Platform for PREJUDICE

How the Nationwide Suspicious Activity Reporting Initiative Invites Racial Profiling, Erodes Civil Liberties, and Undermines Security

A publication of Political Research Associates

by Thomas Cincotta

Platform for Prejudice

How the Nationwide Suspicious Activity Reporting Initiative Invites Racial Profiling, Erodes Civil Liberties, and Undermines Security

By Thomas R. Cincotta

March 2010
Political Research Associates

Political Research Associates (PRA) is a progressive think tank devoted to supporting movements that build a more just and inclusive democratic society. We expose movements, institutions, and ideologies that undermine human rights. PRA seeks to advance progressive thinking and action by providing research-based information, analysis, and referrals.

ISBN #978-0-915987-23-8

Cover Design by Hird Graphic Design
Photographs by iStockphoto and Thomas Cincotta

This report and additional resource material is online at:
www.publiceye.org/jump/sar.html

Political Research Associates
1310 Broadway, Suite 201
Somerville, MA 02144-1837
www.publiceye.org

Platform for Prejudice

How the Nationwide Suspicious Activity Reporting Initiative Invites Racial Profiling, Erodes Civil Liberties, and Undermines Security

Advance Praise for Platform for Prejudice

"If the past decades have taught us anything about police intelligence, it is that an emphasis on information gathering, rather than better analysis techniques, opens the door to constitutional abuses without any measurable security benefit. *Platform for Prejudice* wisely applies that crucial insight, providing a clear-eyed assessment of how and why the Suspicious Activities Reporting Initiative poses significant risks while failing to make us safer."

–David Cunningham, Sociology professor at Brandeis University and author of *There's Something Happening Here: The New Left, The Klan, and FBI Counterintelligence*

. . .

"Thomas Cincotta and Political Research Associates have put together a report that both documents the history of the SAR program and plows new ground, uncovering abuses that demand the attention of policymakers. PRA shines a light on an expanding domestic surveillance apparatus that threatens the liberty of all Americans."

–Mike German, former FBI agent, currently Policy Counsel on National Security, Immigration and Privacy for the ACLU in Washington, D.C.

. . .

"PRA's report on the government's SAR program is a deeply researched, thorough piece – must reading for anyone who cares about the balance between civil liberties and security. This is one issue that will re-shape the American experience as we know it and yet most of us are uninformed. This report can help you begin to learn about the issue."

–M. Bilal Kaleem, Executive Director of Muslim American Society of Boston, the largest Muslim organization in New England

. . .

"In a world where immigrants are already suspect, Cincotta's report unmasks a new government initiative with the sole function of further criminalizing immigrants and communities of color. This stirring report illuminates a system that formalizes collaborations between law enforcement bodies at every level, thus immersing us all in the shadowy depths of a police state. As the Obama administration prepares to implement the initiative nationally, Cincotta offers sharp critique and deep fact-finding to expose this program for what is — a mechanism that inevitably fosters wide-spread racial profiling and perilously ineffective public safety policies."

–Manisha Vaze, Organizer at Families for Freedom (FFF), a New York-based multiethnic defense network by and for immigrants facing and fighting deportation

Foreword

Emergencies are engines of institutional invention in ways that escape the ambit of democracy. Consider the governmental response to the terrorist attacks of September 11, 2001. Many counter-terrorism programs, to be sure, eerily echoed civil rights and civil liberties abuses of the past. The National Security Agency's Terrorist Surveillance Project, for example, reminded many of broad surveillance programs aimed at political dissidents, civil rights groups, and many other Americans during the Cold War era. But other programs seemed ominous innovations. The "extraordinary rendition" and "black sites" policies, for example, turned existing U.S. relationships with foreign governments to unexpected and ominous ends. Out of the heat and panic of 9/11 came a set of new intergovernmental relations that substantially violate international human rights standards. What was innovative in these programs was less the violations that they enabled and more the novel institutional forms they took.

Platform for Prejudice is a judicious and cogent accounting of another set of institutional innovations catalyzed by the 9/11 attacks that may have substantial consequences for constitutional civil liberties. Somewhat paradoxically, while post-9/11 transformations of international relationships have received much media and academic attention, the more subtle changes wrought to our Constitution's fundamental federal-state structure in the name of national security have gone largely unremarked. Political Research Associates' work on and analysis of novel collaborations between federal, state, and local governments thus fills an important gap.

One way of situating the subject of this report is in relation to ongoing debates about federal-state interaction about immigration policy. Under Section 287(g) of the Immigration and Naturalization Act, the Department of Homeland Security has entered into increasing number of agreements with local law enforcement empowering the latter to enforce the federal immigration laws pursuant to memorandums of understanding. The result has been, among other things, a sharp uptick of concern with discriminatory policing.

The parallel development to §287(g)s in national security policy is the focus of this report. It outlines the development in the wake of the 2004 Intelligence Reform and Terrorism Prevention Act of both a set of federal-state intelligence sharing protocols and also a new set of federal-state institutions. In the cause of facilitating information sharing, the 2004 Act set in motion the development of a complex, sprawling, and largely unregulated weaving together of local and state police forces on the one hand with federal law enforcement and intelligence agencies on the other. To my knowledge, *Platform for Prejudice* is the first comprehensive descriptive accounting of these new systems and the threats they pose. The report contains a meticulous description of this new form of federal-state cooperation, as well as a helpful case study of a particular collaboration in Los Angeles.

As the report demonstrates, these post 9/11 innovations raise concerns central to the values promoted by our federal Constitution. While *Platform for Prejudice* pays particular attention to downstream effects on individual constitutional rights, the new policies and institutions described here should raise flags for those concerned with what the Supreme Court has called "Our Federalism": the splitting of sovereignty between national and state governments as a way to create natural rivals for power who would check each other's encroachments on the people's rights. Federalism has been a slogan for many different values in its day. But the fact remains that it was a structural protection originally embedded in the Constitution as a means to secure liberty by diffusing government power.

The collaborations detailed in this report fuse the atom of sovereignty in ways that would have been especially troubling to a Founding generation concerned with a distant leviathan exercising unaccountable powers. *Platform for Prejudice*, in short, is no mere appeal to the civil liberties choir. The questions it raises should be of concern to all Americans who value some fidelity to founding constitutional values.

Aziz Z. Huq
Assistant Professor,
University of Chicago Law School
March 15, 2010

Acknowledgements

The idea of mapping the domestic security infrastructure from a civil liberties perspective was first proposed by Abby Scher and Tarso Luís Ramos, to whom I am indebted for bringing me on to oversee the investigation and study a matter of critical importance for human rights, as well as the integrity of the democratic and egalitarian ideals upon which this country was founded. Thank you for your guidance, trust, and leadership. I am grateful to Chip Berlet for sharing his historical insights, sharp wit, and production know-how. Many thanks are due the staff and interns at PRA for bringing this report to fruition: Maria Planansky, James Huettig, Pam Chamberlain, and Kapya Kaoma read, commented upon, edited, and criticized multiple drafts of the report and provided both political insight and moral support. Shakeel Syed, the energetic and devoted executive director of the Islamic Shura Council (Southern California), and Nancy Murray, the education and outreach director for the ACLU of Massachusetts, gave invaluable feedback. Thanks also to Debbie Hird, our patient and capable graphic designer, and Becca Wilson for editing.

Investigation for this report was carried out by experienced field journalists who painstakingly pursued documents and interviews with key figures in local agencies. I thank Mary Fischer who wrote and compiled material for our Los Angeles case study on the Joint Regional Intelligence Center; Lisa Ruth, who interviewed officials with Florida's state fusion center and the Broward County Sheriff's Office; Andrea Simakis, who interviewed officials with the Boston Regional Intelligence Center and Massachusetts Bay Transportation Authority intelligence unit.

We are extremely appreciative of advisors and organizational allies who contributed insights and support for the project. We stand in solidarity with you. Carol Rose, John Reinstein, and Laura Rotolo of the American Civil Liberties Union of Massachusetts gave us time, extensive input, and access to critical documents from the state fusion center. Those documents are now publicly available at www.stopspying.us/wiki, a new central repository for documents related to domestic surveillance to which multiple organizations have begun to contribute. We are inspired by the ACLU's effort to establish public accountability for fusion centers with

proposed legislation pending in the Massachusetts state legislature, Senate Bill 931 and hope this will be the first of many other such initiatives.

Many thanks to the front-line organizations who struggle to ensure the safety and dignity of their communities and warmly supported this project with their insights, background information, and leads: Bilal Kaleem and Hossam Al-Jabri of the Muslim American Society for Freedom (Boston Chapter); Affad Sheikh and Ameena Qazi of the Council on American-Islamic Relations (Southern California); Hamid Khan and Tamia Pervez of the South Asian Network; Manisha Vaze of Families for Freedom; and Steve Rohde of the Interfaith Committee for Justice and Peace in California. Guidance was also provided by many devoted civil liberties advocates and authors: Eileen Clancy of iWitness Video; Heidi Boghosian, Jim Lafferty, and Urzsula Mazny-Latos of the National Lawyers Guild; Sue Udry of the Defending Dissent Foundation; Chip Pitts and Shahid Buttar of the Bill of Rights Defense Committee; Brigitt Keller of the National Police Accountability Project; sociology professor and COINTELPRO expert David Cunningham; and Mike German, policy counsel for the ACLU. I thank Ross Gelbspan for sharing his experiences researching intelligence agency abuses. I am grateful to all of the members of our national advisory committee and others who have helped along the way.

Finally, I am deeply grateful to my wife, Kari, for picking me up after long hours of research and writing, my mother Janet for emotional support, and my sister Deborah for hosting me on trips to California.

It is easy to feel disempowered when reckoning with the growth of mass surveillance in our country. I sincerely believe that our freedom is too precious to sacrifice on the basis of unfulfilled claims about safety and security. As security cameras, undercover informants, and digital data warehouses proliferate, it is important that Americans assert democratic control over intelligence institutions that have a proven record of going too far. The Suspicious Activities Reporting Initiative is a good place to start restoring oversight and respect for Constitutional principles.

Thomas Cincotta
Director, Civil Liberties Project
Political Research Associates
Somerville, MA
March 17, 2010

Table of Contents

Platform for Prejudice

How the Nationwide Suspicious Activity Reporting Initiative Invites Racial Profiling, Erodes Civil Liberties, and Undermines Security

Platform for Prejudice

How the Nationwide Suspicious Activity Reporting Initiative Invites Racial Profiling, Erodes Civil Liberties, and Undermines Security

By Thomas R. Cincotta

March 2010
Political Research Associates

Introduction

They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety.

-Benjamin Franklin – 1775

The intelligence lapses that failed to prevent the September 11 terrorist attacks prompted an overhaul of U.S. domestic and foreign intelligence systems, including the creation of an expansive new domestic security infrastructure. A key part of this new infrastructure is the Suspicious Activity Reporting Initiative, a framework that guides, orchestrates, and connects the federal government's nationwide "Information Sharing Environment." In this initiative, we see the seeds for a possible repeat of past intelligence abuses, particularly with the weakening of civil liberties safeguards and mobilization of police as intelligence officers.

The Suspicious Activity Reporting Initiative (SAR Initiative) is a useful focus for understanding how the new domestic security infrastructure works because it feeds and links together components of the system, reaching into the populace and forming an intelligence pipeline between the "fusion centers" charged with managing the program and various other agencies. We have found that these new fusion centers – ostensibly designed to counter terrorism – seem to devote most resources and attention to solving common crimes rather than protecting national security. If it is the case that Fusion Centers perform a primarily policing function, rather than counter-terrorism, the public should weigh whether their excessive secrecy and surveillance powers are justified on that basis.

In an attempt to peer inside these secretive agencies and contribute to public knowledge about the extensive domestic security infrastructure, Political Research Associates launched an investigation into how the SAR Initiative works. Our questions included SAR's role in the larger domestic security apparatus, the rules under which it functions, and how its practices affect those individuals and communities most singled out for suspicion of terrorism. This report includes data from our investigations in Boston, Los Angeles, and Miami, as well as a comprehensive analysis of federal and local policies and reports. Based on our Los Angeles investigation, the report contains a thorough case study of the Los Angeles Joint Regional Intelligence Center.

The report is broken up into four sections, which contextualize and explain the SAR Initiative, as well as elucidate the potential hazards of the program:

In Section 1 of this report, we **describe the shape and identify key components of the domestic security infrastructure**. Although many levels of government are involved in Suspicious Activity Reporting (such as the National Security Agency, Coast Guard, Department of Defense, Department of Energy, and private sector advisory councils), this report focuses on fusion centers and state and local police departments.

In Section 2, we explain the origins of the national Suspicious Activities Reporting (SAR) Initiative and analyze faulty assumptions upon which it is based. We call attention to an aggressive new form of policing called "Intelligence-Led Policing" whose pre-emptive approach violates core American values.

In Section 3, we **explore how the SAR Initiative becomes a platform for several types of prejudice**. We document the pattern of racial, ethnic, and religious profiling evident in this approach to intelligence gathering. We also explore political biases that manifest themselves in Suspicious Activities Reporting criteria and intelligence analysis. Further, we examine how the SAR Initiative lowers the threshold for government data collection in ways that fuel both profiling and political policing, and violate long-standing civil liberties protections.

Lastly, in Section 4, we use a case study of the fusion center based in Norwalk, California, the Joint Regional Intelligence Center, to **identify how domestic intelligence collection and sharing jeopardizes civil liberties**. Los Angeles' Fusion Center spearheaded the national SAR Initiative, uses extremely broad criteria for so-called "suspicious" activity, and vigorously encourages the public to report suspicious activities through its controversial iWatch program.

However, as with any investigation of intelligence agencies, the excessive secrecy of the system posed many challenges. Several agencies and departments failed to make their policies available online and to respond to our formal requests for interviews or documents.

I and my colleagues at Political Research Associates believe the United States faces two real and serious threats from terrorists: the first from terrorist acts themselves, which have the demonstrated capacity to cause mass casualties, severe economic damage, and social dislocation; and the second from the possibility that disproportionate and inappropriate responses will do more damage to the fabric of society than that inflicted directly by terrorists themselves. This report strongly suggests that gathering data on lawful activity through Suspicious Activity Reporting amounts to this second kind of harm: the self-inflicted wound. Simply put, the SAR program does more damage to our communities than it does to address real and continuing threats of terrorism.

Executive Summary

Americans need to question whether or not the substantial sacrifices to our Constitutional liberties since the terror attacks on September 11, 2001 have made us significantly more safe and secure. In the case of the Suspicious Activity Reporting Initiative, our conclusion is "No." The **Suspicious Activity Reporting (SAR) Initiative**, a new framework that guides, orchestrates and connects the federal government's nationwide "Information Sharing Environment," undermines civil rights and liberties while not significantly expanding safety and security. The SAR Initiative is highly problematic, because it creates a platform for prejudice that targets two major groupings as potential terrorists: 1) Arabs, Middle Eastern persons, South Asians, and Muslims living in the United States; and 2) people with dissident views across the political spectrum. These prejudices—one based on ethnic, racial, and religious identity, the other based on ideology and belief—threaten the very foundations of our democracy.

This study provides a comprehensive analysis of the Suspicious Activity Reporting (SAR) Initiative including an overview of its role in the domestic intelligence matrix and a case study of Los Angeles' SAR Center.

In this report we:

- ➢ demonstrate that the SAR Initiative has been built on various faulty assumptions;
- ➢ expose the structural flaws that promote a reliance on existing prejudices and stereotypes;
- ➢ explain how the program erodes our Constitutional civil liberties; and
- ➢ question the basic soundness of the "Intelligence Led Policing" paradigm.

OVERVIEW

The factual record demonstrates that the main terrorist threat to people living in the United States comes from foreign terrorists linked to Al Qaeda or similar groups. Yet a revived focus on domestic "extremism" appears to have supplanted systematic, sustained investigation of foreign threats as the highest counter-terrorism priority.

The intelligence lapses that failed to prevent the September 11 terrorist attacks prompted an overhaul of U.S. domestic and foreign intelligence systems, including the creation of an expansive new domestic security infrastructure. Every official review of U.S. intelligence failures prior to the attacks concluded that bureaucratic cultures at the Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI) impeded effective information sharing and analysis.

