-opponents-spied_b_719567.html.

67 Rick Rogers, *Records Detail Security Failure in Base File Theft*, SAN DIEGO UNION-TRIBUNE (May 22, 2008), <http://www.signonsandiego.com/news/military/20080522-9999-1n22theft.html>; *see also*, Rick Rogers, *Marine Took Files as Part of Spy Ring*, SAN DIEGO UNION-TRIBUNE (Oct. 6, 2007), <http://www.signonsandiego.com/news/northcounty/20071006-9999-1n6spies.html>; Rick Rogers, *2 Marines Charged in Thefts Ring*, SAN DIEGO UNION-TRIBUNE (July 18, 2008), http://www.signonsandiego.com/uniontrib/20080718/news_1m18theft.html.

68 William A. Forsyth, *State and Local Intelligence Fusion Centers: An Evaluative Approach in Modeling a State Fusion Center* 48 (Sept., 2005) (thesis, Naval Postgraduate School), *available at* http://www.au.af.mil/au/awc/awgate/nps/forsyth_fusion_ctrs.pdf.

69 Rogers, *supra* note 67; *see* JAY STANLEY, AM. CIVIL LIBERTIES UNION, *THE SURVEILLANCE-INDUSTRIAL COMPLEX* 9 (2004), *available at* http://www.aclu.org/FilesPDFs/surveillance_report.pdf.

DANSKY: “THE DEPARTMENT OF HOMELAND SECURITY HAS A RESPONSIBILITY ... TO CONTRIBUTE TO A ROBUST INFORMATION SHARING ENVIRONMENT...”

1 Margo Schlanger returned to her post as a professor at University of Michigan Law School in late 2011.

2 As of February 2012, the number of DHS-recognized fusion centers in operation had gone up to 77. KSHEMENDRA PAUL, INFO. SHARING ENVIRONMENT, ANNUAL REPORT TO THE CONGRESS: NATIONAL SECURITY THROUGH RESPONSIBLE INFORMATION SHARING 4 (2012), *available at* http://ise.gov/sites/default/files/ISE_Annual_Report_to_Congress_2012.pdf; *Fusion Center Locations and Contact Information*, DEP'T OF HOMELAND SEC., http://www.dhs.gov/files/programs/gc_1301685827335.shtm (last visited Sept. 10, 2012).

3 As of April 2011, the privacy policies of 71 fusion centers have been filed and are available to the general public. Mary Ellen Callahan, *Fusion Centers Meet Important Privacy Milestone*, DEP'T OF HOMELAND SEC. (Apr. 29, 2011), <http://blog.dhs.gov/2011/04/fusion-centers-meet-important-privacy.html>; *Privacy Policies*, NAT'L FUSION CTR. ASS'N, <http://www.nfcausa.org/%28X%281%29S%28ddc1fd3yvpkuby55aa054o45%29%29/default.aspx?MenuItemID=121&MenuGroup=Map&&AspxAutoDetectCookieSupport=1> (last visited Sept. 13, 2012).

WAXMAN: AMERICAN POLICING AND THE INTERIOR DIMENSION OF COUNTERTERRORISM STRATEGY

1 AARON L. FRIEDBERG, *IN THE SHADOW OF THE GARRISON STATE* (2000).

2 *Id.* at 3.

3 *See, e.g.*, Jules Lobel, *The War on Terrorism and Civil Liberties*, 63 U. PITT. L. REV. 767 (2002).

4 *See* Harold D. Lasswell, *The Garrison State*, 46 AM. J. SOCIOLOGY 455 (1941); Harold D. Lasswell, *Does the Garrison State Threaten Civil Rights?*, 275 ANN. AM. ACAD. POL. & SOC. SCI. 111 (1951). On the early Cold War popularity of this phrase to capture anxieties of the times, see SAMUEL P. HUNTINGTON, *THE SOLDIER AND THE STATE* 347 (1957). This was also a favorite phrase of President Eisenhower, who famously worried about the policy sway of the American military-industrial complex.

5 FRIEDBERG, *supra* note 1, at 4.

6 Many of these arguments, including concerns about liberty and accountability, are considered in more detail in Matthew C. Waxman, *National Security Federalism in the Age of Terror*, 64 STAN. L. REV. 289 (2012).

7 GREGORY F. TREVORTON, *INTELLIGENCE FOR AN AGE OF TERROR* 1 (2009).

8 *Id.* at 36.

9 *See* NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 401 (2003).

10 *See id.*, at 215-41, 416-23.

11 *See* Jack R. Greene & Sergio Herzog, *The Implications of Terrorism on the*

Formal and Social Organization of Policing in the US and Israel: Some Concerns and Opportunities, in *TO PROTECT AND TO SERVE: POLICING IN AN AGE OF TERRORISM* 143, 150 (David Weisburd et al. eds., 2009).

12 See David H. Bayley & David Weisburd, *Cops and Spooks: The Role of the Police in Counterterrorism*, in *TO PROTECT AND TO SERVE: POLICING IN AN AGE OF TERRORISM* 81, 86 (David Weisburd et al. eds. 2009); Jacqueline E. Ross, *The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany*, 55 *AM. J. COMPARATIVE L.* 493, 496, 503 (2007).

13 See Stephen D. Mastrofski & James J. Willis, *Police Organization Continuity and Change: Into the Twenty-First Century*, 39 *CRIME & JUSTICE* 55, 58 (2010). On the U.S. system of localized policing in comparison with other democracies, see generally DAVID H. BAYLEY, *PATTERNS OF POLICING: A COMPARATIVE ANALYSIS* (1985).

14 A recent National Research Council study estimates that there are about 13,500 local police departments alone across the country. NAT'L RESEARCH COUNCIL, *FAIRNESS AND EFFECTIVENESS IN POLICING: THE EVIDENCE* 49 (Wesley Skogan & Kathleen Frydl eds., 2004).

15 See Matthew C. Waxman, *Police and National Security: American Local Law Enforcement and Counterterrorism After 9/11*, 3 *J. NAT'L SECURITY L. & POL'Y* 377, 385-87 (2009).

16 See JOHN D. BREWER ET AL., *THE POLICE, PUBLIC ORDER AND THE STATE* 115 (2d ed. 1996); NAT'L RESEARCH COUNCIL, *supra* note 14, at 51.

17 See generally PAUL WILKINSON, *TERRORISM VERSUS DEMOCRACY: THE LIBERAL STATE RESPONSE* 80-89 (3d ed. 2011) (describing this tendency).

18 OREN GROSS & FIONNUALA NÍ AOLÁIN, *LAW IN TIMES OF CRISIS: EMERGENCY POWERS IN THEORY AND PRACTICE* 8 (2006).

19 *Id.* at 60.

20 See NAT'L RESEARCH COUNCIL, *supra* note 14, at 52-53.

21 For historical context and comparison with domestic surveillance in the United Kingdom, see Laura K. Donohue, *Anglo-American Privacy and Surveillance*, 96 *J. CRIM. L. & CRIMINOLOGY* 1059 (2006).

22 See Barton Gellman, *Is the FBI Up to the Job 10 Years After 9/11?*, *TIME*, May 9, 2011 (describing retooling of FBI to combat terrorism after 9/11).

23 See *Progress Report on the Reorganization and Refocus of the FBI: Hearing Before the Subcomm. on the Dep't of Commerce, Justice and State, the Judiciary and Related Agencies of the H. Comm. on Appropriations*, 108th Cong. (2003) (testimony of Robert S. Mueller, III, Dir., FBI), available at <http://www.fbi.gov/news/testimony/progress-report-on-the-reorganization-and-refocus-of-the-fbi>.

24 See Charlie Savage, *F.B.I. Casts Wide Net Under Relaxed Rules for Terror Inquiries, Data Show*, *N.Y. TIMES*, Mar. 27, 2011, at A19.