However, there is reason to question whether the bewilderingly complex domestic security bureaucracy that has emerged in recent years has solved the government's persistent information sharing problems. This vast, Byzantine bureaucracy includes new mechanisms for federal, state, and local collaboration. At the top of the system, federal institutions sift, coordinate, analyze, and direct. At the center of the intelligence matrix, two key organs of inter-agency coordination stand out: 1) state and major metropolitan intelligence **Fusion Centers** loosely overseen and partly funded by the **De-**

partment of Homeland Security, and 2) the FBI's **Joint Terrorism Task Forces**.

At the base of the system, local police departments, ranging in size from rural sheriff's offices to major urban departments, are dedicating resources to form intelligence units. These agencies are key players in Suspicious Activity Reporting, which is based on a concept called **Intelligence-Led Policing**, in which local law enforcement officials take on new intelligence-gathering roles. The SAR Initiative takes these agencies' reporting and funnels it to Fusion Centers, key components of the national security **Information-Sharing Environment** (ISE) that facilitate the movement and exchange of terrorism-related information within the bureaucracy. Municipal police departments, county sheriffs, transit police, campus security agencies, and other law enforcement agencies lacking their own intelligence capacity have been encouraged to plug into the Information Sharing Environment through the intelligence-gathering Fusion Centers.

The SAR Initiative is slated to go nationwide at all 72 Fusion Center sites in the spring of 2010. Before the initiative becomes fully operational, the public has a right to know whether collecting intelligence about non-criminal activity is an effective counter-terrorism tool, how their Constitutional rights will be affected by this major development, and whether the program merits continued and expanded taxpayer investment.

This report maintains that, rather than fixing the existing problem of insufficient information sharing across intelligence agencies, the U.S. government has created an expanding bureaucracy of agencies whose untested information-gathering and sharing processes are flooding already overburdened intelligence systems with junk data, or "noise." In data-systems analysis, this is a familiar and well-studied phenomenon known as GIGO, or "garbage in garbage out." This overabundance of junk data does little to protect us from terrorists and much to threaten our civil liberties. The Christmas Day 2009 attempted bombing in Detroit shows on the one hand that information sharing hurdles have not been fixed, and secondly, part of the problem may be the overwhelming volume of data. Programs that lower the threshold for intelligence gathering and thereby lower the quality of data contribute to this problem.

ISSUES & FINDINGS

Unsubstantiated Claims Create a Flawed Intelligence Paradigm

The soon-to-be national SAR Initiative does not rest on an empirically solid foundation. Our investigation shows that supporters of the vast SAR Initiative have employed four myths to justify expanding the program.

Myth #1: Data-mining can spot terrorists

The SAR Initiative is tasked with producing more raw material to feed into data mining and pattern analysis systems. Initial results from the 2008-2010 SAR pilot project indicate that the Initiative is indeed producing substantially more data to be mined by Fusion Centers and federal intelligence analysts.

When fully operational, the SAR Initiative will feed the FBI's existing **National Security Analysis Center** (NSAC), a collection of more than 1.5 billion government- and private sector-generated records. The NSAC will use these documents to conduct pattern analyses: searching data sets for certain predictive models or patterns of behavior. This software solution sounds sexy, but its efficacy is dubious. So far, attempts to develop a "terrorist profile" are either so broad that they sweep up vast numbers of "false positives" – innocent individuals or organizations incorrectly flagged as potential threats – or so narrow that they are useless in predicting dangerous or criminal conduct. Data mining programs not only intrude into the privacy of millions of innocent people, they risk overwhelming intelligence systems with data garbage, forcing law enforcement to waste critical resources on bad leads and false alarms. In the world of intelligence, more is not necessarily better.

Myth #2: Police are the front line in preventing terrorism

Because it views local officers as initial collection points and producers of investigative leads for suspicious activity data, the SAR process mobilizes neighborhood police as the front lines of the "war on terror." However, local police are not trained as intelligence agents nor is intelligence gathering integral to local law enforcement's mandate. Nonetheless, neighborhood police are now expected to protect communities from terrorism by: developing local intelligence about possible terrorist activity, hardening the most vulnerable targets, and developing effective response and recovery procedures. In the long run, this new surveillance role is bound to erode community trust. Police chiefs around the country have argued out that immigration enforcement duties – e.g. under the §287(g) program – reduce crime reporting within immigrant communities. Similarly, Political Research Associates has found that surveillance of South Asian, Muslim, Arab, and Middle Eastern people creates pervasive feelings of fear, mistrust, and alienation cannot but undercut police-community relations.

Myth #3: Tracking common crimes can uncover terrorist plots

Many believe that sharing SAR Reports among all levels of government and combining them with existing intelligence and crime data will uncover terrorist plots within the United States. Given the rarity of terrorism incidents relative to the overall incidence of crime, the validity of this proposition remains uncertain. Nonetheless, it is used to justify institutionalizing and intensifying surveillance as a tool to address conventional crime. The SAR Initiative is based on the unproven theory that possible "precursor" crimes can be screened to expose linkages to larger-scale terrorist activities. This approach may encourage or even direct police and intelligence analysts to penetrate deeper into people's personal lives when common crimes of any severity are committed by South Asians, Muslims, Arabs, or people of Middle Eastern descent or others profiled as potential threats.

Myth #4: Traffic stops are key to detecting terrorism

Literature on the SAR Initiative often refers to missed opportunities to identify September 11 hijackers during routine traffic stops as justification for increased vigilance and intensified use of this everyday local law enforcement tool. Given that even *suspected* terrorism is rare, heightened suspicion of drivers and passengers can easily translate into racial, ethnic, or religious profiling. Surely officials are not suggesting that all traffic violations should be categorized as "suspicious activities"? Traffic enforcement gives local police an opportunity to collect and share vast amounts of data on millions of U.S. residents and their everyday travel. But increased vigilance on our streets and highways is much more likely to endanger civil rights and liberties than to prevent a terrorist crime. Prejudice and discrimination ultimately harm national security by dividing communities and victimizing stereotyped individuals, sending ripples of alienation and distrust throughout key segments of society.

Flawed Intelligence Paradigm Undermines Counter-terrorism Efforts

The SAR Initiative reflects the new philosophy called Intelligence-Led Policing**.** The term itself is misleading. **Pre-Emptive Policing**, the more accurate term, emphasizes surveillance and seizures of individuals *before* a criminal "predicate" exists, raising critical questions about its compatibility with American Constitutional principles such as the presumption of innocence and the warrant requirement. Also problematic is that the pre-emptive Intelligence-Led model of policing assigns disproportionate [power and influence to intelligence analysts, who may be unsworn, under-trained, and prone to politicization and bias, in part because their training and education requirements are not standardized. Furthermore, a cottage industry of private counter-terrorism training firms, such as Security Solutions International, has emerged that pushes highly inflammatory and discriminatory views about Muslims and Arabs into the ranks of analysts and law enforcement personnel.

At its core, pre-emptive policing severely undercuts the basic notion that police are public servants sworn to protect and serve, rather than intelligence agents whose job is to feed daily observations into data streams winding their way into a nationwide matrix of Fusion Centers and federal agencies. The SAR Initiative casts a wide net of surveillance: it encourages local police, the public, and corporations and businesses to engage in vaguely-defined "pre-operational surveillance" and report activities of a non-criminal nature. Ultimately, government surveillance of Constitutionally-protected, core activities such as the practice of religion and spirituality, political protest, and community organizing will weaken civil liberties and erode community trust.

The SAR Initiative is a Platform for Prejudice

The SAR Initiative enables and institutionalizes racial, ethnic, religious, and political profiling by legitimizing prejudicial assumptions about certain groups' alleged propensity for terrorism.

The history of domestic law enforcement intelligence collection is a minefield of prejudicial practices, many of which constitute civil rights violations. During the last major expansion of domestic-surveillance-as-policing, from 1956 to 1971, so many civil rights lawsuits were filed against local law enforcement agencies for maintaining intelligence files on American citizens that many opted to close their intelligence units.

The seeds for a repeat of similar abuses are evident in the policies of the SAR Initiative, which dismantles important features of the civil liberties safeguards enacted by Congress in the 1970s in response to overreaching security initiatives, notably COINTELPRO.

The SAR Initiative Invites Racial, Ethnic, and Religious Profiling

The SAR Initiative operates in a context that includes intense surveillance of racial and ethnic minority (particularly Arab, Muslim, and South Asian) communities. When collecting information, FBI agents are now authorized to enter mosques, churches, synagogues, and other places of worship without identifying themselves. A Justice Department-financed study found that following September 11, Arab Americans have a greater fear of racial profiling and immigration enforcement than of falling victim to hate crimes.

The SAR Initiative's new information sharing systems allow racialized fears about terrorism to be magnified. Its broad definition of "suspicious activity" and emphasis on so-called "pre-crime" (i.e., innocent) activity creates confusion among police, encourages subjective judgments, and opens the door for habitual, often unconscious stereotypes to enter police decision-making on reporting and investigations. Sometimes the results stretch credulity. On July 3, 2005, a man photographed three Middle Eastern men videotaping the iconic pier at Santa Monica beach. Weeks later, police seized the video, which they characterized as "probing" for a terror attack because the tourists themselves were not in the footage. Police consulted with the FBI, the Los Angeles Terrorism Early Warning Group (precursor to today's Fusion Center), and the state Department of Homeland Security. As a result, Santa Monica police requested $2 million to install pre-emptive measures such as surveillance cameras, additional patrols, and bomb-sniffing dogs to beef up security at the pier. No arrests were made, and tax payers picked up the tab. This episode shows how racial profiling harms us all.

The increased involvement of local and state law enforcement officials, who lack sufficient training and expertise in national security and counter-terrorism practices, will likely increase misconduct based on the race, ethnicity, and religion of targeted groups. Nationwide information sharing also increases the chances that innocent people caught in the surveillance web will experience ongoing difficulties.

Notwithstanding official policies prohibiting the use of racial profiling, biases in input and analysis will likely lead to an over-representation of South Asian, Middle Eastern, Arab, and Muslim populations in SAR data. This will create an untenable situation that will alienate these communities from civil society, at a time when nearly all their leaders want to work to improve safety and cultivate mutual trust.

The SAR Initiative Gives License to Target Legal Dissident Activity

The SAR Initiative jeopardizes free speech by reinvigorating urban intelligence units that have historically abused their investigative authorities for political purposes. Collecting information based on political speech, as opposed to known or suspected crimes, is disastrous for democracy. For example, the Los Angeles Police Department lists "persons espousing extremist views" as suspicious. The SAR process provides an opening for local intelligence units to shift from legitimate counter-terrorism investigation (and following leads gained from tested information sources) to broad surveillance and open-ended political fishing expeditions. Intelligence sharing between local police, sheriff's departments, the federal government, and the private sector is now being codified, mandated, and encouraged, making it far more likely for innocent people to be swept up in the anti-terror dragnet. For example, in 2008 a group of Maryland peace and anti-capital punishment activists experienced surveillance and harassment after an intelligence database categorized them as "extremists."

The SAR Initiative Erodes and Evades Time-Tested Civil Liberties Rules for Information Collection

The SAR Initiative undermines key privacy and civil liberties protections by lowering the standard for storing and sharing intelligence information generated by local police forces. When they collect, maintain, and disseminate criminal intelligence information, all law enforcement agencies receiving federal funding must follow the standards and civil liberty safeguards set forth by a federal regulation called ***28 CFR 23***. This regulation creates standards aimed at ensuring that intelligence gathering and dissemination systems are not used to violate privacy and Constitutional rights. However, the SAR Initiative circumvents these safeguards by: 1) downgrading the reasonable suspicion requirement; 2) picking and choosing when *28 CFR 23* (and its civil liberty protections) apply to a report; and 3) mischaracterizing SAR Reports as "fact based information."

Downgrading the Reasonable Suspicion Requirement.

Downgrading a protective threshold that has been in place for the last thirty years, the SAR Initiative mandates that a criminal intelligence record can be submitted to a database based on a "reasonable *indication*" rather than a "reasonable *suspicion*" of potential terrorist or criminal activity. Suspicious activity has morphed into "observed behavior **reasonably indicative** of pre-operational planning related to terrorism or other criminal activity." By decoupling so-called "suspicious activity" from actual crime, the definition of *reasonably indicative* information has become so broad as to make it virtually meaningless as a guide for law enforcement professionals. Taking the "crime" out of criminal intelligence makes it easier for reports to be based on racial and ethnic characteristics, or political ideology.

Picking and Choosing When Safeguards Apply to SAR Reports.

The SAR Initiative seems to take a back door approach to weakening proper oversight by limiting the application of *28 CFR 23* to SAR Reports. The Program Manager for the Information Sharing Environment has taken a "hands-off" approach to *28 CFR 23*, letting states and local agencies determine when and how to apply the regulation and its protections. Under federal standards, a SAR Report must meet *28 CFR 23* criteria *only if an agency wants to pass the information on to a formal criminal intelligence system* such as the **Regional Information Sharing System (RISS)**. But under the SAR Initiative, formal systems of this kind are being supplanted by new databases such as "Shared Spaces," where information gathered can be shared and stored even if it does not have a criminal predicate. The SAR Initiative enables the government to monitor people and organizations who have committed no crime, thereby weakening fundamental American freedoms, such personal privacy, the right to challenge government policies, and the presumption of innocence.

Mischaracterizing SAR Reports as "Fact Based Information."

The SAR Initiative undermines civil liberties by categorizing SAR Reports as "fact based information" rather than "criminal intelligence." This categorization allows SAR Reports to sidestep the *28 CFR 23* safeguards. This enormous loophole gives enormous—and dangerous—power, allowing law enforcement to amass unverified data about people and organizations while asserting "compliance" with civil liberties protections. Ironically, the government resists public demands to see SAR Reports which fall below Constitutional standards for record retention on the ground the reports are exempt from disclosure because they constitute "criminal intelligence." This fluidity in the characterization of SAR Reports has shielded Fusion Centers from public scrutiny, thus reinforcing the concern that data prohibited by *28 CFR 23* is nonetheless entering national criminal intelligence databases.

CONCLUSIONS & RECOMMENDATIONS

As we approach the tenth anniversary of the terror attacks of September 11, a reevaluation of our domestic security infrastructure and practices is in order. The SAR Initiative's broad criteria encouraged reporting of routine, perfectly legal activities or incidents that "just don't seem right." This enables people to fall back on personal biases and engrained stereotypes of what a terrorist looks or acts like when deciding whether to report a "suspicious activity" to police. Throughout United States history and to this day, racial and ethnic minorities have disproportionately been victimized by police violence, false arrest, and harassment. Several studies have linked higher arrest rates for Blacks and Latinos to officer's personal attitudes and perceptions, a conclusion supported through other research that focused on police prejudice and suspicion based on skin color. In light of this historical and current context, it is not unreasonable to conclude that when following up on or sharing Suspicious Activity Reports, some police will consciously or unconsciously, consider subjects' racial, ethnic, religious, and/or ideological characteristics. As a result, Suspicious Activity Reporting may magnify existing or introduce new patterns of racial and ethnic profiling. The interconnectedness of the new domestic security infrastructure will ensure that potentially biased tips can travel from a neighborhood police substation through Fusion Centers and into nationwide info-spheres.

The SAR Initiative's concern with "extremist" language gives police license to conflate free speech of dissidents with potential terrorism, inviting surveillance of people and organizations across the political spectrum whose views may be unpopular or unusual.

The lack of a consistent, uniform legal framework governing the overall SAR Initiative exacerbates the potential for prejudices to be operative throughout the system. Masses of data have been funneled to Fusion Centers across the country. Although federal standards have somewhat narrowed the criteria for suspicious activities reporting, they remain inconsistent with time-tested civil liberties safeguards. Flawed assumptions about the efficacy of data-mining to identify terror plots, plus other myths used to justify the SAR Initiative are fueling an unwise and risky strategy that targets innocuous lawful activity, rather than concentrating national resources on criminal activity and terrorism. In so doing, the SAR Initiative both erodes Constitutional liberties and threatens to food the national security intelligence pipeline with junk data that distract analysts from actual terrorist threats.

America's counter-terror effort should enable local agencies to share incidents of *reasonably suspicious* criminal activity with intelligence agencies. The country has made enormous strides in developing that sharing capacity and connectivity. The SAR Initiative, however, promotes procedures that can ultimately undermine national security, individual safety, and civil liberties.

Recommendations

1. Congress Should Hold Hearings on the SAR Initiative Prior to National Deployment. Americans have a right to know whether these programs actually fulfill their mandate to keep the population safe. Congress should evaluate the effectiveness, lawfulness, and consistency of the SAR Initiative before it can be deployed and periodically thereafter. This evaluation should be required as a condition for all information-based counter-terrorism programs. Public opinion polls reflect the distressing reality that many Americans have been willing to compromise liberty for the promise of security. All who fall under the protection of the U.S. Constitution – whether or not they accept that bargain – deserve an honest accounting of whether the government has delivered on that promise.

2. Rigorously Oversee All Suspicious Activity Reporting. Since Fusion Centers are run by state and local agencies, State lawmakers should not wait for Congress to take action. States should immediately monitor local domestic intelligence practices. The history of internal surveillance in the United States demonstrates that lax oversight leads to abuses that undermine democratic civil society. External checks and balances on Fusion Centers, which process SAR Reports, are virtually non-existent; most supervision is done by law enforcement itself. Advocates should consider following the lead of the ACLU of Massachusetts in crafting state-level independent oversight mechanisms for all Fusion Center activities to ensure compliance with Constitutional safeguards.

3. Fill Seats on the Privacy and Civil Liberties Oversight Board. Vigorous oversight is desperately needed to counterbalance the government's enormous capacity to share information and spy on innocent persons. To ensure that far-reaching surveillance technologies track terrorists rather than innocent people, Congress formed the Privacy and Civil Liberties Oversight Board. Since taking office, President Obama has allowed the board to languish, and its 2010 budget allocation sits unspent. The President should move quickly to fill all of the Board's seats with strong representation from affected communities and experienced civil liberties advocates.

4. Congress Should Pass the End Racial Profiling Act (ERPA). Passing the proposed ERPA – without a national security exemption – is a critical step to ensuring safety for all of our communities. This Act would bar certain law enforcement agencies from using racial profiling as an investigatory tool. Lengthy detentions, unwarranted scrutiny and/or harassment by government agents have unduly harmed people who have done nothing illegal. Profiling violates Constitutional guarantees and international human rights norms and distracts law enforcement from real terrorist suspects, putting everyone at risk. Further, the harm created by targeting ethnic communities only provides more ideological fodder for foreign terrorists that seek to recruit supporters within our borders.

5. Remove Non-Criminal Activity from SAR Report Criteria. SAR Programs lower the Constitutional threshold for information gathering and sharing. In its current form, the SAR Initiative will likely lead police to increasingly stop, question, and even detain individuals engaged in First Amendment-protected activity, including harmless legal conduct like photography, or on the basis of racial, ethnic, or religious characteristics. The Justice Department should amend the civil liberties safeguard *28 CFR 23* to stipulate that Suspicious Activity Reports constitute "criminal intelligence" which may only be stored if data meets the long-utilized standard of reasonable suspicion of criminal conduct. Failing that, at a minimum, the Justice Department must revise suspicious activity criteria to completely bar photography, protest gatherings, demonstrations, political lectures and other First Amendment activities as indicators of suspicious conduct. Such changes will reduce the amount of irrelevant data and increase safety and security; they should be made compulsory for any agency that wishes to participate in the Information Sharing Environment. .

6. Regulate new "Shared Spaces" Information Sharing Infrastructure. Congress and the Justice Department should take regulatory action and enact legislation to make "Shared Spaces" – a new form of intelligence database – officially subject to the Constitutional safeguards embodied in *28 CFR 23.* **7. Expose Domestic Surveillance**. Excessive secrecy limits public knowledge of local intelligence practices. Litigators defending the rights of political dissenters should routinely request records maintained in the SAR Initiative system. City, county and state governments should require local law enforcement and Fusion Center officials to detail their surveillance and documentation practices. Community activists should demand that public officials answer questions like:

- Who is responsible for the collection of intelligence information?
- What information is being collected and for what purpose?
- With whom will the information be shared?
- How long will it be retained?
- How accurate and reliable is the information?
- How will the data be secured against loss or unauthorized access?
- Will individuals know the basis for decisions affecting them, such as searches, detentions, or an intimidating knock on the door?
- How are surveillance cameras contributing to this network?
- How will individuals be able to respond to false and erroneous information?
- Are procedures in place to purge inaccurate and irrelevant data?
- Who audits the system?
- Which agencies have which missions?
- What is the role of the military in domestic intelligence?

8. Restore Constitutional Checks and Balances. Legislators should enlist courts as a critical check and balance for the new nationwide intelligence apparatus by requiring judicial permission before agencies can access personal identifying information in SAR Reports. Lawmakers should require a judicial determination whenever the government seeks to unveil the names of persons identified through data collection or mining.

9. Enhance Privacy Protections in Information-Sharing Systems. The Markle Foundation's Task Force on National Security in the Information Age and the Center for Democracy and Technology developed detailed recommendations concerning privacy protections that should be built into information sharing systems. They clearly identify steps to bring privacy laws into the 21st Century. Policymakers should refer to these guides to ensure that systems are structured appropriately. Some recommendations have already made it into law. Policy leaders need to recognize that while architects of SAR Initiative policies often claim that SAR programs abide by safeguards, the fact that standard operating procedures call for collecting non-criminal data strongly suggests that SAR practices do not adhere to the law.

10. Revisit the Need for Fusion Centers in the Post-September 11 Bureaucracy. With 72 new Fusion Centers, an intelligence net is being cast inward, bringing more of us under the government's watchful eye. The FBI's Joint Terrorism Task Forces (JTTF), which operate under the clearly-defined authority and oversight of the Department of Justice, already take the lead in investigating and stemming potential terrorist plots across the country. The redundancy of certain activities and the lack of Congressional oversight of Fusion Centers warrant the attention of public interest researchers, journalists, and policy makers. It is worth considering whether the public might be better served by relocating the Fusion Centers' data fusing function to JTTFs, thereby achieving increased of public accountability while also streamlining the bureaucracy.

11. Reject Intelligence-Led Policing in favor of Community Policing and Traditional Law Enforcement. Our research fails to find a justification for mandating that local law enforcement adopt a pre-emptive policing model. The term "intelligence-led policing" masks the fact that it is really *pre-emptive* policing, which raises serious Constitutional issues. Should police have the right to investigate non-criminal behavior indefinitely, with no limits—or built-in safeguards? Endless tracking of individuals such as outspoken political activists or religious leaders in any community to maintain "situational awareness" of alleged potential terrorism chills First Amendment rights and erodes public trust.

Pre-emptive policing is a concern not only for civil libertarians and affected communities, but also for law enforcement executives. The International Association of Chiefs of Police should reject the functional re-classification of officers as intelligence agents. Law enforcement agencies around the country have raised questions about the value of deputizing local cops as immigration agents because doing so makes certain people afraid to report crime, jeopardizing public safety. Chiefs of police should seriously consider whether it is useful to reassign officers as intelligence analysts, removing them from community problem-solving and crime response. Supervisors should take into account the detrimental effects of the intelligence-gathering approach, such as the sowing of mistrust, especially within communities that are preemptively targeted. A traditional law enforcement approach to deterring terrorism—rather than an intelligence paradigm—would allow police to focus on their core competencies and actionable leads, rather than casting a broad net and wasting resources by monitoring many innocent activities.

Platform for Prejudice

How the Nationwide Suspicious Activities Reporting Initiative Invites Racial Profiling, Erodes Civil Liberties, and Undermines Security

Veins of the Domestic Security Matrix

Americans need to question whether or not the substantial sacrifices to our Constitutional liberties since the terror attacks on September 11, 2001 have made us significantly more safe and secure. In the case of the Suspicious Activity Reporting Initiative, our conclusion is "No."

The **Suspicious Activity Reporting Initiative**, a new framework that guides, orchestrates, and connects the federal government's nationwide "Information Sharing Environment," undermines civil rights and liberties as well as security to the extent that it targets non-criminal behavior and political speech.. The SAR Initiative is highly problematic, because it creates a platform for prejudice that targets two major groupings as potential terrorists: 1) Muslims and Arabs living in the United States, and other nationalities or ethnicities perceived by many Americans through the lens of stereotypes; and 2) people with dissident views across the political spectrum. These prejudices—one based on ethnic, racial, and religious identity; the other based on ideology and belief—threaten the very foundations of our democracy.

In March 2008, the Los Angeles Police Department issued LAPD Special Order #11, which charges its officers to create "suspicious activity reports" (SARs) compiling "information of a criminal or <u>non-criminal</u> nature." The Departments of Justice and Homeland Security soon recommended that other U.S. cities take up LAPD's practice and launched a pilot project in twelve sites for the past two years. As of March 2010, the Department of Justice is poised to declare that Suspicious Activity Reporting is ready for deployment nationwide.

This study provides a comprehensive analysis of the Suspicious Activity Reporting (SAR) Initiative, including an overview of its role in the domestic intelligence matrix and a case study of the Los Angeles SAR Center.

In this report we:

- demonstrate that the SAR Initiative has been built on various faulty assumptions;
- expose the structural flaws that promote a reliance on existing prejudices and stereotypes;
- explain how the program erodes our Constitutional civil liberties; and
- question the basic soundness of the "Intelligence Led Policing" paradigm.

The failure of American intelligence prior to September 11, 2001 prompted a call for more effective data sharing, smarter analysis, and a vigilant political leadership attuned to heeding intelligence warnings. In response, the U.S. government undertook a sweeping restructuring and expansion of its domestic counterintelligence apparatus to promote information sharing and joint action.

Domestic intelligence in the past managed only an informal and unstructured cooperation based primarily on paper records. Today, interagency collaboration is reaching new heights of electronic and organizational sophistication.

With the Intelligence Reform and Terrorism Prevention Act of 2004, Congress mandated a fundamental reordering of America's intelligence-gathering institutions. It also called for the creation of an "**Information Sharing Environment**" (commonly known as the "ISE") to facilitate the exchange of terrorism information among all appropriate federal, state, and local agencies and the private sector through the use of common guidelines and technologies.[1]

Establishing uniform standards for Suspicious Activities Reporting and a technological infrastructure enabling rapid and wide sharing potentially gives government more power to detect terror plots. Domestic institutions at every level are now better positioned to collect information on U.S. citizens and residents, share incident reports, and target designated individuals.

But enhanced coordination brings risk: specifically, a greater potential for civil liberties abuses—if authorities are not effectively monitored for compliance with reasonable safeguards. With its enormous advances in electronic record keeping and transmission, the current apparatus dwarfs the resources the FBI had at its disposal when it carried out illegal surveillance and disruption operations from the 1950s through the 1980s. All U.S. residents are now vulnerable to the most advanced spying technologies the United States has ever adopted.

This report looks at how local and regional law enforcement agencies are implementing the SAR Initiative, and examines the potential im-

POLICE/TRAFFIC STOP: Literature on the SAR Initiative often refers to missed opportunities to identify September 11 hijackers during routine traffic stops to justify vigilant and intensified use of this everyday law enforcement tool.

Image Source: iStockphoto

pact of rapid, system-wide information sharing on individuals' privacy and civil liberties.

It is nearly impossible to draw clear lines of demarcation between local agencies and the multiplicity of other entities comprising today's domestic security matrix. Numerous federal agencies have been mandated to adopt Suspicious Activity Reporting processes. The departments of Energy and Defense, the Border Patrol, National Security Agency (20,000 employees) and Central Intelligence Agency (30,000 employees) all collect and/or share domestic intelligence.[2] Any appraisal of the ramifications of the government's new intelligence-sharing network should scrutinize these agencies. Such an examination, however, is beyond the scope of this report, which looks at the Suspicious Activities Reporting Initiative primarily through the lens of local law enforcement. [3]

THE SHAPE OF THE SURVEILLANCE INFRASTRUCTURE: ESSENTIAL COMPONENTS OF THE INFORMATION SHARING ENVIRONMENT

Government is pursuing the mandate for more information sharing through a "bewildering variety of new mechanisms."[4] The Suspicious Activities Reporting Initiative links these elements like veins connecting organs, pumping information from the collective tissue to intelligence-digesting bodies at the center.

At one end of the system, federal institutions like the National Counter Terrorism Center and the Office of the Director of National Intelligence (ODNI) coordinate, sift, analyze, and direct. In the center of the intelligence matrix, two key organs of interagency coordination stand out: 1) state and major urban area intelligence **Fusion Centers** loosely overseen by the Department of Homeland Security (DHS), and 2) the FBI's **Joint Terrorism Task Forces** (JTTFs). JTTFs are inter-agency policing bodies that preceded 9/11, but grew quickly in number. By contrast, there were zero formal Fusion Centers on 9/11 and there are now 72. Their role would appear to be the intelligence counterpart to the JTTF's policing function, but there is significant overlap and redundancy.

Down at the bottom, the SAR Initiative is reinvigorating intelligence units in urban- and state-level police departments. Local police departments, county sheriffs, and campus cops without the resources to hire intelligence analysts can plug into the nationwide Intelligence Sharing Environment (ISE) through Fusion Centers. Other local law enforcement agencies tap into the network by joining FBI-led Joint Terrorism Task Forces (JTTF), and lending personnel to the FBI.

At the top of this vast and Byzantine new bureaucracy, multiple agency-based advisory groups collaborate to carry out strategic and operational planning. Together, these groupings deploy various mechanisms of state power–diplomatic, financial, military, intelligence, and law enforcement.[5]

Ultimate authority for the SAR Initiative rests with the Program Manager for the (Information Sharing Environment) ISE, a division of the Office of the Director of National Intelligence, an entirely new department established by President Bush to oversee twelve federal intelligence agencies.[6] The Program Manager is responsible for establishing guidelines and standards and ensuring that information is shared with all levels of government and the private sector.

Department of Homeland Security (DHS) & Fusion Centers

Every official review of U.S. intelligence failures prior to the September 11 attacks concluded that bureaucratic cultures at the Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI) impeded effective information sharing and analysis.

In 2002 the president and Congress created the cabinet-level Department of Homeland Security (DHS).[7] Although the CIA and FBI retained their independence, 22 agencies comprising 170,000 employees were lumped into this reorganization, the most sweeping since the National Security Act of 1947 created the Department of Defense.[8]

The overall impact of the Department of Homeland Security will not be known for years, but it has already left its mark by establishing 72 operational Fusion Centers within the United States and its territories. Since DHS launched them in 2003, placing them under the Office of Intelligence Analysis, Fusion Centers have evolved largely independently of one another. Nurtured by more than $327 million in direct grant funding from 2004 through 2008, Fusion Centers won an additional $250 million in President Obama's stimulus plan for upgrading, modifying, or constructing new sites.[9]

One of former DHS Secretary Michael Chertoff's top goals was to promote intelligence sharing horizontally across federal defense agencies and vertically from federal to state to local governments.[10] Fusion Centers tie local collectors and users of intelligence data into a national information sharing network. They also break down bureaucratic barriers by assigning employees of these government entities to shared physical workspaces, often leasing space in the same buildings as FBI field offices.

Fusion Centers facilitate the collection of massive amounts of information[11] and are key to the SAR Initiative. Data streams into them from many sources, including data warehouses built by Lexis-Nexis and Axciom, intelligence groups, the federal government, as well as a plethora of public records systems, private databases, and open sources (mainly print, broadcast, and online news media). All Suspicious Activities Reports (SAR Reports) are funneled to Fusion Centers.[12] For example, New Mexico's Fusion Center, called the All Source Intelligence Center, has access to 240 state, regional, and federal agency databases, including agricultural and parks agencies.[13] To jointly assess the "threat environment," sworn and civilian intelligence analysts from DHS, FBI, the National Guard, and local law enforcement sit side-by-side to synthesize this voluminous data — including SAR Reports.[14]

Tips flow into Fusion Centers from police officers and citizens. When a Fusion Center receives or generates information determined to have a linkage or "potential nexus" to terrorism, it must send it upstream into the nationwide Information Sharing Environment (ISE).

Local police and FBI Joint Terrorism Task Forces (not the Fusion Centers) are primarily responsible for field investigations. Because state Fusion Centers often lack a local investigative capacity, they must rely on urban Fusion Centers operated by large police departments for data inputs.