25 See *the Office of Intelligence and Analysis*, DEP'T OF HOMELAND SEC., OFFICE OF INTELLIGENCE AND ANALYSIS, <http://www.dhs.gov/xabout/structure/>

gc_1220886590914.shtm (last visited Oct. 8, 2012).

26 See Pub. L. No. 108–458, 118 Stat. 3638 (2004).

27 See, e.g., RICHARD C. SHELBY, ADDITIONAL VIEWS OF SEPTEMBER 11 AND THE IMPERATIVE OF REFORM IN THE U.S. INTELLIGENCE COMMUNITY 75–76 (2002), available at <http://intelligence.senate.gov/shelby.pdf>; William Odom, *Why the FBI Can't Be Reformed*, WASH. POST, June 29, 2005, at A21; THE RAND CORP., THE FIFTH ANNUAL REPORT TO THE PRESIDENT AND THE CONGRESS OF THE ADVISORY PANEL TO ASSESS DOMESTIC RESPONSE CAPABILITIES FOR TERRORISM INVOLVING WEAPONS OF MASS DESTRUCTION 30 (2003), available at http://www.rand.org/content/dam/rand/www/external/nsrd/terrpanel/volume_v/volume_v.pdf.

28 NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., *supra* note 9, at 423 see also William J. Bratton, *We Don't Need Our Own MI5*, WASH. POST, Oct. 18, 2006, at A21.

29 Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108–458, §1016, 118 Stat. 3638, 3664–3670 (2004) (amended by Pub. L. No. 110–53 §504, 121 Stat. 266, 313–17 (2007)).

30 OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, UNITED STATES INTELLIGENCE COMMUNITY INFORMATION SHARING STRATEGY 18 (2008).

31 See *Printz v. United States*, 521 U.S. 898 (1997) (holding unconstitutional the Brady Handgun Violence Prevention Act's provision requiring that local law enforcement officers conduct background checks).

32 See *id.* at 940 (Stevens, J., dissenting); see also Ann Althouse, *The Vigor of Anti-Commandeering Doctrine in Times of Terror*, 69 BROOK. L. REV. 1231 (2004) (discussing why the doctrine was not challenged after 9/11). Some constitutional experts predicted that 9/11 would mark the “end of the federalism revolution,” as the federal government would necessarily have to assert greater authority over state and local institutions. See Linda Greenhouse, *Will the Court Reassert National Authority?*, N.Y. TIMES, Sept. 30, 2001, at 4.14 (discussing view among constitutional scholars that 9/11 would prompt a reversal of Supreme Court federalism jurisprudence in favor of strong federal powers with respect to states).

33 See *Printz*, 521 U.S. at 936 (O'Connor, J., concurring); see also Lynn A. Baker, *Conditional Federal Spending and States' Rights*, 574 ANN. AM. ACAD. POL. & SOC. SCI. 104 (2001) (arguing that federal conditional spending practices threaten state autonomy).

34 See Waxman, *National Security Federalism in the Age of Terror*, *supra* note 6 (discussing common “top-down” accounts of indirect federal control over state and local governments' anti-terrorism activities).

35 See Waxman, *Police and National Security: American Local Law Enforcement and Counterterrorism After 9/11*, *supra* note 15, at 388–90.

36 See Paul G. Chevigny, *Politics and the Control of Local Surveillance*, 69 CORNELL L. REV. 735 (1984); David E. Kaplan, *Spies Among Us*, U.S. NEWS & WORLD REP. (May 8, 2006), <http://www.usnews.com/usnews/news/>

articles/060508/8homeland.htm.

37 See Mary M. Cheh, *Legislative Oversight of Police: Lessons Learned from an Investigation of Police Handling of Demonstrations in Washington, D.C.*, 32 J. LEGIS. 1, 1 (2005).

38 See K. JACK RILEY ET AL., STATE AND LOCAL INTELLIGENCE IN THE WAR ON TERRORISM 31 (2005); Rick Weiss, *Vast DNA Bank Pits Policing vs. Privacy; Data Stored on 3 Million Americans*, WASH. POST, June 3, 2006, at A1.

39 See JOHN ROLLINS, CONG. RESEARCH SERV., FUSION CENTERS: ISSUES AND OPTIONS FOR CONGRESS 21-23 (2008), available at <http://www.fas.org/sgp/crs/intel/RL34070.pdf>.

40 See Mastrofski & Willis, *supra* note 13, at 124.

41 See Daniel Richman, *The Past, Present, and Future of Violent Crime Federalism*, 34 CRIME & JUSTICE 377, 420-21 (2006); Waxman, *National Security Federalism in the Age of Terror*, *supra* note 109; Ernest A. Young, *Welcome to the Dark Side: Liberals Rediscover Federalism in the Wake of the War on Terror*, 69 BROOK. L. REV. 1285 (2004).

This is a highly contested view, however. Samuel Rascoff cautions against putting too much stock in the role of local police as guardians of liberty in the counterterrorism area. See Samuel J. Rascoff, *The Law of Homegrown (Counter) Terrorism*, 88 TEX. L. REV. 1715, 1722-23 (2010); see also Robert Dreyfuss, *The Cops Are Watching You*, NATION (May 16, 2002), available at <http://www.thenation.com/article/cops-are-watching-you> (reporting that cooptation of local police agencies into counterterrorism intelligence programs undermines freedom).

42 See FRIEDBERG, *supra* note 1, at 340-48.

43 See Bayley & Weisburd, *supra* note 12, at 86; Cynthia Lum et al., *Police Activities to Counter Terrorism: What We Know and What We Need to Know*, in TO PROTECT AND TO SERVE: POLICING IN AN AGE OF TERRORISM 101, 102 (David Weisburd et al. eds., 2009).

44 Cf. Juliette Kayyem, *A Waste of Time*, BOSTON REV. (2004) (“The local and state role is likely to remain most relevant in limited circumstances regarding intelligence: when the federal government has a credible threat against a locale and local authorities are put to work to stop it.”). Some disadvantages of using local police for counterterrorism are catalogued in Bayley & Weisburd, *supra* note 12, at 93-95.

45 See Meg Stalcup & Joshua Craze, *How We Train Our Cops to Fear Islam*, WASH. MONTHLY (March/April 2011), <http://www.washingtonmonthly.com/features/2011/1103.stalcup-craze.html>; Shaun Waterman, *Anti-Terrorism Training Draws Scrutiny*, WASH. TIMES, March 29, 2011, at A4.

46 See Kim Lane Scheppele, *We Are All Post-9/11 Now*, 75 FORDHAM L. REV. 607, 623-28 (2006).

47 See Marc Sageman, *A Strategy for Fighting International Islamist Terrorists*, 618 ANN. AM. ACAD. POL. & SOC. SCI. 223 (2008). For a discussion of the

advantages and drawbacks of relying on local police for anti-terrorism intelligence, see Bayley & Weisburd, *supra* note 12, at 91-95.

48 RILEY ET AL., *supra* note 38, at 1.

49 See JEROME P. BJELOPERA, CONG. RESEARCH SERV., TERRORISM INFORMATION SHARING AND THE NATIONWIDE SUSPICIOUS ACTIVITY REPORT INITIATIVE: BACKGROUND AND ISSUES FOR CONGRESS 15-16 (2011), *available at* <http://fpc.state.gov/documents/organization/166837.pdf>.

50 See Sageman, *supra* note 47; Rascoff, *supra* note 144, at 1728-31.

51 Stephen J. Schulhofer et al., *American Policing at a Crossroads: Unsustainable Policies and the Procedural Justice Alternative*, 101 J. CRIM. L. & CRIMINOLOGY 335, 369 (2011); *see also* Tom R. Tyler et al., *Legitimacy and Deterrence Effects in Counterterrorism Policing: A Study of Muslim Americans*, 44 L. & SOCIETY REV. 365 (2010) (arguing, based on empirical studies, that perceptions of procedural fairness in promotes communities' cooperation with police).