Department of Justice (DOJ) / Federal Bureau of Investigation (FBI)

After September 11, the FBI dramatically shifted its primary mission from law enforcement to counter-terrorism intelligence and prevention. This transition has not been easy. According to one law enforcement expert, "FBI culture still respects door-kicking investigation more than deskbound analysis."[15] Nonetheless, the reformulation of priorities is reflected in significant organizational changes. The agency doubled its force, to 12,000 agents,[16] created an Office of Intelligence, formed a new National Security Branch as a counterweight to its law enforcement function,[17] and established field intelligence groups in all 56 field offices.[18]

The FBI also administers the Terrorism Screening Center (TSC), which maintains the Consolidated Terrorism Watchlist, a controversial and unclassified database of domestic intelligence data unrelated to international terrorism.[19] The TSC holds biographical data on about 400,000 suspected or known terrorists in 1.3 million records; it hosts a 24-hour, 7-days-a-week call center and provides data to frontline screening agents, the Transportation Security Administration, and the Customs and Border Patrol's entry database.[20]

FBI Joint Terrorism Task Forces (JTTFs)

The FBI Joint Terrorism Task Forces (JTTFs) are a key node of interagency coordination at the heart of the domestic intelligence infrastructure.[21] As a central counter-terrorism tool, JTTFs conduct surveillance, pursue leads, gather evidence, provide security for special events, conduct training, respond to incidents, and make arrests.[22]

Prior to September 11, only 35 task forces existed. Soon after, JTTFs were set up in each of the FBI's 56 field offices.[23] Today, JTTFs are based in 106 cities nationwide. They employ more than 4,400 individuals, more than four times the pre-September 11 total. Over 600 state and local agencies, along with 50 federal agencies participate in JTTFs.

As multi-agency coordinating bodies, JTTFs allow the federal government to tap into local police resources across several jurisdictions, and enable the FBI to tackle complex, multi-jurisdictional issues.[24] Local police lend full-time staff to JTTFs to work with federal agencies such as Immigration and Customs Enforcement, Customs and Border Patrol, the Secret Service, and Transportation Security Administration.

Enhanced coordination brings risk: specifically, a greater potential for civil liberties abuses—if authorities are not effectively monitored for compliance with reasonable safeguards.

Due to lack of public accountability, inadequate local oversight, and prejudice-based surveillance and profiling, JTTF activities raise numerous civil liberties concerns. In part because they answer to the FBI, police officers assigned to JTTFs follow permissive rules for domestic investigations and are cloaked in layers of secrecy that evade traditional oversight mechanisms.[25] For example, partnership agreements routinely provide that the actions of local officers assigned to the JTTF are confidential; even local chiefs of police are unaware of their subordinates' activities with the JTTF.[26] JTTFs have targeted political dissidents for surveillance and harassment, reinforcing concerns that the nation's "homeland security" apparatus is vulnerable to deployment for purposes of political repression.[27]

National Counterterrorism Center (NCTC)

The National Counterterrorism Center (NCTC) is the primary U.S. government agency responsible for analyzing and integrating all intelligence pertaining to terrorism – except for purely domestic terrorism, for which the FBI is the lead agency.[28] It reports to the Director of National Intelligence. Large components of the CIA, Pentagon, and FBI counter-terrorism divisions are located on NCTC's campus. NCTC maintains an international terrorism watchlist called "Terrorist Identities Datamart Environment" (TIDE), which lists about 550,000 known or suspected terrorists. NCTC garnered attention after a man on this watchlist attempted to ignite an incendiary device on Northwest Flight 253 in Detroit on December 25, 2009.[29]

State, Local, and Tribal Law Enforcement

Fully integrating local law enforcement into the Information Sharing Environment (ISE) is a core goal of the SAR Initiative. Soon after the September 11, 2001 attacks, the U.S. Departments of Justice and Homeland Security sent half a billion dollars to the states to beef up local and state intelligence operations and enhance local law enforcement agencies' capacity to respond to future attacks.[30] Funded programs included: increasing emergency response planning personnel; updating response plans for chemical, biological, or radiological attacks; ensuring the interoperability of communications systems; and increasing focus on terrorism preparedness.[31]

The counter-terrorism capabilities of local police departments — from rural sheriff offices to major police departments with dedicated intelligence staff — vary widely.[32] New York City developed a counter-terrorism bureau with more than 100 detectives assigned to the FBI's Joint Terrorism Task Force, detectives deployed overseas, and over 700 investigators devoting almost 50 percent of their resources to counter-terrorism.[33]

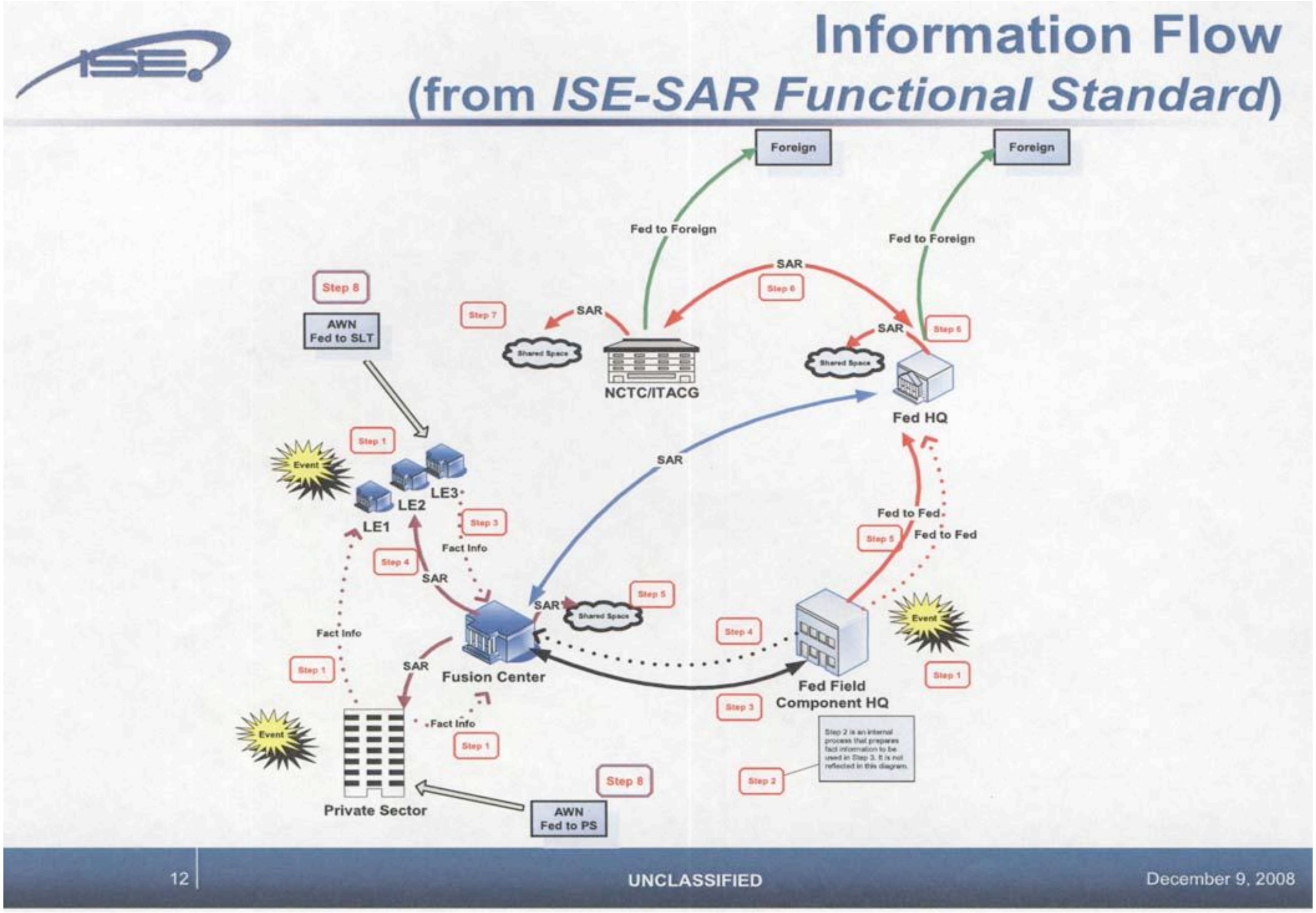
Privacy and Civil Liberties Oversight Board (PCLOB)

With the SAR Initiative aiming to mobilize 800,000 American police officers as intelligence gatherers, oversight needs and challenges are growing by the day. But so far, few government resources have been devoted to counter-balancing the massive new intelligence infrastructure with institutional mechanisms to ensure compliance with Constitutional civil liberties protections, privacy safeguards, and international law.

According to a 2009 ACLU white paper, “[T]he independent oversight structures that have been created to oversee these vast, city-sized institutions are pitifully small and weak.”[34]

The 9/11 Commission recommended creating an executive branch entity to oversee adherence to civil liberties principles, but offered scant guidance on implementation.[35] In 2004, Congress established the Privacy and Civil Liberties Board (PCLOB), a hollow shell located in the Executive Office of the President without a shred of independent authority.[36]

In 2007, Congress removed the PCLOB from the White House and gave it independent agency status. However, as of March 2010, the Board had yet to be named and had no staff. For



Information Flow
(from *ISE-SAR Functional Standard*)

Step 2 is an internal process that prepares fact information to be used in Step 3. It is not reflected in this diagram.

12 UNCLASSIFIED December 9, 2008

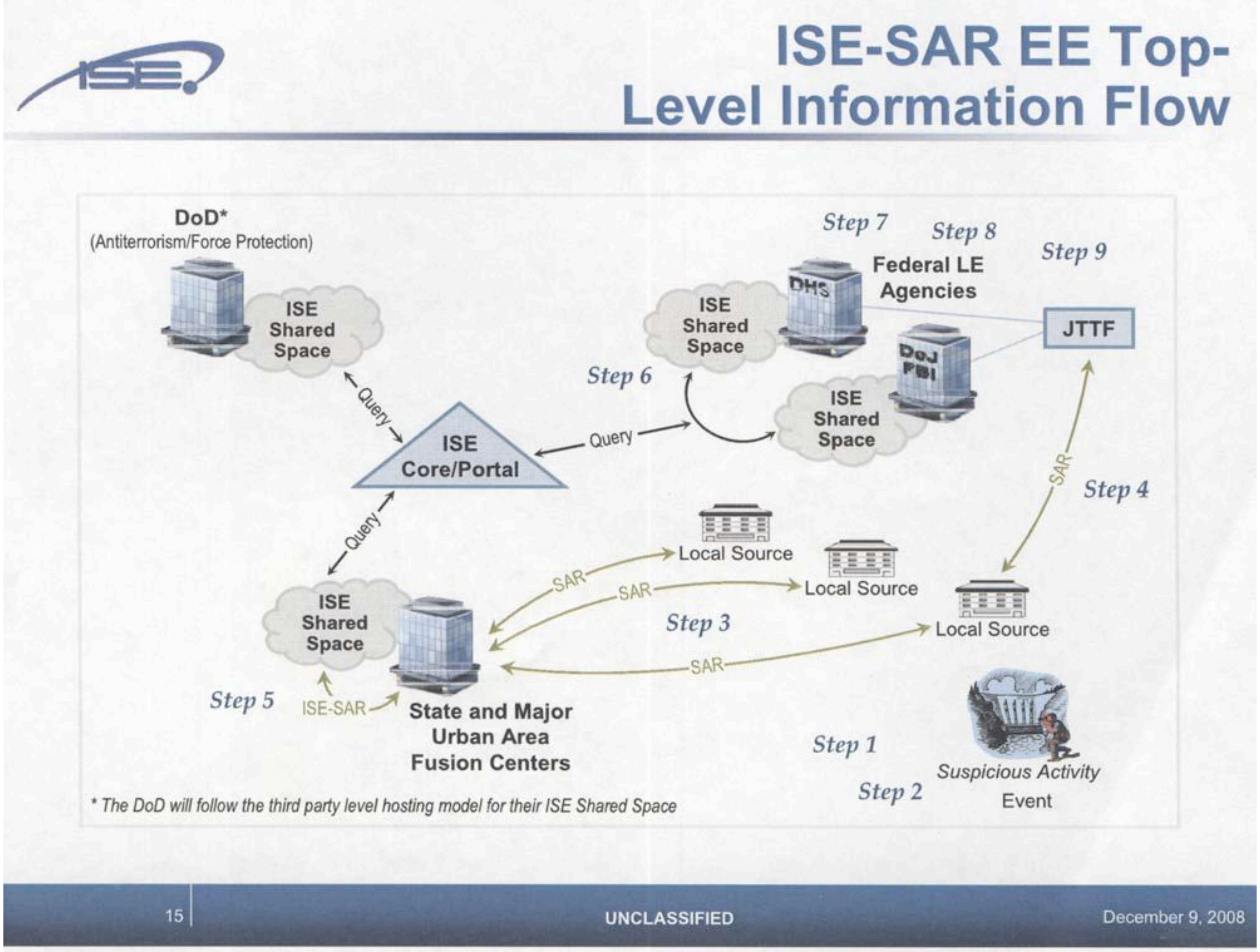
Figure 1 depicts how local law enforcement agencies (LE1, LE2, LE3) are linked to other institutions in the infrastructure through Suspicious Activity Reports.

the 2009 fiscal year, Congress allocated less than $7 million to the PCLOB, although it must monitor an intelligence establishment with a budget of at least $57 billion and tens of thousands of employees.[37]

INTEGRATING POLICE INTO THE INFRASTRUCTURE THROUGH FUSION CENTERS

The SAR process integrates law enforcement into the domestic security apparatus by channeling the information flow through Fusion Centers, which serve as a key conduit between local agencies and other ISE participants.

The sharing of sensitive and classified information has reached unprecedented levels. Since September 11, more than 6,000 state and local police officers have been granted access to classified material involving alleged terrorist threats, "the broadest dissemination of secret information in U.S. history," according to the FBI.[38] Federal officials view Fusion Centers as a "force multiplier" to tap into the data collection potential of close to a million officers in over 15,000 law enforcement agencies, plus local emergency responders. "There is never enough information when it comes to terrorism," says Major Steven G. O'Donnell, deputy superintendent of the Rhode Island State Police.[39]


ISE-SAR EE Top-Level Information Flow

* The DoD will follow the third party level hosting model for their ISE Shared Space

15 UNCLASSIFIED December 9, 2008

Figure 2 depicts how local law enforcement agencies route Suspicious Activity Reports.

The SAR Initiative provides collectors of information with a defined data exchange and dissemination process in which local agencies make SAR Reports available to state and/or urban area Fusion Centers. Federal agencies forward their reports to the appropriate regional, district, or headquarters office. If a local agency can determine that a given activity directly connects to terrorism-related criminal activity, it provides the information to the JTTF, which conducts a threat assessment and/or investigation.

At Boston's Fusion Center, also known as the Regional Intelligence Center ("BRIC"), run by the Boston Police Department, superintendent Paul Fitzgerald explains,

> We collect from our region and we fuse it together as best we can and put it back out so that everyone's getting the best information they can get and then we forward it up to the state [fusion center], and if the other three hubs are doing that then the state has something to fuse and throw back out.[40]

By incorporating police into intelligence-gathering systems, the SAR process helps break down the bureaucratic wall between law enforcement and intelligence. According to Mark Kagan, a former analyst with the Department of Defense, "Law enforcement and intelligence have been – and in many circumstances still are – mutually exclusive if not antagonistic to each other. What law enforcement people do is not what intelligence people do and they like to see it that way, and so often it stays that way."[41] Well-resourced institutions have argued for integrating police into domestic security in this way. For example, in a 2002 essay for the conservative Heritage Foundation in 2002, Dana R. Dillon downplayed police intelligence abuses when she wrote:

> The intelligence Fusion Center and federal agencies must create systems that maximize the efforts of state and local police rather than a one-way transfer of information that cuts them out. The most expeditious means of accomplishing that goal is for state and local governments to reestablish LEA [law enforcement agency] intelligence units. Many of these organizations were dissolved in the 1970s because of relatively few (and isolated) alleged abuses of the intelligence they gathered. The U.S. Attorney General and State Attorneys General can publish frameworks for activity to prevent the abuse of such centers.[42]

Unfortunately, history shows that police need more than a "framework" to prevent abuse; they need rigorous independent oversight and clear guidelines. In an illustration of how far the pendulum has swung, the SAR Initiative seriously weakens protections that Congress and the Department of Justice enacted in the 1970s to prevent police departments from abusing their new powers.

The Nationwide Suspicious Activities Report Initiative

Rather than fixing the existing problem of insufficient information sharing across intelligence agencies, the U.S. government has created an expanding collection of agencies whose untested information-gathering and sharing processes are flooding already overburdened intelligence systems with junk data, or "noise." In data-systems analysis, this is a familiar and well-studied phenomenon known as GIGO, or "garbage in garbage out."

The planned nationwide expansion of the Suspicious Activities Reporting (SAR) Initiative threatens to significantly increase the volume of noise entering the system. The limited information available to the public at this time suggests that these unfiltered "data dots" rarely if ever yield valuable puzzle pieces that lead to terrorism detection and prevention. Instead, they may obscure the pictures that real intelligence gathering and analysis must reveal in order to keep us safe.

ORIGINS: FROM "TIPS AND LEADS" TO SAR REPORTS

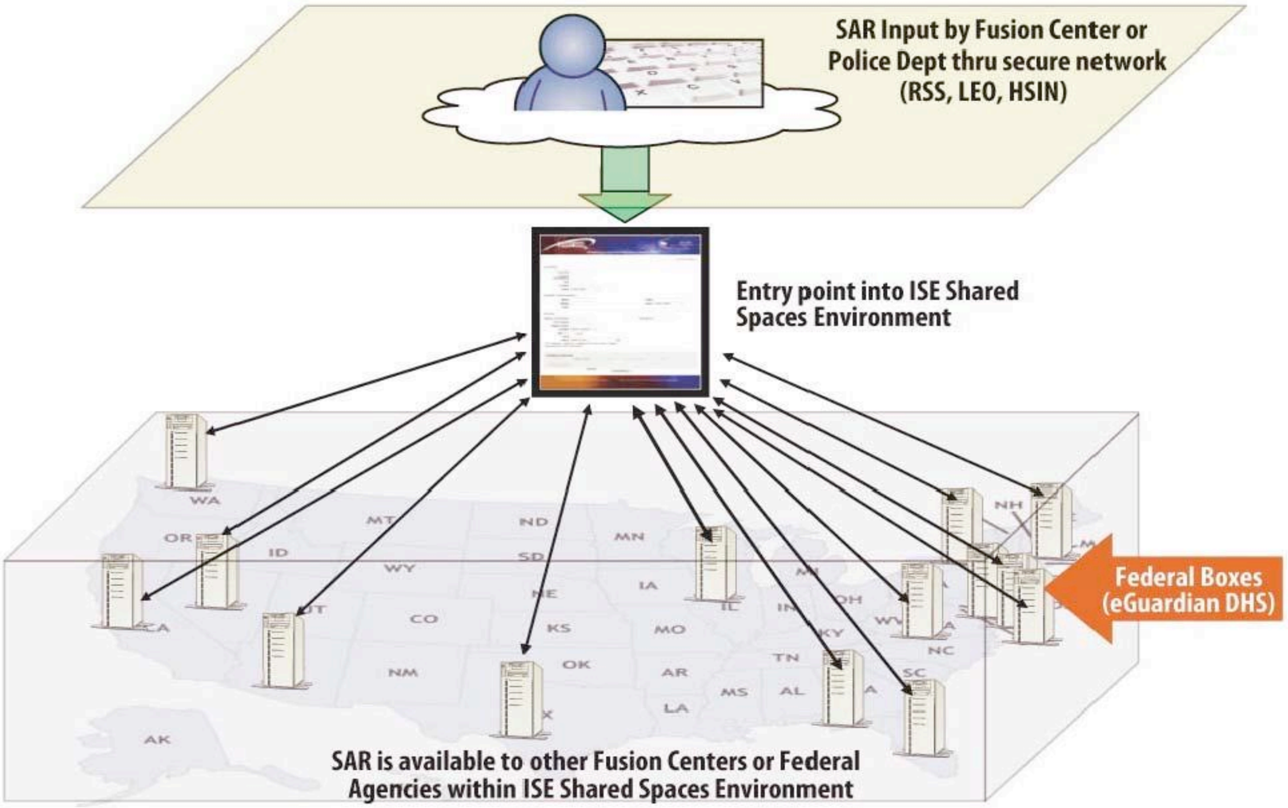
Since September 11, law enforcement and homeland security agencies nationwide have encouraged different ways to report "suspicious activity."

Despite emphasizing that "people are not suspicious, behavior is," these SAR programs have frequently documented public prejudice rather than threats to public safety. For example, in 2004, the Coast Guard implemented "America's Waterway Watch" to encourage boaters and pier workers to report "suspicious" boat rentals or persons videotaping from shore in a furtive manner.[43] [See Appendix 1 for a copy of the Coast Guard SAR Form]. Similarly, in 2006, after a series of "suspicious" boat rentals, including the case of Middle Eastern men without fishing gear who rented a boat and were seen "taking pictures of a local landmark," the New Jersey State Police formed the Maritime Security Initiative.[44] In 2007, the FBI launched an international search for two Middle Eastern-looking men after a Seattle ferry captain witnessed them taking pictures below deck. The men, citizens of an EU country, turned themselves in after seeing their photo in *The New York Times*. The two software consultants explained that they had been simply astounded by the ferry's girth and wanted to show friends and family back home.[45] Similarly, in 2005 three men of Middle Eastern descent were stopped and questioned after being seen videotaping the iconic Santa Monica pier in a "suspicious" manner.[46]

These incidents — none of which resulted in criminal prosecutions, but likely entailed the collection and sharing of personal data — preceded the national SAR Initiative, which was unveiled in 2006 and formally launched as a pilot project in 2008. The Initiative established national standards to assess suspicious activity, introduced a uniform and synchronized system for sharing and searching SAR-based data, and instituted new measures to increase the production and sharing of SAR Reports by more policing agencies.

Documenting suspicious activities has been standard operating procedure for federal, state, and local law enforcement agencies for decades, but the process has generally been fragmented and disjointed. Police detectives' "Tips and Leads" files are the natural cousin to SAR Reports. For instance, Boston police keep confidential reports on field observations (FIO), frisks (F), and searches (S), called "FIOFS.[47] Under FIOFS procedures, officers check a box marked "terrorism" when they encounter "suspected terrorist activity," including "groups of individuals living together with no visible means of support."[48]

Tips and Leads files support specific law enforcement investigations leading to possible prosecutions and court cases. The SAR program systematizes the collection of locally generated data for a different purpose: collecting intelligence on threats to national security. Prior to the SAR Initiative, data from Tips and Leads forms was easily lost among the incident reports found in local Computer Aided Dispatch systems. Processes for analyzing and disseminating these data were largely ad hoc, centered on individual agency needs, and often heavily dependent on long-established personal relationships, rather than a coordinated sharing strategy.[49] The lack of standardization among jurisdictions hampered efficiency.


SAR Input by Fusion Center or Police Dept thru secure network (RSS, LEO, HSIN)
Entry point into ISE Shared Spaces Environment
Federal Boxes (eGuardian DHS)
SAR is available to other Fusion Centers or Federal Agencies within ISE Shared Spaces Environment
WA
OR
CA
ID
MT
WY
UT
CO
NM
ND
SD
NE
KS
OK
MN
IA
MO
AR
LA
IL
IN
OH
KY
TN
MS
AL
WV
NC
SC
NH
AK

SHARED SPACES GRAPHIC: Fusion Centers are required to replicate data from their systems to an external server. A secure portal is created that allows a Fusion Center to decide which information it will share into a "Shared Space." Once the information enters the "Shared Space," the Fusion Center's system searches all databases in the National Fusion Center Network; this allows a Fusion Center to aggregate any and all relevant information that exists throughout the network.

Image Source: DOJ, Bureau of Justice Assistance as reproduced by the Congressional Research Service.

STANDARDIZING SAR TECHNOLOGICAL INFRASTRUCTURE

In 2006, the federal government began to institutionalize SAR processes by leveraging community policing and intelligence-led policing strategies [see Timeline in Appendix 2]. As this report goes to press in March, 2010, a national Program Management Office is being established to transition the SAR Initiative from a pilot program (with 14 pilot sites) to nationwide implementation.[50]

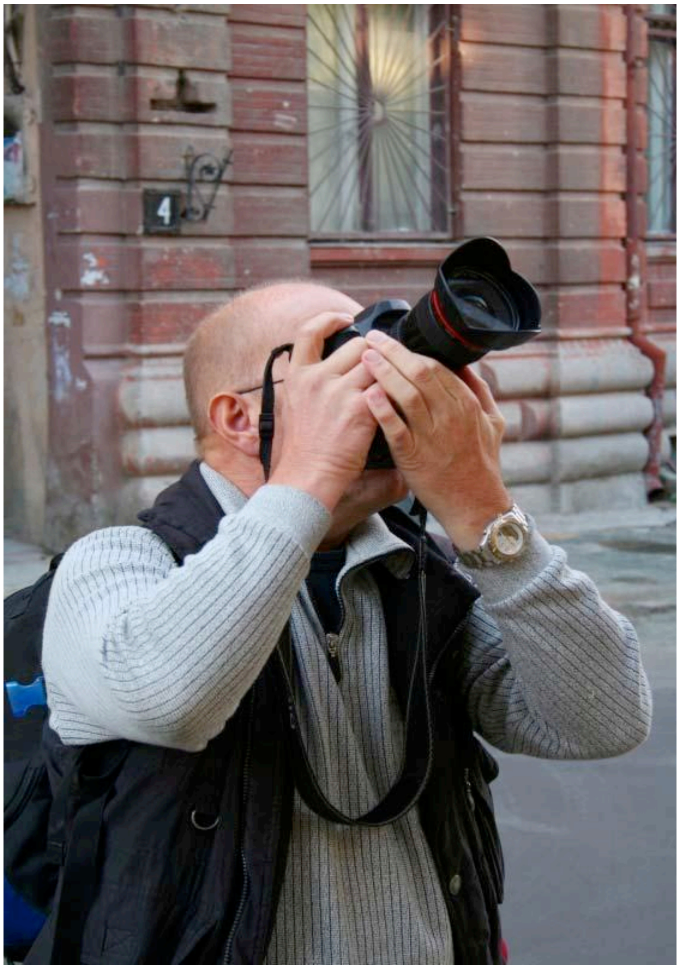


PHOTO TAKER: Legal activities, such as photography, constitute suspicious activities. One such photographer, Duane Kerzic, [not pictured] was arrested in 2008 while taking photos on a public platform at New York's Penn Station. He was taking pictures for Amtrak's Annual Photo Contest.
Source: iStockphoto

The SAR pilot program creates a national information-sharing infrastructure with common operating systems and software, thereby allowing federal agencies to easily access data collected by state and local agencies. Participants are required to use a standard reporting format and common national data collection codes, so that police records can be integrated with sensitive federal data for analysis, or for tracking individuals and groups under surveillance. This new system does not rely on local police uploading information to a specific federal database. Rather, local agencies and Fusion Centers can save reports deemed "related to terrorism" on locally-controlled electronic "Shared Spaces" accessible to all authorized participants in the Information Sharing Environment (ISE).

So far, the national SAR Initiative has failed to establish a singular, high national standard of privacy protection. SAR standards allow agencies to share reports in a "Detailed Format" (includes personal information) or a "Summary Format" (does not reveal such information). Unfortunately, America's patchwork of differing, sometimes contradictory privacy laws means that jurisdictions use these formats differently. Further, ISE participants are not required to obtain judicial approval — a keystone of the American checks and balances system — before requestors can see the personal information in a report.[51]

It appears the new information exchange network built by the SAR Initiative will facilitate the unprecedented growth and unregulated pooling of locally-produced intelligence data. Anyone concerned about government's power to identify, monitor, and target individuals for adverse, discriminatory treatment will be troubled by its expanded capacity to rapidly share data nationwide. Investigation by secretive agencies can have a chilling effect on the exercise of First Amendment rights. Therefore, as the government's ability to develop more tools to collect and share information mushrooms, the necessity for adequate controls and safeguards grows exponentially. Before this program is unleashed nationwide, it is worth assessing the effectiveness of Suspicious Activity Reporting as a key counter-terrorism tool.

UNSUBSTANTIATED CLAIMS CREATE A FLAWED INTELLIGENCE PARADIGM

Assessing the value of this attempt to nationalize intelligence gathering and sharing requires evaluating the claims used to justify it.

Supporters of the SAR Initiative have deployed four "myths in the making" to justify expanding Suspicious Activity Reporting and easing restrictions on collecting information. Close examination of these propositions suggests that the SAR Initiative does not rest on an empirically solid foundation.

Myth #1: Data-mining can spot terrorists

One of the SAR Initiative's main goals is producing more data to feed into data mining programs.[52] Support for data mining increased after it was learned that certain database searches could have disclosed connections between Nawaf al Hazmi and Khalid al Midhar — the two September 11 hijackers who were on a government watchlist prior to the attacks — with seven other hijackers previously unknown to the government.[53] Post-September 11 efforts to "connect the dots" have included expanded use of data mining and pattern analysis programs. [See Appendix 3]

Initial results from the 2008-2010 SAR pilot project indicate that the Initiative is indeed producing substantially more data for Fusion Centers and federal intelligence analysts to mine. When fully operational, the SAR Initiative will feed the FBI's existing **National Security Analysis Center** (NSAC), a collection of more than 1.5 billion government- and private sector-generated records. The NSAC will use these documents to link up and search electronic data sets for certain connections, patterns of behavior, and other predictive models.[54] Data mining involves pattern-based queries, pattern analysis software, searches, or other analyses of one or more electronic databases. It is a type of database analysis that attempts to discover useful patterns or relationships in a group of data — particularly the discovery of previously unknown relationships — especially when derived from different databases.[55] It is not known whether the predictive models use subjects' religion, ethnicity, family names, or national origin to generate lists of suspicious individuals meriting further scrutiny.

These software solutions sound compelling, but their efficacy is dubious. So far, attempts to develop a "terrorist profile" are either so broad that they sweep up vast numbers of "false positives" — innocent individuals or organizations incorrectly flagged as potential threats — or so narrow that they are useless in predicting dangerous or criminal conduct.

"The idea behind fusion centers is to input massive amounts of data," says former FBI agent Colleen Rowley, "but that doesn't mean the quality of the information is increased. Every study done says this approach has not been able to be successful and get lots of false positives."[56]

A 2008 National Research Council study concluded that highly automated tools and techniques cannot be easily applied to the difficult problem of detecting and preempting a terrorist attack, and success may be beyond reach:

> Far more problematic are automated data-mining techniques that search databases for unusual patterns of activity not already known to be associated with terrorism. Although these methods have been useful in the private sector for spotting consumer fraud, they are less helpful for counter-terrorism precisely because so little is known about what patterns indicate terrorist activity; as a result, they are likely to generate huge numbers of false leads. Actions such as arrest, search, or denial of rights should never be taken solely on the basis of an automated data-mining result.[57]

The National Research Council concluded that "automated identification of terrorists through data mining (or any known methodology) is neither feasible nor desirable as a goal of technology development efforts."[58]

The so-called "success stories" that have uncovered links to terrorism typically resulted from old-fashioned, thorough detective work, rather than software-based pattern analysis of nuggets of information in SAR Reports. For example, in the infamous string of gas station robberies in Southern California, committed to finance a planned attack on malls and mosques, the link to terrorism was uncovered during a search warrant of the suspect's residence — not by intelligence analysis, as Los Angeles County and federal officials have suggested.[59]

The link to terrorism was uncovered during a search warrant of the suspect's residence — not by intelligence analysis, as Los Angeles County and federal officials have suggested.

Instead of understanding this kind of instance as a lesson learned, the SAR Initiative takes a leap in the opposite direction by devoting enormous resources to data-mining systems. Data mining not only intrudes into the privacy of millions of innocent people, it risks overwhelming intelligence systems with data garbage, forcing law enforcement to waste critical resources on bad leads and false alarms.

Myth #2: Police are the front line in preventing terrorism

Because it views local officers as the logical originators of investigative leads for all suspicious activity data, the SAR Initiative mobilizes neighborhood police as the front lines of the "war on terror." However, local police are not trained as intelligence agents nor is intelligence gathering integral to local law enforcement's mandate. Nonetheless, neighborhood police are now expected to protect communities from terrorism by developing local intelligence about possible terrorist activity, hardening the most vulnerable targets, and developing effective response and recovery procedures.