52 See Martin Innes, *Policing Uncertainty: Countering Terror Through Community Intelligence and Democratic Policing*, 605 ANN. AM. ACAD. OF POL. & SOC. SCI. 222, 236 (2006).

53 This term has many different meanings, but generally "community policing" is "a partnership philosophy that increases collaboration (or at least consultation) between the community and the police, decentralizes police organizational hierarchy, gives greater discretion to lower ranks, places greater influence in the hands of the community in determining police priorities, and promotes a social service ethos." JERRY RATCLIFFE, INTELLIGENCE-LED POLICING 3 (2008).

54 See SETH G. JONES & MARTIN C. LIBICKI, HOW TERRORIST GROUPS END: LESSONS FOR COUNTERING AL QA'IDA 27 (2008); RILEY ET AL., *supra* note 38, at ix; Badi Hasisi et al., *The Impacts of Policing Terrorism on Society: Lessons from Israel and the U.S.*, in *TO PROTECT AND TO SERVE: POLICING IN AN AGE OF TERRORISM* 177, 181-87 (David Weisburd et al. eds., 2009).

55 For empirical lessons that support this conclusion drawn from the French experience, see Jacqueline Ross, Thierry Delpuech & Renaud Epstein, *The Joint Production of Intelligence in Local Security Partnerships: French Initiatives*, in *LEGITIMACY AND POLICING* (Tom Tyler & Jeffrey Fagan, eds., forthcoming, 2012).

56 See PETER NEUMANN, BIPARTISAN POLICY CTR., PREVENTING VIOLENT RADICALIZATION IN AMERICA 32-33 (2011).

57 See FAIZA PATEL, BRENNAN CTR. FOR JUSTICE, RETHINKING RADICALIZATION 14-18 (2011) (arguing that local law enforcement agencies adopt reductionist and misguided theories of radicalization). Nevertheless, local efforts at engagement will sometimes be more successful than federal outreach to such communities because of those communities' negative perceptions of the FBI. *See id.* at 31.

58 See NEUMANN, *supra* note 56, at 7-8 & 44; Laurie Goodstein, *Police in Los Angeles Step Up Efforts to Gain Muslims' Trust*, N.Y. TIMES (Mar. 9, 2011), <http://www.nytimes.com/2011/03/10/us/10muslims.html> (reporting that local police

outreach efforts to Muslim-Americans is often more effective than the FBI's).

59 See, e.g., Bayley & Weisburd, *supra* note 12, at 92; Innes, *supra* note 155, at 224.

60 See David Thacher, *The Local Role in Homeland Security*, 39 LAW & SOC'Y REV. 635, 661 (2005).

61 See *id.* at 661-62; Fox Butterfield, *Police Are Split on Questioning of Mideast Men*, N.Y. TIMES, Nov. 22, 2001, at A1; see also Goldstein, *supra* note 58 (reporting that local police outreach efforts to Muslim-Americans is often more effective than the FBI's).

62 See Richman, *supra* note 41, at 419-21.

63 Rascoff, *supra* note 41, at 1734.

64 Detroit, Michigan, is home to a large Arab-American community, so its police forces refused to take part in the federal initiative. See Shannon McCaffrey, *New FBI Sweep Worries Muslims*, DETROIT FREE PRESS, May 27, 2004; Siobhan Gorman, *Detroit Finds Some Answers*, NAT'L J., Mar. 29, 2003, at 998.

65 See PATEL, *supra* note 57, at 24-25; Waxman, *National Security Federalism in the Age of Terror*, *supra* note 6, at 324-39.

66 See Ellen Scrivner, *The Impact of September 11th on Community Policing*, in COMMUNITY POLICING: THE PAST, PRESENT AND FUTURE 183, 187 (Lorie Fridell & Mary Ann Wycoff eds., 2004).

67 See Mastrofski & Willis, *supra* note 13, at 120-25.

68 Richman, *supra* note 41, at 420.

69 See Jonny Dymond, *American Jihad: Facing up to Homegrown Militancy*, BBC NEWS (Apr. 18, 2011), <http://www.bbc.co.uk/news/world-us-canada-13068133>.

70 See NAT'L RESEARCH COUNCIL, PROTECTING INDIVIDUAL PRIVACY IN THE STRUGGLE AGAINST TERRORISTS 16 (2008).

71 According to Brian Michael Jenkins of the RAND Corporation, "As [terrorism] metastasizes, cops are it. We're going to win this at the local level." Quoted in William Finnegan, *The Terrorism Beat: How Is the N.Y.P.D. Defending the City?*, NEW YORKER, July 25, 2005, at 58, 61.

72 NAT'L RESEARCH COUNCIL, *supra* note 14, at 16.

73 See *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).

74 See Michael C. Dorf & Charles F. Sabel, *A Constitution of Democratic Experimentalism*, 98 COLUM. L. REV. 267, 287 (1998).

75 See Schulhofer et al., *supra* note 51, at 66.

76 See Waxman, *National Security Federalism in the Age of Terror*, *supra* note 6, at 345-46; see also Matthew Waxman, *Policing Terrorism*, DEFINING IDEAS, May 4, 2012, available at <http://www.hoover.org/publications/defining-ideas/article/116471>.

77 In October 2012, for example, the Senate Permanent Subcommittee on Investigations published a lengthy investigative report that was highly critical

of fusion centers. STAFF OF S. SUBCOMM. ON INVESTIGATIONS, COMM. ON HOMELAND SEC. & GOVERNMENTAL AFFAIRS, 112th CONG., FEDERAL SUPPORT FOR AND INVOLVEMENT IN STATE AND LOCAL FUSION CENTERS (2012). This echoed some criticisms leveled by The Constitution Project weeks earlier. *See* THE CONSTITUTION PROJECT, RECOMMENDATIONS FOR FUSION CENTERS: PRESERVING PRIVACY AND CIVIL LIBERTIES WHILE PROTECTING AGAINST CRIME AND TERRORISM (2012).

78 *See* BJELOPERA, *supra* note 152, at 11-15; PROGRAM MANAGER, INFORMATION SHARING ENVIRONMENT, PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES ANALYSIS AND RECOMMENDATIONS: NATIONWIDE SUSPICIOUS ACTIVITY REPORTING INITIATIVE 26 (2010), available at www.ise.gov/sites/default/files/NSI_PCRCL_Analysis_July2010.pdf.

79 Matthew C. Waxman, *NYPD's Power of Threat Perception*, COUNCIL ON FOREIGN RELATIONS (Aug. 9, 2012), <http://www.cfr.org/intelligence/nypds-powers-threat-perception/p28802>.

80 An example is federal-local collaborations in Minnesota to deal with Somali-Americans recruited by al-Shabab. *See* Editorial, *Using Outreach to Combat Terrorism*, STAR TRIBUNE (Minneapolis), Aug. 29, 2011, at A12.

81 *See* NEUMANN, *supra* note 56, at 22; *see also* Martin Innes, *Policing Uncertainty: Countering Terror Through Community Intelligence and Democratic Policing*, 605 ANN. AM. ACAD. OF POL. & SOC. SCI. 222 (2006) (describing British anti-terrorism reorientation toward neighborhood policing strategies).

82 *See* THE WHITE HOUSE, EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES 3, 6 (2011), available at http://www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf.

83 *See* Waxman, *National Security Federalism in the Age of Terror*, *supra* note 6, at 349.

84 *Cf.* Eli Lake, *Intelligence Agencies Slammed Over Christmas Plot*, WASH. TIMES (May 19, 2010), available at <http://www.washingtontimes.com/news/2010/may/19/intelligence-agencies-slammed-over-christmas-plot/> (describing political fallout among federal intelligence agencies that failed to connect intelligence dots regarding December 2009 airline terrorist attempt).