By adopting a pre-emptive model called "intelligence-led policing," the SAR Initiative creates a risk that local jurisdictions will undermine their core functions, moving from "protect and serve" to "suspect and report." The Initiative has already begun reinvigorating urban police intelligence units, many of which illegally spied on labor militants, union organizers, and leftist political activists from the late 1800s through the early 1970s, and infiltrated antiwar and civil rights groups in the 1960s.[60] Advocates for the SAR Initiative often stress the slogan "all terrorism is local."[61] Joan McNamara, head of the LAPD's counter-terrorism bureau, frames police as the "first preventers" of terrorism, in a "dramatic paradigm shift," both for the federal government and for local agencies themselves.[62] Former LAPD Chief William Bratton summarized the predominant view: "The key to combating terrorism lies in community engagement, developing partnerships beyond mere liaison and sustaining and building on a base of trust with the community and partner agencies."[63] Through the SAR Initiative's lens, the terrorist threat is not based at a training camp in Yemen or a safehouse in Germany or Pakistan; it is here at home.[64] In fact, the political motivations driving large-scale terror threats originate abroad in the form of grievances with U.S. foreign policy or military occupations.[65]

The shift in priorities underlying the SAR Initiative may have adverse consequences not only for the nation's ability to effectively counter international threats (by diverting resources and leadership), but also by increasing government surveillance of U.S. communities, inviting racial profiling, and opening the doors to repression of political activity. Given the political motivations underlying terrorist acts, SAR processes may embolden local police to monitor free speech activities, thus hampering political freedom and democratic participation. The religious dimensions of some terrorist attacks against the United States also increase the risk that police will illegally and heavy-handedly monitor certain forms of religious express, as with Massachusetts Governor Mitt

Romney's suggestion in 2005 that mosques be wiretapped.

Myth #3: Tracking common crimes can detect terrorist plots

Rhetoric surrounding the SAR Initiative often assumes that terrorist plots can be detected by analyzing other criminal activity. Many believe that sharing SAR Reports among all levels of government and combining them with other crime and intelligence data will uncover terrorist plots within the United States. Given the rarity of terrorist incidents relative to the overall incidence of crime, the validity of this proposition remains uncertain. Nonetheless, it is used to justify institutionalizing and intensifying surveillance as a tool to address conventional crime.[66]

The SAR pilot program has found that most participants in the ISE are leveraging the SAR process to meet their department's expansive "all-crimes" mandate.[67] For example, at the Boston Regional Intelligence Center, Superintendent Paul Fitzgerald emphasized how intelligence analysts work on solving normal crimes:

> We have a really great focus on all crimes. We have analysts assigned to every crime. We are heavy on homeland security and violent crime; those are what are designated as our 2 priorities. We are very, very focused and have unbelievable up to date info on car breaks, B&Es [breaking and entering cases], commercial B&Es, larcenies from motor vehicles. Every topic of crime is covered every day out of the BRIC so it hasn't taken away, it's only really benefited us because we have analysts assigned from other departments and they share all that information . . . so we're really able to look for any trends, similar motives.[68]

This approach is bolstered by experts' belief that some types of criminal activity — including identity theft, trafficking in illegal merchandise, money laundering, and wire fraud — have a "nexus" to terrorism. In some cases, these crimes have been linked to terrorists' efforts to finance operations or support groups like Hezbollah.[69] However, a 2006 Department of Justice-financed study cautioned that making such linkages can be extremely difficult due to a shortage of validated research about the precursor crimes-terrorism nexus.[70]

In effect, the SAR Initiative is based on the unproven theory that possible "precursor" crimes can fruitfully expose linkages to larger-scale terrorist activities. This approach invites abuse by legitimizing efforts to penetrate deeper into peoples' personal lives when common crimes of any severity are committed by South Asians, Muslims, Arabs, or people of Middle Eastern descent or others labeled as potential threats.

The SAR pilot program has found that most participants in the ISE are leveraging the SAR process to meet their department's expansive "all-crimes" mandate.

Myth #4: Traffic stops are key to detecting terrorism

Literature on the SAR Initiative often refers to missed opportunities to identify September 11 hijackers during routine traffic stops to justify vigilant, intensified use of this everyday law enforcement tool. One district attorney theorized, "Had a system been in place to share this information with the FBI, it may have alerted them that a suspected al-Qa'ida operative was present within the National Capital Region."[71]

Former NYPD Terrorism Interdiction Unit leader Lou Savelli writes, "Keep in mind how many of the 9-11-01 hijackers had contact with law enforcement officers in various parts of the country and how many unsuspecting law enforcement officers, in any capacity, may have such contact with terrorists today or in the future."[72] The intelligence chief for the Miami-Dade Police Department, Maj. Michael Ronczkowski, says that traffic stops give police an opportunity to "encounter thousands of people, many with extreme ideologies, something rarely done by federal law enforcement officials."[73]

In the context of considering domestic counterterrorism strategy, what are the implications of this repeated emphasis on traffic stops? Given the fact that terrorism, even *suspected* terrorism, is rare, heightened suspicion of drivers and passengers can easily translate into discriminatory profiling based on national origin, race, religion or ethnicity.[74] Following are some cases in point:

- Are officials suggesting that all traffic violations should be entered as "suspicious activities?" Ziad Jarrah, a 9/11 hijacker, was stopped in Maryland for speeding and paid his ticket. Should his data have been shared system-wide? On what basis should he have been subject to additional detention and questioning?
- Will officers query watch lists at the Terrorist Screening Center for every stop, or only when the driver matches a racial, ethnic, or religious stereotype of what constitutes a terrorist? Is there an unspoken policy that local police will subject certain classes of people to database checks, such as Muslims, foreign nationals, and people of Middle Eastern, Arab, or South Asian descent?
- If 9-11 hijacker Mohammed Atta had been arrested in Florida for his unpaid traffic ticket, should authorities have led a deeper investigation of his life? Do officials suggest that Fusion Centers conduct a link analysis for every individual suspected of violating the traffic code?
- Will indicators of political persuasion such as anti-government bumper stickers or driver attire trigger the collection and sharing of data?

Traffic enforcement gives local police an opportunity to collect and share vast amounts of data on millions of U.S. residents and their everyday travel. However, increased vigilance on our streets and highways is much more likely to endanger civil rights and liberties than to prevent a terrorist crime.

The advantage of 20-20 hindsight in regards to missed opportunities to apprehend terrorists before they could strike creates powerful and understandable incentives to implement policies that might have prevented those past attacks. Given the known consequences of having failed to apprehend those individuals, even draconian measures can have the ring of common sense about them – at least to individuals and communities that wouldn't expect to be profiled under such measures. A background check and comprehensive "link analysis" on every Muslim and Arab within America's borders might have nabbed Mohammed Atta, but at a cost to our Constitutional freedoms that would have been unacceptable.

Prejudice and discrimination ultimately harm national security by dividing communities and victimizing stereotyped individuals, sending ripples of alienation and distrust throughout key segments of society.

FLAWED INTELLIGENCE PARADIGM UNDERMINES COUNTER-TERRORISM EFFORTS

Intelligence Paradigm Increases Domestic Surveillance and Undermines Trust

The SAR Initiative reflects a new philosophy, founded on "Intelligence-Led Policing" (ILP), which shifts law enforcement from a crime-solving paradigm to an intelligence paradigm focused on detecting threats and preventing terrorist acts.[75]

Without any public debate whatsoever, the National Criminal Intelligence Sharing Plan (NCISP) has called on every local policing agency to develop an intelligence function in order to "protect the American public against terrorism and all other criminal acts that threaten its safety."[76] In fact, the NCISP uses the term "intelligence-led policing" 30 times in that document without ever defining the concept.[77]

The intelligence community has wholeheartedly embraced the philosophy without weighing the potential effects of this major shift on community trust. Ameena Qazi, a civil rights attorney who has represented numerous Muslims accused of "suspicious activities," says that pervasive surveillance of Arab and Muslim communities erodes participation in mosques and leads to isolation and distrust of government:

> American Muslims have consistently affirmed our willingness to assist law enforcement in protecting our nation's security, but we've observed an unfortunate trend of law enforcement overstepping its bounds by routinely targeting American Muslims for intrusive questioning or surveillance, and now we are seeing the nexus between this targeting and repercussions in a person's immigration applications or travel experiences. In turn, this has led some individuals to question their active engagement in mosques, or participation with Muslim organizations, thinking that the more they burrow the less likely they are to face adverse government action. And it is exactly this sort of isolation that has the potential to breed antisocial or antiestablishment behavior, not to mention depressing the same constitutional values law enforcement is sworn to protect[78]

Law enforcement leaders should conduct a full assessment of the effects of pre-emptive policing on democratic society and community safety. Police chiefs around the country have argued out that immigration enforcement duties – e.g. under the §287(g) program – reduce crime reporting within immigrant communities. Similarly, Political Research Associates has found that surveillance of South Asian, Muslim, Arab, and Middle Eastern people creates pervasive feelings of fear, mistrust, and alienation cannot but undercut police-community relations.

Intelligence-Led Policing is Pre-Emptive Policing

Although originally articulated as a law enforcement operational strategy to reduce crime by combining crime analysis with criminal intelligence, in recent years intelligence-led policing is being sold as a key tool of counterterrorism.[79] In the counterterrorism context the term is something of a misnomer. Intelligence-led policing is more accurately described as a form of "pre-emptive policing," which emphasizes surveillance and seizures of individuals before a criminal "predicate" exists.

Intelligence-led policing suffers from strategic overreach, even sliding into mission creep, in that it gives police license to target perceived threats on the basis of national origin, ideology, or religion.

As a law enforcement approach, intelligence-led policing departs from the community-oriented philosophies of policing that many departments have gradually adopted over the past 20 years. Intelligence-led policing elevates the role of data collection and analysis, emphasizing intensified surveillance to search for non-criminal threats or suspicious conduct, as opposed to actual incidents of crime.

In short, it is threat- rather than incident-driven. Analysis is based on tips, leads, SAR Reports, and sophisticated software programs rather than known facts from reported crime data and investigations. According to a leading scholar on ILP from the United Kingdom, J.H. Ratcliffe, intelligence-led policing:

- …emphasizes information gathering through the extensive use of confidential informants, offender interviews, analysis of recorded crime and calls for service, surveillance of suspects, and community sources of information.
- …assigns a central role for civilian and sworn intelligence analysts who examine and synthesize the information to create a more holistic view of the environment, from which enforcement targets, preven-

tion activities, and further intelligence-gathering operations can be determined.

- …shifts the focus from reactive, individual case investigations to a management philosophy that places greater emphasis on information collection, sharing, and collaborative, strategic solutions to crime.[80]

ILP is an "underlying philosophy of how intelligence fits into the operations of a law enforcement organization," rather than an "add-on responsibility,"[81] and its ideological ascendancy in the ISE represents a complete structural shift.

Pre-emptive policing may violate Constitutional norms

The concept of pre-emption implies surveillance and seizures of individuals before a criminal predicate exists, raising critical questions about its compatibility with American constitutional principles, such as the presumption of innocence and the warrant requirement.

As embraced in the National Criminal Intelligence Sharing Plan, intelligence-led policing suffers from strategic overreach, even sliding into mission creep, in that it gives police license to target perceived threats on the basis of national origin, ideology, or religion.[82] The view of Maj. Ronczkowski, the head of Miami-Dade's Homeland Security Bureau, exemplifies this danger:

> [Local law enforcement] are more apt to encounter the passive or active supporters of the extremist ideology or even a member of the active cadre. Local law enforcement should not be taking a posture of looking for someone with a destructive device, but rather look for those puzzle pieces that can lead to identification of the pre-incident indicators that exist in every terrorist act.[83]

Also problematic, pre-emptive, intelligence-led model of policing assigns disproportionate power and influence to intelligence analysts, who may be unsworn, under-trained, and prone to politicization and bias, in part because their training and education requirements are not standardized.[84] Furthermore, a cottage industry of private counter-terrorism training firms has emerged that pushes highly inflammatory and discriminatory views about Muslims and Arabs into the ranks of analysts and law enforcement personnel. For example, Security Solutions International holds seminars on the origins of Radical Islam, including a course on "the Legal Wing of Jihad in America," which alleges that some Muslim-American advocacy organizations attempt to undermine American society by nominating Muslim sympathizers to political office and law enforcement ranks to then gain access to computer databases.[85]

Several incidents show that analysts are prone to religious prejudice and confusing political rhetoric (particularly anti-government views) with terrorist threats:

- In February 2009, North Central Texas Fusion System issued a "Prevention Awareness Bulletin" that called on law enforcement to report the activities of

CAMERA: Santa Monica police requested $2 million to install pre-emptive measures such as surveillance cameras, additional patrols, and bomb-sniffing dogs to beef up security at its famed pier. The request followed the seizure of a video of the pier taken by three Middle Eastern male tourists. Police characterized the act as "probing" for a terror attack because the tourists themselves were not in the shots. No arrests were made.

Source: iStockphoto

Muslim civil rights organizations and antiwar groups.[86]

- In March 2009, the Missouri State Highway Patrol was forced to halt distribution of a report prepared by the Missouri Information Analysis Center that linked militants in the modern militia movement to supporters of third-party presidential candidates such as Congressman Ron Paul of Texas and former Congressman Bob Barr of Iowa.[87]
- The Virginia Fusion Center's 2009 Threat Assessment identified "subversive thought" as a marker for violent terrorism and claimed that university based student groups were a "radicalization node for almost every type of extremist group."[88]
- In March 2008, DHS produced a "terrorism watchlist" about a Muslim conference in Georgia, even though it "did not have any evidence the conference or the speakers promoted radical extremism or terrorist activity," and such speech is constitutionally protected.[89]
- In another case where DHS affiliates unlawfully collected information about American citizens or lawful U.S. residents, analysts wrote and disseminated a report on the Nation of Islam based on eight months of surveillance in 2007 when the leader of the group, Louis Farrakhan, was in poor health and appeared to be yielding power.[90]

Although the DHS retracted and took remedial action due to some of these reports, these incidents illustrate law enforcement's tendency to use counter-terrorism intelligence systems for illegal purposes.

Intelligence-led policing provides ideological and philosophical support to the SAR Initiative's approach of casting a wide surveillance net. In the words of Sam Rohrer, a Republican member of the Pennsylvania House of Representatives, "The danger with the Intelligence-led policing view is that, without the protection of a proper balance, the basic right of the presumption of innocence is destroyed, and with it our freedom."[91]

The SAR Initiative Lowers the Quality of Information and Increases False Positives – Undermining Both Security and Civil Liberties

Enlisting police as intelligence officers to report instances of broadly-defined suspicious conduct will lead to more reports, but not necessarily better intelligence. The SAR Initiative seems to improve the volume of information moving through the system, but pays less attention to the quality of what is being shared. Over-collecting and over-reporting innocuous information does not improve national security; it undermines it.

According to a RAND Corporation report, there are concerns about current efforts "simply collecting so much data that are of such low quality that they do not provide much [counterterror] benefit," particularly with regard to SAR Reports.[92] In the financial sector, even before September 11, 2001, there were concerns that the "volume of suspicious activities reports was interfering with effective law enforcement."[93] An NCTC official observed in the press, "In many instances the threshold for reporting is low, which makes it extremely difficult to evaluate some of this information."[94] NSA monitoring of communications to U.S. citizens led that agency each month to pass thousands of vague tips to the FBI that produced very few leads.[95]

Efforts focused on identifying a few threatening actors against a background of many innocent ones will "invariably generate false positives — individuals or organizations incorrectly flagged as potential threats," points out Brian Jackson in a 2009 RAND report.[96] Intrusions into private lives in a broad search for terrorists raises valid concerns about the misuse and abuse of such data, about its accuracy, and about "the possibility that the government could, through its collection and analysis of data, inappropriately influence individual conduct," cautions the nonpartisan National Research Council.[97]

The network's diverse, decentralized structure may exacerbate these problems. According to RAND,

> "if the central focus is on information-sharing among those organizations, these spurious hits will travel to many separate intelligence organizations, both increasing the chances that the false identification will result in costs imposed on the individual and creating burdens and potentially wasted effort for multiple organizations."[98]

In one case, a false entry in the Terrorism Screening Database led to the same person being incorrectly detained 21 times in a single year.[99] The system of dispersed authority and responsibility also makes it harder to standardize practices to maintain accurate information. In the words of Bruce Fein, once a staffer to former Republican Congressman Bob Barr of Georgia:

> Since anything might be a clue as to a possible psychological inclination to commit terrorism, everything is fair game for intelligence collection. But when everything is relevant, nothing is relevant. Finding something useful in the mass of undifferentiated intelligence reports and analysis is thus akin to looking for a needle in a haystack. That may explain why there is no credible evidence that Fusion Centers have frustrated a single terrorist plot – their primary *raison d'être*.[100]

The SAR Initiative is a Platform for Prejudice

The effects of the SAR Initiative will likely be as troubling as the core assumptions and policing philosophies at its foundation. The SAR Initiative creates a platform through which prejudices and social biases can be amplified and ultimately acted upon.