SCHWARZ: TRANSCRIPT OF REMARKS

1 Nardone v. United States, 308 U.S. 338 (1939); Weiss v. United States, 308 U.S. 321 (1939).

2 Irvine v. California, 347 US 128 (1954).

GOITEIN: INTRODUCTION TO THE FIRST AMENDMENT AND DOMESTIC INTELLIGENCE GATHERING

1 *See generally* Complaint, *Fazaga v. FBI*, No. 11-00301 (C.D. Cal. 2011).

2 *See* FAIZA PATEL, BRENNAN CTR. FOR JUSTICE, *RETHINKING RADICALIZATION* 21-22 (2011) (citing testimony of FBI Director Robert Mueller and other evidence of FBI mosque infiltration).

3 *See, e.g.*, JOHN HUGHES, *ISLAMIC EXTREMISM AND THE WAR OF IDEAS: LESSONS FROM INDONESIA* 2 (2010).

4 *See* JOSEPH I. LIEBERMAN & SUSAN M. COLLINS, *A TICKING TIME BOMB: COUNTERTERRORISM LESSONS FROM THE U.S. GOVERNMENT'S FAILURE TO PREVENT THE FORT HOOD ATTACK* 48-49, 66-67 (2010).

5 *See* PATEL, *supra* note 2, at 14-18 (citing and discussing NYPD and FBI policies on radicalization).

6 EMILY BERMAN, BRENNAN CTR. FOR JUSTICE, *DOMESTIC INTELLIGENCE: NEW POWERS, NEW RISKS* 17 (2011).

7 *See* PATEL, *supra* note 2, at 18.

8 MARC SAGEMAN, *LEADERLESS JIHAD: TERROR NETWORKS IN THE TWENTY-FIRST CENTURY* 51 (2008).

9 *See* *Laird v. Tatum*, 408 U.S. 1, 13-14 (1972).

10 In addition, some lower courts have held that plaintiffs in civil cases may have standing to challenge investigative activity on First Amendment grounds if they allege a harm beyond a subjective “chill” — for example, if a church alleges that there has been a decline in attendance at worship services. *See* *Presbyterian Church (U.S.A.) v. United States*, 870 F.2d 518, 520-21 (9th Cir. 1989); *see also* *Socialist Workers Party v. Attorney Gen. of the U.S.*, 419 U.S. 1314, 1318-19 (1974) (Marshall, J., as Circuit Judge) (holding that organizers of national convention of the Young Socialist Alliance had standing to challenge investigative activity because they alleged that the activity would dissuade attendance). Standing also may exist if plaintiffs allege that the investigators acted as *agents provocateurs*. *Handschu v. Special Servs. Div.*, 349 F.Supp. 766, 769-70 (S.D.N.Y. 1972).

11 The case law on this question is indeed scant, and that which exists suggests a high bar for challenging investigative activity that takes place in public gatherings of religious or political groups. *See, e.g.*, *Presbyterian Church (U.S.A.) v. United States*, 752 F.Supp. 1505, 1515 (D. Ariz. 1990) (holding that the government’s undercover infiltration of church services is permissible under the First Amendment if the government’s intent is not to disrupt First Amendment activities and if the government does not exceed the scope of the invitation that is extended to the public).

12 *Brandenburg v. Ohio*, 395 U. S. 444 (1969).

13 Chuck Rosenberg, Partner, Hogan Lovells, previously served as U.S. Attorney

for the Eastern District of Virginia, Chief of Staff to Deputy Attorney General Jim Comey (2004-2005), Counselor to Attorney General John Ashcroft (2003-2004), and Counsel to FBI Director Bob Mueller (2002-2003). Mr. Rosenberg spoke at the symposium but did not submit his comments for publication.

14 See LIEBERMAN & COLLINS, *supra* note 4, at 49.

15 Aziz Z. Huq, *The Signaling Function of Religious Speech in Domestic Counterterrorism*, 89 TEX. L. REV. 833, 851 & n.102 (2011) (citing Lawrence Gene Sager, *Fair Measure: The Legal Status of Underenforced Constitutional Norms*, 91 HARV. L. REV. 1212, 1216 (1978)).

MAZNAVI & ZAMAN: FBI SURVEILLANCE AND CUSTOMS AND BORDER PATROL QUESTIONING: IMPACT ON THE FIRST AMENDMENT RIGHTS OF THE AMERICAN MUSLIM COMMUNITY

1 See Michael Isikoff, *FBI: Touchy New Targeting*, NEWSWEEK, Feb. 3, 2003, at 4 (reporting that the FBI ordered field offices to tally the number of mosques in their localities); Eric Lichtblau, *F.B.I. Tells Offices to Count Local Muslims and Mosques*, N.Y. TIMES, Jan. 27, 2003, at A13 (discussing the FBI's demographic measures generally, including mosque surveys); EMILY BERMAN, BRENNAN CTR. FOR JUSTICE, DOMESTIC INTELLIGENCE: NEW POWERS, NEW RISKS 29 (2011) (noting that "FBI Director Robert Mueller ordered all FBI branch offices to count the number of mosques within their jurisdictions as a starting point for proactive investigation of potential terrorists").

2 MICHAEL B. MUKASEY, DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS § II(B)(4)(a)(i) (2008) [hereinafter "MUKASEY GUIDELINES"], available at <http://www.justice.gov/ag/readingroom/guidelines.pdf>.

3 *Id.* at §II.A.1.

4 *Id.* at § II.

5 Allison Jones, *The 2008 FBI Guidelines: Contradiction of Original Purpose*, 19 B.U. PUB. INT. L. J. 137, 168 (2009).

6 *Id.* at 165.

7 Mukasey Guidelines, *supra* note 2, at § II.

8 See BERMAN, *supra* note 1, at 54, n. 123.

9 *Id.* at 25.

10 *Id.*

11 *Id.*

12 *Id.* at 30.

13 FED. BUREAU OF INVESTIGATION, DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE [hereinafter "DIOG"], available at <http://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/fbi-domestic-investigations-and-operations-guide-diog-2011->

version/fbi-domestic-investigations-and-operations-guide-diog-october-15-2011-part-01-of-03/view.

14 Muslim Advocates v. U.S. Dep't of Justice, No. 09-1754 (D.D.C. Sept. 16, 2009).

15 DIOG, *supra* note 13, at § 5.1.

16 *Id.*

17 *Id.* at § 4.2.

18 *Id.* at §§ 3, 5.1.

19 *Id.* at § 5.3; *see also* BERMAN, *supra* note 1, at 27.

20 DIOG, *supra* note 13, at §§ 4.3(C), 4.3.3.2.2.

21 *Id.* at § 4.3(D).

22 *Id.* at 4.3(C).

23 BERMAN, *supra* note 1, at 27.

24 DIOG, *supra* note 13, at § 4.3(C).

25 BERMAN, *supra* note 1, at 28.

26 Spencer S. Hsu, *FBI Director says Justice Dept. is Investigating Possible Exam Violations*, WASH. POST (Jul. 28, 2010), <http://www.washingtonpost.com/wp-dyn/content/article/2010/07/28/AR2010072800619.html>.

27 *FBI in Houston Met the Community Leadership Advising to Lookout for Radicalization*, PAK. CHRONICLE WEEKLY NEWSPAPER, May 18, 2010 (on file with editor).

28 *See* MUSLIM ADVOCATES, UNREASONABLE INTRUSIONS: INVESTIGATING THE POLITICS, FAITH, & FINANCES OF AMERICANS RETURNING HOME 6-7 (2009) [hereinafter "MUSLIM ADVOCATES REPORT"], *available at* http://www.muslimadvocates.org/documents/Unreasonable_Intrusions_2009.pdf.