Since the era of slavery, racial and ethnic minorities have disproportionately been victimized by false arrest, verbal abuse, harassment, and unjustified police violence, in the United States. Several studies have linked higher arrest rates for Blacks and Latinos to an officer's personal biased attitudes and perceptions – a conclusion supported by other research that has documented police prejudice and suspicion based on skin color.[101] Since 2006, the New York City Police Department has stopped 500,000 pedestrians each year for suspected criminal involvement. Raw statistics for these encounters suggest large racial disparities – 89 percent of the stops involved nonwhites, according to data compiled by the RAND Corporation.[102] Further, 90 percent of those stops did not lead to an arrest, even though police collected personal information.

PRAYER: FBI agents hunting for information about worshippers can now go into mosques and churches without identifying themselves.
Image Source: iStockphoto

A 1998 U.S. Department of Justice investigation of the New Jersey State Police generated public consciousness of racial profiling as the practice of singling out members of racial or ethnic groups for relatively minor traffic or petty criminal offenses in order to question or search them for drugs or guns. The phenomenon of racial profiling is so pervasive that the phrase, "driving while black or brown" has entered the national lexicon. Today, more than twenty states have passed laws prohibiting racial profiling and/or mandating data collection on stops and searches to screen for systemic bias.

The fact that the Los Angeles Police Department created the prototype for the nationwide SAR Initiative will inevitably raise suspicions of bias in the program. The LAPD has become notorious for use of excessive force and aggressive behavior in Black and Latino communities. In the late 1990s, the actions of the LAPD Rampart Division generated one of the largest scandals involving documented police misconduct, including convictions of police officers for unprovoked shootings and beatings, planting of evidence, framing suspects, perjury, and subsequent cover-ups.[103]

In light of preexisting systemic racial bias in policing practices, it is not unreasonable to expect that when filing, following up on, or sharing Suspicious Activity Reports, some police will consciously or otherwise employ racial, ethnic, and/or religious stereotypes. As a result, Suspicious Activity Reporting may magnify existing or introduce new patterns of racial and ethnic profiling. In fact, "driving while Muslim" is already a phenomenon identified by civil rights advocates working with Arab, Middle Eastern, and South Asian communities.

The interconnectedness of the new domestic security infrastructure will ensure that potentially biased tips can travel from a neighborhood police substation through Fusion Centers and into nationwide info-spheres. The initial indignity and harm of police misconduct may linger and reverberate due to the fact that one's personal information may be stored and shared with powerful intelligence agencies.

THE SAR INITIATIVE INVITES RACIAL, ETHNIC, AND RELIGIOUS PROFILING

According to Heather J. Davies and Gerard R. Murphy in *Protecting Your Community from Terrorism:*

> Within hours of the Twin Towers' collapse and the attack on the Pentagon, U.S. residents and visitors, particularly Arabs, Muslims, and Sikhs, were harassed or attacked because they shared – or were perceived to share – the terrorists' national background or religion. . . . Law enforcement's challenge since then has been to maintain an appropriate balance between the security interests of our country and the constitutional rights of every American.[104]

The SAR Initiative's information-sharing system creates new opportunities to magnify and multiply racialized fears about terrorism. Although ISE officials have developed guidelines meant to focus on individuals' behavior rather than their national origin or racial or ethnic characteristics, a race- or nationality-neutral process is impossible when local police operate in an atmosphere that constantly validates prejudice against individuals commonly thought to resemble the September 11 attackers.

The attempted Christmas Day 2009 "underwear" bombing of NWA Flight 253 unleashed renewed bigoted demands for racial profiling, despite the fact that it has been long-discredited as a law enforcement counter-terror technique.[105] Broad profiles based on individuals' national origin, race, or religion are neither legitimate nor effective in combating terrorism.[106]

In the June 2003 *Guidance Regarding the Use of Race by Federal Law Enforcement Agencies*, the Department of Justice acknowledges that "racial profiling at its core concerns the invidious use of race or ethnicity as a criterion on conducting stops, searches and other law enforcement investigative procedures."[107]

Apart from other serious problems, using apparent race, ethnicity, religion, or other simple identity criteria to identify individuals as threats creates an enormous pool of "suspects" and diverts attention away from potential threats that do not fit crude stereotypes. The SAR Initiative can potentially compound instances of racial and ethnic bias by disseminating reports nationwide. Further, its broad definition for "suspicious activity" and emphasis on lawful "pre-crime" activity creates confusion among police and opens the door for subjective stereotypes to enter police decision-making.

Since September 11, 2001, the U.S. government has mobilized law enforcement personnel into a domestic security apparatus that has targeted people solely on the basis of nationality and citizenship status through methods ranging from increased interrogations to detentions. The "special registration" program enacted by the Bush administration, called the National Security Entry-Exit Registration System (NSEERS), resulted in the "preventative detention" of about 5,000 men on the basis of their birthplace and later sought 19,000 additional people for "voluntary interviews." More than 170,000 men from 24 predominantly Muslim countries and North Korea were fingerprinted and interviewed; 83,000 individuals are still registered within the NSEERS database.[108]

Yet none of these contacts produced a single terrorism conviction. According to Juliett Kayyem and Philip Heymann, these unproductive tactics "caused serious harm within communities in the United States as well as with foreign governments, who viewed the response as draconian and unwieldy."[109]

The SAR Initiative operates in a context that includes intense surveillance of Muslim communities, as well as Arab Americans, South Asians, and Middle Easterners. Since the September 11 attacks, FBI Joint Terrorism Task Force investigators have interviewed more than 15,000 persons "of interest" in connection with alleged terrorist activity.[110] Furthermore, FBI agents hunting for information about worshippers are now authorized to go into mosques and churches without identifying themselves.[111] As a result of such government initiatives, a Justice Department-financed study found that since September 11, Arab Americans have a greater fear of racial profiling and immigration enforcement than of falling victim to hate crimes.[112]

In the current political climate, police are under pressure to treat citizen Suspicious Activity Reports seriously, even when available facts do not indicate an iota of criminal activity. The increased involvement of insufficiently trained local and state law enforcement officials in national security and counter-terrorism activities will likely increase misconduct based on ignorance-based and prejudice-based profiling.

But even before the national SAR Initiative took shape, hunting for vaguely defined "suspicious activities" appeared to be an invitation to conduct racial profiling. Here are two examples:

- On July 3, 2005, a man observed (and photographed) three Middle Eastern men videotaping the popular pier at Santa Monica beach. Several weeks later police seized the video, which they characterized as "probing" for a terror attack because the tourists themselves were not in the shots. Police consulted with the FBI, the Los Angeles Terrorism Early Warning Group (precursor to today's JRIC Fusion Center) and the state Department of Homeland Security. As a result, Santa Monica police requested $2 million to install pre-emptive measures such as surveillance cameras, additional patrols, and bomb-sniffing dogs to beef up security at the pier. No arrests were made.[113]
- In February 2008, men of Middle Eastern origin prompted concern at St. Pius X Catholic Church in Rock Island, Illinois for taking photos inside the church and of its exterior; they were later identified as a resident new to the area and his friends.[114]

Racial profiling not only harms the targeted individual, but the taxpayers who foot the bill for expensive and intrusive surveillance measures.

Examples of Racial, Ethnic, and Religious Profiling from 2004-2005 Homeland Security Operations Morning Briefs

The SAR Initiative relies on multiple layers of vetting to weed out incidents that do not "reasonably indicate" a connection with criminal or terrorist activity. Due to the secretive treatment of most SAR Reports, it is difficult to discern how much reporting is based on racial, ethnic, or religious characteristics. However, a series of Homeland Security Operations Morning Briefs from 2004-2005 provide possible clues. These briefs are daily compilations of articles, operational reports, and intelligence briefings from partner agencies such as the FBI and Central Intelligence Agency. Even though presumably they were vetted by experts before landing on the DHS Secretary's desk, several of the following Morning Briefs describe conduct where the only "suspicious" factor appeared to be a subject's Middle Eastern appearance.[115]

MASSACHUSETTS: Possible Video Surveillance of Interstate Highway. According to military reporting, on 22 September, in Lexington, a military member reported observing four Middle Eastern individuals standing on an I-95 overpass videotaping the northbound traffic and recording information into a notebook. Reportedly, the same military member recalled observing two of the individuals on the same overpass in late February or early March 2004.[116]

MAINE: Suspicious Persons in Southwest Harbor. According to 23 September U.S. Coast Guard reporting, a concerned citizen reported suspicious behavior by three men of possible Middle Eastern descent at a convenience store located in Southwest Harbor. The men were asking if any local businesses rented power boats, kayaks, or bikes. The men were driving a maroon-colored van with Florida license plates. The reporting citizen stated that although he initially thought the men's behavior was suspicious, he did not think to report it, until he learned that the Queen Mary II would be making a port visit to Bar Harbor on 27 September. An investigation is ongoing.[117]

WASHINGTON: Suspicious Activity of Two Middle Eastern Males on Ferry. According to USCG reporting, on 27 September, in Seattle, two Middle Eastern males were observed studying the schematic of the Wenatchee Ferry for an extended period of time. As soon as the two males noticed an employee approaching, they immediately walked away from the schematic and picked up a magazine to ward off attention...[118]

ILLINOIS: Possible Surveillance Activity. According to the Illinois State Terrorism Intelligence Center (STIC), on 22 October, in Joilet, at a worksite at the McDonough Street Bridge, a construction foreman observed a male of possible Middle Eastern origin taking photographs of the bridge...[119]

DISTRICT OF COLUMBIA: Suspicious Videotaping. According to U.S. Secret Service reporting, on 18 November, [name and date of birth redacted by PRA] was observed videotaping near the White House. Reportedly, [subject] was in the D.C. to attend a demonstration in protest of Iran.[120]

NEW YORK / DISTRICT OF COLUMBIA: Concerned Citizen Reports Middle Eastern Male Behaving Suspiciously on Train. According to a concerned citizen call-in to the Homeland Security Operations Center, on 19 December, the concerned citizen witnessed a possible Middle Eastern male behaving suspiciously on an Amtrak train. During a trip from New York Penn Station to Washington, D.C. Union Station, the concerned citizen reported that the possible Middle Eastern male switched back and forth between English and Farsi while talking on two different cell phones for three hours (the whole length of the trip)...[121]

NEW JERSEY: Concerned Citizen Describes Middle Eastern Male Store Owner's Behavior as Suspicious. … [A] concerned citizen… reported that a Middle Eastern male store owner behaved suspiciously. The concerned citizen made four trips to an ink cartridge replacement store near his home anticipating the store's grand opening, and on the fourth trip, 17 December, he engaged the owner, a Middle Eastern male, in friendly conversation. During the course of the conversation, the store owner reportedly stated that he used to work for "Osama Bin Laden." The concerned citizen stated that he could not determine if the man was joking or not...[122]

In the racially charged atmosphere surrounding terrorism, the SAR Initiative will inevitably increase profiling and discriminatory investigatory practices based on race, nationality, national origin, ethnicity, and religion. These practices will ultimately undermine national security by dividing communities and eroding trust in American institutions. "What these guys have done is create an environment where every person begins to suspect the other and with the infighting and inward suspicion, the community becomes its own victim," explains Shakeel Syed, executive director of the Islamic Shura Council in Southern California. Unjust persecution of select groups also gives ammunition to foreign political movements wanting to exploit the perception that America is hostile to Islam and people from Middle Eastern, South Asian, and Arab lands.

Inadequate Protections against Racial, Ethnic, and Religious Profiling

The SAR Initiative's record in confronting the problem of racial and ethnic profiling is mixed. On the one hand, the latest federal Functional Standard, Version 1.5, relegates profiling to a single footnote. In addition, guidelines for gathering, processing, analysis and review of SAR Reports contain no admonitions against racial, religious, or ethnic profiling.[123]

On the other hand, officials at the forefront of the SAR Initiative publicly acknowledge the dangers of profiling. ISE officials have told Congress that training for frontline personnel, senior and expert officers, investigators and analysts should emphasize that Suspicious Activity Reporting is based on clearly defined behaviors and not individual characteristics like race, culture, religion, or political associations.[124] Authors of some guidelines appear to take the challenge seriously. For example, the initial civil liberties analysis for the SAR Evaluation Environment stresses:

> The determination to document a suspicious incident as an ISE-SAR cannot be based solely on a subject's race, ethnicity, national origin, religious preferences or the exercise of First Amendment or other constitutional rights. In addition, for federal agencies, the Privacy Act of 1974 prohibits the collection and maintenance of information in these categories except to the extent that the information is pertinent to and within the scope of an authorized law enforcement activity.[125]

ISE's Program Manager also recommends that local agencies implement internal checks to ensure against profiling based on race, ethnicity, national origin, or religion.[126] To that end, DOJ's *Privacy and Civil Liberties Policy Development Guide and Implementation Templates* recommends that local policies clearly identify what information may not be sought, retained, shared, or disclosed by the agencies: information about individuals or organizations based solely on their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.[127]

In the racially charged atmosphere surrounding terrorism, the SAR Initiative will inevitably increase profiling and discriminatory investigatory practices based on race, nationality, national origin, ethnicity, and religion.

Notwithstanding these official policies, biases in input and analysis will likely lead to an over-representation of South Asian, Middle Eastern, Arab, and Muslim populations in SAR data. Thus far, the strongest check against such practices has been public outrage. In Los Angeles, police planned to map Muslim communities based on U.S. census data in 2007 to identify "potential hotbeds of extremism." Chief Bratton called it an effort to "understand communities" rather than targeting or profiling.[128] LAPD scrapped the plan after a wave of community pressure, but other agencies may try the same thing.

THE SAR INITIATIVE GIVES LICENSE TO TARGET LEGAL DISSIDENT ACTIVITY

The SAR process provides an opening for local intelligence units to shift from legitimate counter-terrorism investigation (and following leads gained from tested information sources) to broad surveillance and open-ended political fishing expeditions. Intelligence sharing between local police, sheriff's departments, the federal government, and the private sector is now being codified, mandated, and encouraged, making it far more likely for innocent people to be swept up in the anti-terror dragnet.

Conservative political figures such as Sen. Joseph Lieberman (Independent-CT) and Homeland Security leaders like Janet Napolitano and Robert Mueller have sounded alarms about the rise of "homegrown extremism" that can fuel unfair assumptions or scrutiny of people who are simply exercising their free speech rights.

The SAR Initiative undermines key privacy and civil liberties protections by lowering the standard for storing and sharing intelligence information generated by local police forces. When they collect, maintain, and disseminate criminal intelligence information, all law enforcement agencies receiving federal funding must follow the standards and civil liberty safeguards set forth by a federal regulation, ***28 CFR 23***. This regulation creates standards aimed at ensuring that intelligence gathering and dissemination systems are not used to violate privacy and Constitutional rights.

In the view of former DHS Secretary Michael Chertoff, the domestic security apparatus is geared toward developing intelligence from "thousands and thousands of routine, everyday observations and activities and interactions – each of which may be taken in isolation as not a particularly meaningful piece of information, but when fused together, give us a sense of the patterns and flow that really is at the core of what intelligence is all about."[129] The SAR Initiative makes mass surveillance a reality by broadly defining suspicious activity to include actions that *could lead* to terrorism at some future point. This pre-emptive approach will inevitably lead to government harassment, tracking and even detention of innocent people. In fact, it already has.