29 *Id.* at 7-8.

30 *See* Murad Hussain, *Defending the Faithful: Speaking the Language of Group Harm in Free Exercise Challenges to Counterterrorism Profiling*, 117 YALE L. J. 920, 934 (2008).

31 8 U.S.C. § 1225(d)(3).

32 U.S. CUSTOMS AND BORDER PROTECTION, INSPECTOR'S FIELD MANUAL 18.6 (2006), *available at* <http://www.ilw.com/immigrationdaily/News/2008,0513-cbp.pdf>.

33 U.S. v. Flores-Montano, 541 U.S. 149, 152-53 (2004).

34 U.S. v. Arnold, 523 F.3d 941 (9th Cir. 2008) (holding that searches of laptops are *per se* routine for Fourth Amendment purposes, rendering them presumptively permissible under the border search exception to the Fourth Amendment. The court did not consider whether the Fourth Amendment protections apply at the border to medial, financial, personal, and proprietary business information of law-abiding Americans).

35 *Flores-Montano*, 541 U.S. at 152-53.

36 *See* Timothy Zick, *Territoriality and the First Amendment: Free Speech at – and Beyond – Our Borders*, 85 NOTRE DAME L. REV. 1551, 1568 (2009-2010); *see*

also *U.S. v. Ickes*, 393 F.3d 501, 506-08 (4th Cir. 2005) (rejecting the argument based on the First Amendment that a higher level of suspicion is needed for searches of “expressive material,” and refusing to promulgate a reasonable suspicion requirement for border searches where the risk is high that expressive material will be exposed).

37 *U.S. v. Silva*, 715 F.2d 43, 47 (2d Cir. 1982).

38 *Brent v. Ashley*, 247 F.3d 1294, 1299-1300 (11th Cir. 2001).

39 SHIRIN SINNAR ET AL., ASIAN LAW CAUCUS, RETURNING HOME: HOW U.S. GOVERNMENT PRACTICES UNDERMINE CIVIL RIGHTS AT OUR NATION’S DOORSTEP 13 (2009), available at <http://www.asianlawcaucus.org/alc/publications/us-border-report-returning-home/>.

40 *Id.* at 7.

41 *Id.* at 14.

42 *Id.* at 11.

43 MUSLIM ADVOCATES REPORT, *supra* note 28, at 7.

44 *Ngyuen v. INS*, 533 U.S. 53, 67 (2001).

45 MUSLIM ADVOCATES REPORT, *supra* note 28, at 5.

46 SINNAR, *supra* note 39, at 14.

47 *Id.*

48 Letter from the Am. Civil Liberties Union and Muslim Advocates to Richard L. Skinner, Inspector General, Dep’t Homeland Sec. (Dec. 16, 2010), available at http://www.aclu.org/files/assets/DHS_IG_Letter__Appendix.121610.pdf.

49 *Id.*

MARTIN: PROTECTIONS FOR FIRST AMENDMENT-PROTECTED SPEECH AND RELIGION WHEN INVESTIGATING TERRORISM

1 S. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, FINAL REPORT: INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS (BOOK II), S. REP. NO. 94-755 (1976), available at <http://www.archive.org/details/finalreportofsel02unit>; S. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, SUPPLEMENTARY DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS (BOOK III), S. REP. NO. 94-755 (1976), available at <http://archive.org/details/finalreportofsel03unit>.

2 GARY M. STERN, CTR. FOR NAT’L SEC. STUDIES, THE FBI’S MISGUIDED PROBE OF CISPES (1988).

3 DEP’T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FBI’S INVESTIGATIONS OF CERTAIN DOMESTIC ADVOCACY GROUPS (2010), available at <http://www.justice.gov/oig/special/s1009r.pdf>.

4 See *District of Columbia v. Heller*, 554 U.S. 570 (2008).

- 5 *Brandenburg v. Ohio*, 395 U.S. 444 (1969).
- 6 *Holder v. Humanitarian Law Project*, 130 S. Ct. 2705 (2010).
- 7 *See supra* pp. 53-56.
- 8 *See* MUZAFFAR A. CHISTI, MIGRATION POLICY INST., AMERICA'S CHALLENGE: DOMESTIC SECURITY, CIVIL LIBERTIES, AND NATIONAL UNITY AFTER 9/11 (2003).
- 9 *See* EMILY BERMAN, BRENNAN CTR. FOR JUSTICE, DOMESTIC INTELLIGENCE: NEW POWERS, NEW RISKS 13-25 (2011).
- 10 *See id.*
- 11 *See id.*
- 12 *See supra* pp. 41-52.
- 13 BRIAN WALSH & BENJAMIN KEANE. OVERCRIMINALIZATION AND THE CONSTITUTION (2011), *available at* <http://www.heritage.org/research/reports/2011/04/overcriminalization-and-the-constitution>.
- 14 FYODOR DOSTOYEVSKY, CRIME AND PUNISHMENT (1866).

BERMAN: INTRODUCTION TO REGULATION OF DOMESTIC INTELLIGENCE GATHERING AND POTENTIAL FOR REFORM

1 U.S. CONST. amend. IV (“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”).

2 U.S. CONST. amend. I, (“Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.”).

3 U.S. CONST. amend. XIV, § 1 (“All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of Section 1. All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.”).

4 *See supra* pp. 101-03.

5 MICHAEL B. MUKASEY, DEPT OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS Intro. B, *available at* <http://www>.

justice.gov/ag/readingroom/guidelines.pdf.

6 *Id.* at § 4.

7 DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS (2006); DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS (2007); 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 (2010); DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, A REVIEW OF THE FBI'S INVESTIGATIONS OF CERTAIN DOMESTIC ADVOCACY GROUPS (2010).

8 *See, e.g.*, EMILY BERMAN, BRENNAN CTR. FOR JUSTICE, DOMESTIC INTELLIGENCE: NEW POWERS, NEW RISKS (2011).

9 Philip Mudd, Senior Research Fellow, Counterterrorism Strategy Initiative, New America Foundation, former Deputy Director, FBI National Security Branch. Mr. Mudd spoke at the symposium but did not submit his remarks for publication.

10 Suzanne Spaulding, Principal, Bingham Consulting Group, Former Assistant General Counsel, Central Intelligence Agency. Ms. Spaulding spoke at the symposium but did not submit her remarks for publication.

BUTTAR: NATIONAL SECURITY VS. DEMOCRACY IN AMERICA

1 *See, e.g.*, Spencer S. Hsu, *FBI Papers Show Terror Inquiries Into PETA; Other Groups Tracked*, WASH. POST (Dec. 20, 2005), <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/19/AR2005121901777.html>; Andy Grimm & Cynthia Dizikes, *FBI Raids Anti-war Activists' Homes*, CHI. TRIBUNE (Sep. 24, 2010), http://articles.chicagotribune.com/2010-09-24/news/ct-met-fbi-terrorism-investigation-20100924_1_fbi-agents-anti-war-activists-federal-agents.

2 *See* Will Potter, *Daniel McGowan Moved to Another Communications Management Unit*, GREEN IS THE NEW RED (Mar. 4, 2011), <http://www.greenisthenewred.com/blog/daniel-mcgowan-moved-cmu-terre-haute/4419/>.

3 Devlin Barrett, *Five Charged in Plan to Bomb Ohio Bridge*, WALL ST. J. (May 1, 2012), <http://online.wsj.com/article/SB10001424052702304050304577377851612024974.html>; *'Occupy' Anarchists Arrested for 'Plotting to Blow Up Ohio Bridge' After Months of FBI Surveillance*, DAILY MAIL (May 1, 2012), <http://www.dailymail.co.uk/news/article-2137918/Cleveland-Bridge-bomb-plot-Occupy-anarchists-arrested-plotting-blow-Ohio-bridge.html>.

4 *Three NATO Protesters Charged with Terrorism; Protesters Say They Were Only Brewing Beer*, CHICAGOIST (May 19, 2012), http://chicagoist.com/2012/05/19/three_nato_protesters_charged_with.php; *Arrested Protester Charges Mistreatment After Police Raid Apartment*, CBS CHICAGO (May 18, 2012), <http://chicago>.

cbslocal.com/2012/05/18/arrested-protester-charges-mistreatment-after-police-raid-apartment/; Ralph Lopez, *Update III: 3 NATO Activists Charged with Terror Plot after Posting Video of Police Harassment*, DAILY KOS (May 19, 2012), <http://www.dailykos.com/story/2012/05/20/1093156/-3-NATO-Activists-Charged-with-Terror-Plot-After-Posting-Video-of-Police-Harassment>; Candice Bernd, *Chicago: This is What a Police State Looks Like*, ALTERNET (June 2, 2012), http://www.alternet.org/newsandviews/article/937544/chicago%3A_this_is_what_a_police_state_looks_like.

5 Nick Pinto, *Secret Government Informer "Karen Sullivan" Infiltrated Minnesota Activist Groups*, CITYPAGES (Jan. 12, 2011), http://blogs.citypages.com/blotter/2011/01/secret_government_informer_karen_sullivan.php; Peter Wallsten, *Activists Cry Foul over FBI Probe*, WASH. POST (June 13, 2011), http://www.washingtonpost.com/politics/activists-cry-foul-over-fbi-probe/2011/06/09/AGPRskTH_story.html.

6 Holder v. Humanitarian Law Project, 130 S. Ct. 2705 (2010); *FBI Raids: An Attack on First Amendment Rights*, STOPFBI.NET (Oct. 14, 2010), <http://www.stopfbi.net/content/fbi-raids-attack-first-amendment-rights>; Teresa Albano, *Activists Call FBI Raids Massive 'Fishing Expedition'*, PEOPLE'S WORLD (Sept. 26, 2010), <http://www.peoplesworld.org/activists-call-fbi-raids-massive-fishing-expedition/>; Simone Weekly, *Carlos Montes, 'Brown Berets' Latino Activist, Believes SWAT Raid of his L.A. County Home was Front for FBI Investigation*, L.A. WEEKLY (July 7, 2011), http://blogs.laweekly.com/informer/2011/07/carlos_montes_la_fbi_investigation.php.

7 See NAT'L NETWORK FOR IMMIGRANT & REFUGEE RIGHTS, INJUSTICE FOR ALL: THE RISE OF THE U.S. IMMIGRATION POLICING REGIME (2010) [hereinafter "INJUSTICE FOR ALL"], available at http://173.236.53.234/~nnirorg/drupal/sites/default/files/injustice_for_all_-_web_report.pdf (documenting "a brutal system of immigration control and policing that criminalizes immigration status, normalizes the forcible separation of families, destabilizes communities and workplaces, and fuels widespread civil rights violations").

8 Sarah Berlin, *FBI: Preying on Immigrants to Hoodwink the Public*, AM. CONSTITUTION SOC'Y (July 18, 2011), <http://www.acslaw.org/acsblog/fbi-preying-on-immigrants-to-hoodwink-the-public>.

9 See Shankar Vedantam, *No Opt-out for Immigration Enforcement*, WASH. POST (Oct. 1, 2010), <http://www.washingtonpost.com/wp-dyn/content/article/2010/09/30/AR2010093007268.html>; Lee Romney & Paloma Esquivel, *Noncriminals Swept Up in Federal Deportation Program*, L.A. TIMES (April 25, 2010), <http://articles.latimes.com/2011/apr/25/local/la-me-secure-communities-20110425>. See also INJUSTICE FOR ALL, *supra* note 7.

10 Sarah Phelan, *Civil Rights Advocates Say S-Comm Reforms Are Spin, Part of Bigger FBI Biometric Tracking Plan*, S.F. BAY GUARDIAN ONLINE (June 17, 2011), <http://www.sfbg.com/politics/2011/06/17/civil-rights-advocates-say-s-comm>

reforms-are-spin-part-bigger-fbi-biometric-tra; *Next Generation Identification Documents*, Uncover the Truth: ICE and Police Collaborations (July 6, 2011), <http://uncoverthetruth.org/foia-documents/ngi-documents/>.

11 See Mallory Simon & Mariano Castillo, *Texas Plane Crash Pilot: 'I Have Just Had Enough'*, CNN (Feb. 18, 2010), http://articles.cnn.com/2010-02-18/us/texas.plane.crash.profile_1_plane-crashed-pilot?_s=PM:US.

12 See *George Tiller Killed: Abortion Doctor Shot at Church*, THE HUFFINGTON POST (July 1, 2009), http://www.huffingtonpost.com/2009/05/31/george-tiller-killed-abor_n_209504.html.

13 See Jay Sorgi, *7 Dead, Including Shooter, After Massacre at Sikh Temple in Oak Creek*, TMJ4 (Aug. 5, 2012), <http://www.todaystmj4.com/news/local/165061026.html>.

14 See MITCHELL SILBER & ARVIN BHATT, N.Y. POLICE DEP'T, *RADICALIZATION IN THE WEST: THE HOMEGROWN THREAT 6* (2007), available at <http://publicintelligence.net/nypd-radicalization-in-the-west-the-homegrown-threat/>.

15 See Memorandum from Aziz Huq, Brennan Ctr. for Justice, Concerns with Mitchell D. Silber and Arvin Bhatt, N.Y. Police Dep't, *Radicalization in the West: The Homegrown Threat* (Aug. 30, 2007), available at http://brennan.3cdn.net/436ea44aae969ab3c5_sbm6vtxgi.pdf.

16 See FAIZA PATEL, BRENNAN CTR. FOR JUSTICE, *RETHINKING RADICALIZATION* (2011), available at http://brennan.3cdn.net/f737600b433d98d25e_6pm6beukt.pdf.

17 See Press Release, Nat'l Academy of Sciences, *All Counterterrorism Programs That Collect and Mine Data Should Be Evaluated for Effectiveness, Privacy Impacts; Congress Should Consider New Privacy Safeguards* (Oct. 7, 2008), available at <http://www8.nationalacademies.org/onpinews/newsitem.aspx?recordid=10072008a> ("Pattern-Seeking Data-Mining Methods Are of Limited Usefulness").

18 See, e.g., Paul Harris, *Newburgh Four: Poor, Black, and Jailed Under FBI 'Entrapment' Tactics*, THE GUARDIAN (Dec. 12, 2011), <http://www.guardian.co.uk/world/2011/dec/12/newburgh-four-fbi-entrapment-terror>; Graham Rayman, *The Alarming Record of the F.B.I.'s Informant in the Bronx Bomb Plot*, VILLAGE VOICE (Jul. 8, 2009), <http://www.villagevoice.com/2009-07-08/news/the-alarming-record-of-the-f-b-i-s-informant-in-the-bronx-bomb-plot/> (describing a defendant "arrested in a crack house surrounded by bottles of his own urine"); see also Paul Harris, *Fake Terror Plots, Paid Informants: The Tactics of FBI 'Entrapment' Questioned*, THE GUARDIAN (Nov. 16, 2011), <http://www.guardian.co.uk/world/2011/nov/16/fbi-entrapment-fake-terror-plots>.

19 The Department of Justice has met with advocacy groups on several occasions to consider amending its 2003 Guidance on the Use of Race in Law Enforcement. Unfortunately, however, that policy has remained under review for the past two years, no changes have been implemented yet, and there appears

to be no concrete end in sight. Keith Rushing, *Rights Groups Call on Attorney General to Strengthen Racial Profiling Guidance*, RIGHTS WORKING GRP. (May 8, 2012), <http://www.rightsworkinggroup.org/content/rights-groups-call-attorney-general-strengthen-racial-profiling-guidance>.

20 See T.W. Farnam, *Some Congressional Thank-You Notes?*, WASH. POST (Apr. 13, 2011), available at http://www.washingtonpost.com/todays_paper/A%20Section/2011-04-14/A/17/18.0.2396200584_epaper.html (demonstrating that ideas presented by constituents can conceivably find their way to the congressional record, although such examples include “a lot of flattery of campaign donors”).

21 See Paul Blumenthal, *Congress Had No Time to Read the USA PATRIOT Act*, SUNLIGHT FOUND. (Mar. 2, 2009), available at <http://sunlightfoundation.com/blog/2009/03/02/congress-had-no-time-to-read-the-usa-patriot-act/>.

22 Rina Palta, *What You Need to Know About SF's Joint Terrorism Task Force*, KALW NEWS: THE INFORMANT (Apr. 6, 2011), <http://informant.kalwnews.org/2011/04/what-you-need-to-know-about-san-francisco-joint-terrorism-task-force/>; Emily Odgers, *Grassroots Coalition Forces Public Debate on Police Policies in Berkeley, CA*, PEOPLE'S BLOG FOR THE CONSTITUTION (May 25, 2012), <http://www.constitutioncampaign.org/blog/?p=7729#.ULkxJWfsbjM>; Desiree Hellegers, *Portland Versus the FBI*, COUNTERPUNCH (June 24-26, 2005), <http://www.counterpunch.org/2005/06/24/portland-versus-the-fbi/>.

23 See *The End Racial Profiling Act of 2010*, THE LEADERSHIP CONFERENCE, <http://www.civilrights.org/publications/reports/racial-profiling2011/the-end-of-racial.html> (last visited Dec. 3, 2012).

24 DEP'T OF JUSTICE, GUIDANCE REGARDING THE USE OF RACE BY FEDERAL LAW ENFORCEMENT AGENCIES (2003), available at <http://www.scribd.com/doc/22092319/DOJ-Guidance-Regarding-the-Use-of-Race-by-Federal-Law-Enforcement-Agencies-June-2003>.

25 See *Petition to the Dept of Justice*, RIGHTS WORKING GRP., available at <http://www.rightsworkinggroup.org/content/petition-department-justice> (last visited Oct. 4, 2012).

26 See, e.g., DIR. OF NAT'L INTELLIGENCE, INFO. SHARING ENV'T (ISE), FUNCTIONAL STANDARD (FS), SUSPICIOUS ACTIVITY REPORTING (SAR) 7 (2009), available at http://ise.gov/sites/default/files/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf (“[T]he same constitutional standards that apply when conducting ordinary criminal investigations also apply to local law enforcement and homeland security officers conducting [Suspicious Activity Report] inquiries. This means, for example, that constitutional protections and agency policies and procedures that apply to a law enforcement officer’s authority to stop, stop and frisk (“Terry Stop”), request identification, or detain and question an individual would apply in the same measure whether or not the observed behavior related to terrorism or any other criminal activity.”); George Lippman, *Improve Local Policing Programs*, DAILY CAL. (Sep. 18, 2012), available at <http://www.dailycal.org/2012/09/18/improve-local-policing-programs/> (“[T]he city

[of Berkeley, CA] is promising to cease reporting merely ‘suspicious’ though legal activities to the national network of intelligence fusion centers.”).

27 28 C.F.R. 23

28 Nadia Kayyali, *Groundbreaking Strides Toward Civil Liberties in Berkeley*, PEOPLE’S BLOG FOR THE CONSTITUTION (Sept. 21, 2012), <http://www.constitutioncampaign.org/blog/?p=9892#.UHx7-a7AHjM>.

29 EDWARD H. LEVI, DEP’T OF JUSTICE, DOMESTIC SECURITY INVESTIGATION GUIDELINES § I.A (1976).

HUQ: “[O]UR DOMINANT NOTION OF PRIVACY IS TOO LIMITED TO DO THE WORK NECESSARY FOR EFFECTIVE REGULATION OF DOMESTIC INTELLIGENCE.”

1 Lior J. Strahilevitz, *Reunifying Privacy Law*, 98 CAL. L. REV. 2007 (2010).

2 HELEN NISSENBAUM, *PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE* (2010).

3 JOHN STUART MILL, *ON LIBERTY* (1859).

4 U.S. CONST. amend. IV (“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”).

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

6 5 U.S.C. § 552(b) (2006).

7 31 U.S.C. §§ 5311- 5312 (2006).

8 *United States v. Garcia*, 474 F.3d 994 (7th Cir. 2007). Editor’s note: Since Professor Aziz’s remarks at the convening in 2011, the United States Supreme Court has ruled that attaching a GPS tracker to a vehicle without a warrant violates the Fourth Amendment. *See U.S. v. Jones*, 565 U.S. --, 132 S. Ct. 945 (2012).

9 20 U.S.C. § 1232g (2006).

10 18 U.S.C. § 2703; *see also* Orin S. Kerr, *A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1216 (2004) (noting uncertainty over the proper legal treatment of opened e-mail).

11 *Smith v. Maryland*, 442 U.S. 735 (1979) (phone numbers); *United States v. Miller*, 425 U.S. 435 (1976) (bank records).

12 *United States v. White*, 401 U.S. 745 (1971).

13 *Whalen v. Roe*, 429 U.S. 589 (1977).

14 50 U.S.C. § 1801(h) (2006).

15 *DARPA’s S&T Privacy Principles*, DEF. ADVANCED RESEARCH PROJECTS AGENCY, http://www.darpa.mil/About/Initiative/DARPA%E2%80%99s_S_T_Privacy_Principles.aspx (last updated Oct. 5, 2011).

16 *NAACP v. Button*, 371 U.S. 415 (1963).

ABOUT THE CONTRIBUTORS

The Honorable Leroy D. Baca is the elected Sheriff of Los Angeles County, winning his fourth term in 2010. He commands the nation's largest sheriff's department; it has a staff of 18,000 and a \$2.5 billion annual budget. Sheriff Baca pioneered "public trust policing," an initiative that permits a diverse array of community leaders to advise the department. Baca's department also operates 14 non-profit youth centers and 10 regional training centers for at-risk youth.

Emily Berman is a visiting Assistant Professor at Brooklyn Law School. Before her faculty appointment, Berman was Counsel in the Liberty and National Security Program at the Brennan Center for Justice. Her most recent report, *Domestic Intelligence: New Powers, New Risks*, examines the FBI's guidelines for domestic intelligence investigations. Berman was a clerk for Judge John Walker of the U.S. Court of Appeals for the Second Circuit and was editor-in-chief of the *New York University Law Review*.

The Honorable John O. Brennan is the Director of the Central Intelligence Agency. He previously served as Assistant to the President for Homeland Security and Counterterrorism from January 2009 until January 2013. He also served as Homeland Security Advisor and Deputy National Security Advisor for Counterterrorism. Brennan was President and CEO of The Analysis Corp. in McLean, Va., from 2005 to 2009. Before entering the private sector, he spent 25 years at the CIA. Brennan was Chief of Staff to CIA Director George Tenet and was Deputy Executive Director from 2001 to 2003. Brennan is the founding Director of the Terrorist Threat Integration Center, the predecessor to the National Counterterrorism Center. He graduated from Fordham University and received an M.A. in Government with a concentration in Middle Eastern Studies from the University of Texas at Austin.

Shahid Buttar is the Executive Director of the Bill of Rights Defense Committee. He also leads the People's Campaign for the Constitution in its efforts to defend civil liberties, constitutional rights, and rule of law principles threatened by the war on terror. Buttar previously directed the Muslim Advocates' program to combat racial and religious profiling by federal authorities, and was an associate director of the American Constitution Society. Buttar graduated from Stanford Law School.

Kara Dansky is Senior Counsel for the Center for Justice at the American Civil Liberties Union. She previously served as Section Lead of the Impact Assessment Section at the Department of Homeland Security's Office for Civil Rights and Civil Liberties from August 2010 until August 2012. As Section Lead, Dansky evaluated Department programs, policies, and procedures to ensure they complied with Constitutional, statutory, regulatory, and other legal requirements. Dansky also was the founding Executive Director of the Stanford Criminal Justice Center, a research and policy institute at Stanford Law School. Dansky has also worked as a public defender in Seattle. She was a staff clerk for the U.S. Court of Appeals for the Third Circuit and clerked for U.S. District Court Judge Martha Vazquez. Dansky graduated from The John Hopkins University and the University of Pennsylvania Law School.

Michael German is a Policy Counsel for the American Civil Liberties Union's Washington, D.C., legislative office. He develops policy positions and strategies on pending legislation and executive branch actions concerning national security and open government. German concentrates on issues such as domestic surveillance, data mining, privacy, whistleblower protection, and intelligence and law enforcement oversight. Before joining the ACLU in 2006, German spent 16 years as a Special Agent for the Federal Bureau of Investigation. He specialized in domestic terrorism and covert operations. German has also served as an adjunct professor at the National Defense University, and is a Senior Fellow with GlobalSecurity.org. His first book, *Thinking Like a Terrorist*, was published in 2007. He is a graduate of Wake Forest University and Northwestern University School of Law.

Elizabeth Goitein is Co-Director of the Liberty and National Security Program at the Brennan Center. Before joining the Brennan Center, she was counsel to former U.S. Sen. Russ Feingold, where she handled national security matters, including government secrecy and privacy rights. She was a trial attorney at the Department of Justice for several years and clerked for Judge Michael Daly Hawkins of the U.S. Court of Appeals for the Ninth Circuit.

Aziz Huq is an assistant professor at the University of Chicago Law School. He is a former director of the Liberty and National Security Program at the Brennan Center. Aziz graduated from Columbia Law School where he was awarded the John Ordranax Prize for general proficiency in legal study. He clerked for Judge Robert Sack of the U.S. Court of Appeals for the Second Circuit and for Supreme Court Justice Ruth Bader Ginsburg. Huq has served as a Senior Consultant Analyst for the International Crisis Group in Afghanistan, Nepal, Sri Lanka, and Pakistan. In 2007, he was awarded a Carnegie Scholars Fellowship. Huq is one of three principal investigators in an ongoing National Science Foundation-sponsored study on counterterrorism policing.

Kate Martin is the Director of the Center for National Security Studies, a think tank and advocacy organization working to protect civil liberties and human rights. Martin and the Center won the 2005 Eugene S. Pulliam First Amendment Award by the Society for Professional Journalists. Martin has served as a lecturer on national security and intelligence issues at George Washington University Law School and at Georgetown University Law Center. She was general counsel to the National Security Archive from 1995 to 2001. She frequently testifies before Congress on national security and civil liberties issues.

Nura Maznavi is a Chicago civil rights lawyer. From 2009 to 2011, Maznavi worked as a lawyer for Muslim Advocates, leading the organization's Program to End Racial and Religious Profiling. A former Fulbright Scholar, Maznavi was a staff lawyer for the U.S. Court of Appeals for the Ninth Circuit. She is a graduate of Pomona College and George Washington University Law School.

Faiza Patel is Co-Director of the Liberty and National Security Program at the Brennan Center and author of the recent report, *A Proposal for an NYPD Inspector General*. Previously, she was a senior policy officer at the Organization for the Prohibition of Chemical Weapons at The Hague and clerked for Judge Rustam Sidhwa at the International Criminal Tribunal for the Former Yugoslavia. Patel is also a member of the U.N. Working Group on the Use of Mercenaries.

Frederick A.O. Schwarz, Jr. is Chief Counsel of the Brennan Center, which he joined full time in 2002. On behalf of the Center, Mr. Schwarz has tried three cases, and frequently testifies before Congress. He plays a critical role in all of the Center's work. While at the Brennan Center, Schwarz was awarded the New York State Bar Association's Gold Medal for distinguished service. Schwarz graduated *magna cum laude* from Harvard and *magna cum laude* from its law school, where he was an editor of the Law Review. After clerking for Chief Judge J. Edward Lumbard of the U.S. Court of Appeals for the Second Circuit, he spent a year as Assistant Commissioner for Law for the government of Northern Nigeria on a Ford Foundation grant. From 1975 to 1976, Schwarz was Chief Counsel to the Church Committee (formally known as the Senate Select Committee to Study Governmental Activities with Respect to Intelligence Activities). He was New York City Corporation Counsel under Mayor Edward Koch from 1982 to 1986. In 1989, Schwarz chaired New York City's Charter Revision Commission. He also chaired of the New York City Campaign Finance Board from 2003 to 2008. Schwarz is the author of two books. The most recent, written at the Brennan Center (with Aziz Huq), is *Unchecked and Unbalanced: Presidential Power in a Time of Terror* (The New Press, 2007; paperback 2008). His earlier work was *Nigeria: The Tribes, The Nation, or the Race — The Politics of Independence* (The MIT Press, 1965).

Geoffrey R. Stone is the Edward H. Levi Distinguished Service Professor at the University of Chicago Law School. Prof. Stone served as Dean of the school for seven years starting in 1987. He is a graduate of the school, where he was editor-in-chief of the law review. Prof. Stone clerked for Supreme Court Justice William Brennan Jr. He is the author or co-author of many books on constitutional law, including *Speaking Out: Reflections on Law, Liberty and Justice* (2010), and *Perilous Times: Free Speech in Wartime* (2004), which won the American Political Science Association's annual Kammerer Award for best Political Science book. Prof. Stone is a fellow of the American Academy of Arts and Sciences and a board member of the American Constitution Society.

The Honorable Bennie G. Thompson was recently elected to his tenth term as a Democratic Congressman from Mississippi's Second District. His congressional district, which covers most of western Mississippi, is a blend of rural and metropolitan communities. With 44 years of continuous public service, he is the longest serving African American elected official in the state. Thompson is the ranking member and former chairman of the House Committee on Homeland Security. During his tenure as chairman, the Committee bolstered the resources and operational capacity within the Department of Homeland Security by authorizing TSA, the Coast Guard, and other critical components.

Matthew C. Waxman is a professor at Columbia Law School, specializing in international and national security law. He is also an adjunct senior fellow at the Council on Foreign Relations and a member of the Hoover Institution's Task Force on National Security and Law. From 2005 to 2007, Prof. Waxman was Principal Deputy Director of Policy Planning at the State Department and also worked for Condoleezza Rice when she was National Security Adviser. He worked in the Defense Department as Deputy Assistant Secretary for Detainee Affairs. Prof. Waxman graduated from Yale and its law school. He was a Fulbright Scholar and clerked for Judge Joel Flaum of the U.S. Court of Appeals for the Seventh Circuit and for former Supreme Court Justice David Souter.

Since September 11, 2001, advancements in technology and shifts in counterterrorism strategies have transformed America's national security infrastructure. These shifts have eroded the boundaries between law enforcement and intelligence gathering and resulted in surveillance and intelligence collection programs that are more invasive than ever.

Domestic Intelligence: Our Rights and Our Safety captures the voices of leading government officials, academics, and advocates on the burgeoning role of law enforcement in the collection of domestic intelligence. Brought together by a Brennan Center for Justice symposium, this diverse range of perspectives challenges us to reevaluate how we can secure the safety of the nation while remaining faithful to the liberties we seek to protect.

BRENNAN
CENTER
FOR JUSTICE

at New York University School of Law

161 Avenue of the Americas
12th Floor
New York, NY 10013
(646) 292-8310
www.brennancenter.org