The SAR Initiative Collects Information on Lawful Activity

The SAR Initiative has trained thousands of local, regional, and state law enforcement officers to look out for and report legal activity that could signal pre-operational surveillance by terrorists. Fred Burton, a terrorism expert who orchestrated the arrest of 1993 World Trade Center bombing mastermind Ramzi Yousef, says:

> Your average street cop has the ability to just do more intelligence collection through interfacing with their area of responsibility . . . Most pre-operational surveillance – such as taking a picture or shooting scenic video – is innocent-looking in nature and generally doesn't break the law. The problem isn't the legality of the activity, it's that virtually no one is taking note that it's even happening. Fewer still write it up in an intelligence report to the local JTTF for further investigation.[130]

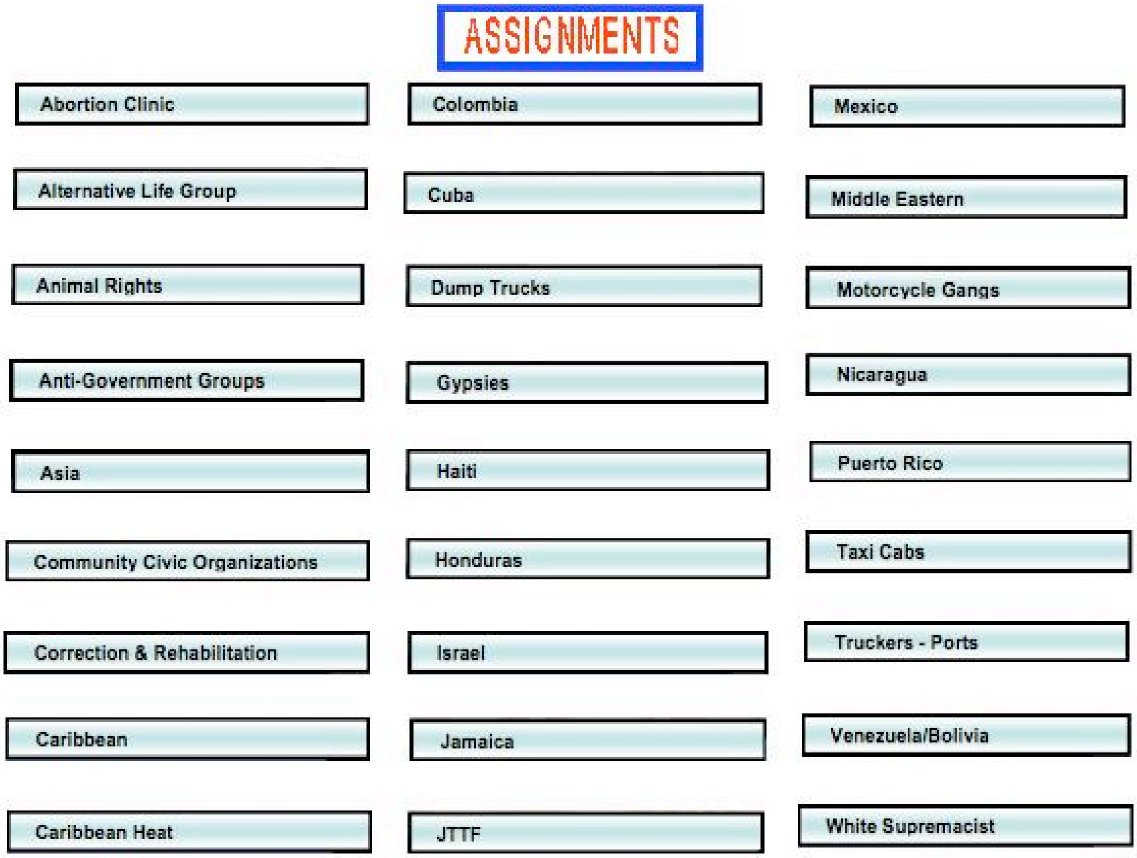
Focusing on activities such as theft, site breach, cyber attacks, or acquisition of unusual quantities of toxic materials does not unreasonably jeopardize civil liberties.[131] But in order to cast a larger, wider net of surveillance, ISE officials stray far from these legitimate investigatory areas. Through the SAR Initiative, they encourage corporations, local police, and the public to report activities of a *non-criminal* nature, defining "pre-operational surveillance" in such broad terms that it includes activities that are far more likely to be carried out by law-abiding persons than by terrorists.

In January 2008, the Director of National Intelligence issued standards for state and local police to report suspicious activities to Fusion Centers that included:

- Taking pictures / video of facility / infrastructure / personnel or surrounding environment.
- Showing unusual interest in facility / infrastructure / personnel; for example, observing it through binoculars, taking notes, drawing maps, or drawing structures of the facility.
- Monitoring the activity of people, facilities, processes, or systems.[132]

Similarly, Washington D.C., Los Angeles, and Miami-Dade SAR policies mandate reporting on innocuous, non-criminal, and First Amendment-protected activities, such as: taking measurements, using binoculars, taking pictures or video "with no apparent aesthetic value," drawing diagrams and taking notes, or espousing extremist views.[133] In Miami, sign of surveillance for terrorist target selection. However, they claim that suspicion is warranted when photographers do not let law enforcement view pictures, or have "no people in pictures when the photographer claims to be a tourist," or when pictures are taken at "odd times."[134]

LAPD commander Joan McNamara asserts that the SAR Initiative should be "built upon behaviors and activities that have been historically linked to pre-operational planning and preparation for terrorist attacks."[135] Never mind the fact that any savvy would-be terrorist can discreetly video or photograph scenes with most cell phones, or can legally download from



ASSIGNMENTS

Abortion Clinic
Alternative Life Group
Animal Rights
Anti-Government Groups
Asia
Community Civic Organizations
Correction & Rehabilitation
Caribbean
Caribbean Heat

Colombia
Cuba
Dump Trucks
Gypsies
Haiti
Honduras
Israel
Jamaica
JTTF

Mexico
Middle Eastern
Motorcycle Gangs
Nicaragua
Puerto Rico
Taxi Cabs
Truckers - Ports
Venezuela/Bolivia
White Supremacist

MIAMI DADE: Assignments at the Homeland Security Bureau for the Miami-Dade Police Department are often grouped around political orientation and immigrant-group identity.

Source: Prepared testimony of Major Michael R. Ronczkowski, Miami-Dade Police Department Homeland Security Bureau, before the Committee on Homeland Security and Governmental Affairs, U.S. Senate. October 30, 2007.

Image Source: Prepared statement of testimony by Major Michael R. Ronczkowski, Miami-Dade Police Department, Homeland Security Bureau, before the Committee on Homeland Security and Governmental Affairs, United States Senate. October 30, 2007.

the Internet photographs, videos, designs, aerial photography (via Google Maps) and even live street views of many popular stadiums, public facilities, bridges, airports, and tourist attractions. Nonetheless, police have harassed many people for openly (and quite legally) photographing trains, buildings, and bridges:

- An amateur photographer was questioned by an undercover police officer when he was taking a picture of New York City's Verrazano Narrows Bridge. The officer explained that bridges could not be photographed up close, but postcard-type shots from afar are allowed. While the photographer was not harassed, the officer did explain that protocol was that he should be detained and questioned. These drastic measures were encouraged even when there were no signs warning passers-by such policies.[136]
- Amtrak's monthly newsletter stated that photography was allowed in public areas. Photography of train stations was also encouraged by Amtrak's Annual Photo Contest. Duane Kerzic, however, discovered a drastically different treatment of photographers when he was arrested in 2008 while standing on a public platform at New York's Penn Station. Ironically, he was taking photos to submit in the following year's contest.[137]
- In September 2007, a 24-year-old Muslim-American journalism student at Syracuse University was taking photographs of flags in front of a New York City Veterans Affairs building as part of a class assignment when she was detained by a V.A. police officer. After being taken to an office and questioned, her pictures were deleted from her camera and she was released.[138]
- In October 2005, a 55-year-old artist and fine arts professor at the University of Washington was stopped by Washington State police as he was photographing electrical power lines as part of an art project. Following being searched and handcuffed, the professor was forced to sit in the back of a police cruiser for about 30 minutes before ultimately being released.[139]
- Arun Wiita, a Columbia University grad student attempting to photograph all of New York City's subway stations, was stopped by police after he had photographed five stations. Wiita was handcuffed and detained while the officer checked his background and reviewed his digital pictures, and ultimately the young man was released without charges.[140]
- In February 2003, Jack and Susan Wright were interrogated by a Massachusetts state police trooper while watching ducks with binoculars at Barton's Cove after someone reported a suspicious person walking with khaki shorts and a dark hooded sweatshirt. They were stopped by police two other times that same year for bird watching.[141]

In each of the above cases, police-generated data can reside in police intelligence unit or Fusion Center databases for up to five years, even if a review finds no nexus to terrorism.[142]

In response to criticism from civil liberties advocates, the Director of National Intelligence (DNI) revamped standards in May 2009. It is difficult to gauge the effect of the new criteria. When we asked Agent Jennifer Cook-Pritt, who heads the Florida Fusion Center, if she was aware of the change, she replied that there was "no major change in the functional definition" of Suspicious Activity Reporting in the May revision.[143] Indeed, the latest criteria still include "potential criminal or non-criminal activity requiring additional fact information during investigation."[144] A footnote explains that "these activities are generally First Amendment-protected activities and should not be reported in a SAR [Report] or ISE-SAR [Report] absent articulable facts and circumstances that support the agency's suspicion that the behavior observed is not innocent."[145] Taking pictures or video of facilities is still listed; We are unaware of any agency that has narrowed SAR criteria since April 2009.

The DNI's revised standards will be nothing more than window dressing unless leading agencies in the ISE abandon targeting non-criminal activity as a goal. Regardless of what the SAR Initiative's "functional standards" may say, existing federal law only permits intelligence systems to track and record criminal activity that constitutes a significant, recognized threat to people or property. (*28 CFR 23* defines such activity as organized criminal activity or activity that is undertaken to seek illegal power or profits.) [146]

The SAR Initiative Emboldens Illegal Surveillance of Free Speech and Political Participation

The SAR Initiative jeopardizes free speech by reconstituting urban intelligence units that have historically abused their investigative authorities for political purposes. Suspicious activity criteria issued by several agencies directly identify certain forms of political speech as potentially indicative of terrorism.

Explains civil rights attorney Frank Donner, during the Cold War, local intelligence operations "replenish[ed] the supply of subversives from the ranks of dissidents" and "discredit[ed] the predictable movements of protest against the threat of war, nuclear weaponry, environmental contamination, and economic injustice."[147] Today, application of the "terrorist" label to political dissidents is a powerful tool to thwart legitimate, grassroots citizen opposition to U.S. foreign or domestic policy. The SAR Initiative gives governmental agencies a powerful tool to intimidate, monitor, spy on or otherwise harm the rights and privacy of political activists of any stripe.

Due to the secrecy shrouding all domestic intelligence programs, including the SAR Initiative, there is currently no way to verify if SAR Reports are being used for political purposes. Nevertheless, the Initiative's practices justify heightened concern about threats to our democracy.

The SAR Initiative emphasizes the role of street officers as intelligence collectors. Officers are encouraged to record observations of legal activity, including constitutionally protected political speech.[148] The Washington, D.C. Metropolitan Police's SAR policy collects data about the following kinds of conduct:

- Person(s) espousing extremist views (e.g., verbalizing support of terrorism, inciting or recruiting others to engage in terrorist activity, etc.) (SAR Code 2126);
- Person(s) bragging about affiliation or membership with an extremist organization (SAR Code 2127); and
- Person(s) displaying overt support of known terrorist networks (e.g., by maintaining posters of terrorist leaders, etc.) (SAR Code 2129).[149]

BINOCULARS: First Amendment-protected activities, such as taking measurements, using binoculars, or taking pictures or video "with no apparent aesthetic value," can constitute as suspicious activities.

Image Source: iStockphoto

Likewise, LAPD orders officers to document situations where an individual or group:

- Espouses extremist views (Code 2126);
- Brags about affiliation with extremist organizations such as “white power,” militias, Ku Klux Klan, etc. (Code 2127);
- Affiliates with an organization that supports overthrow of government or violence.
- Associates with organizations involved with supporting, advocating, or implementing violent acts or the overthrow of the United States government (Code 2173).[150]

The above-referenced SAR codes could apply to a wide range of activist organizations. None of them define the term “extremism” or explicitly require an immediate threat of criminal conduct to trigger reporting.

During the analysis stage, investigators identify and track those who share the assumed politics or religious motives of groups the FBI has designated as possible terrorist threats (including such amorphous groupings as “anarchists” and “anti-abortion extremists.”[151]) An expert on Intelligence-Led Policing describes four broad questions addressed by intelligence analysis.

- Who poses threats? [This response identifies and describes behaviors of people in movements or ideologies who pose criminal threats to community safety.]
- Who is doing what with whom? [This includes the identities, descriptions, and characteristics of conspirators or people who provide logistics in support of terrorism and criminal enterprises.]
- What is the modus operandi of the threat? [Intelligence analysis seeks to identify how criminal enterprises operate. It also seeks to determine what criminal, terrorist, or extremist groups typically target and the common methods of attacking the targets.]
- What is needed to catch offenders and prevent crime incidents or trends? [Intelligence requirements seek specific types of information that are needed to fully understand the threat environment.][152]

These broad questions underscore how the “situational awareness” sought by intelligence analysts legitimizes government spying on people who have done nothing criminal, but supposedly share the worldview of suspected terrorists.

Even if SAR Reports do not enter nationwide databases, the originating law enforcement agency can retain its reports for up to five years (or longer if a review determines that the information is still actionable). Civil rights attorney Frank Donner argues that the initial step of identifying “potential threats” paves the way for the future adverse treatment of political dissidents.[153]

The history of domestic intelligence collection is a minefield of prejudicial practices, many of which constitute civil rights violations. During the last major expansion of domestic-surveillance-as-policing, from 1956 to 1971, so many civil rights lawsuits were filed against local law enforcement agencies for maintaining intelligence files on American citizens that many opted to close their intelligence units.

The seeds for a repeat of similar abuses are evident in the policies of the SAR Initiative, which dismantles important features of the civil liberties safeguards enacted by Congress in the 1970s in response to COINTELPRO, the FBI’s covert and illegal counterintelligence program.

COINTELPRO’s stated goal was to “expose, disrupt, misdirect, discredit, or otherwise neutralize” individuals and organizations the Bureau characterized as national security threats, a clear mandate for local police intelligence units to help the FBI monitor and thwart legal political activities. Congress documented extensive cooperation between the FBI and police in cities like Oakland, Los Angeles, Chicago, and San Diego in executing COINTELPRO. Massive dossiers were compiled on targets like the Black Panther Party, Southern Christian Leadership Conference, Student Nonviolent Coordinating Committee, Nation of Islam, and the National Organization for Women. The FBI directed local police to deploy informants and agents provocateurs who, in some cases, promoted violence. Activists' homes and offices were raided with little or no legal basis. FBI neutralization and disruption activities led to violent suppression of African American civil rights organizations, as well as the creation of militarized urban police units that encouraged armed confrontation with dissidents.[154]

Under the SAR Initiative, there is much greater potential for the fruits of political spying to be shared nationwide. Intelligence sharing between local police, sheriff's departments, and the federal government is now not only encouraged, it is being codified and mandated, making it far more likely for political activists to be swept up in the anti-terror dragnet, spied on, tracked and harassed.

Law enforcement and intelligence agencies have recently activated and intensified surveillance of political dissidents as part of a "preemptive" strategy to subvert, chill, or disrupt political protest at major national and international events such as the 2004 and 2008 Republican and Democratic National Conventions, the 2009 G-20 summit in Pittsburgh, presidential inaugurations, and Miami's 2003 FTAA summit. Before such events, and using Fusion Centers as a hub, local intelligence units work with federal agencies to monitor a wide swath of advocacy and direct action organizations.[155] For example, in 2008 the Ramsey County Sheriff's Department deployed undercover agents to infiltrate social justice groups planning protests at the Republican National Convention in St. Paul, Minnesota.[156] Prior to the 2004 RNC Convention, NYPD police detectives infiltrated and reported on peaceful activist groups as far away as Kansas City.[157]

On numerous occasions, animal rights rallies, environmental demonstrations, anti-war protests, student protests against military recruiting on campus, labor union organizing, and demonstrations against police brutality have all found their way into the databases of the California Anti-Terrorism Center and the Los Angeles County Terrorism Early Warning Center (LACTEW), which pre-dates the region's Fusion Center, known as the Joint Regional Intelligence Center (JRIC).

In 2008, the public learned that a Maryland State Police trooper had covertly infiltrated peaceful anti-war, prisoner rights, environmental, death penalty, and Quaker organizations in the Baltimore area. Police officials tried to assure the public that files labeling activists "terrorist" and "extremist" resided on a standalone computer isolated from other networks, in spite of evidence that correspondence from DHS regarding activists was found in Maryland police files.[158]

In 2009, officials from ISE, the departments of Homeland Security and Justice, and the Office of the Director of National Intelligence met with the Muslim Political Affairs Council, ACLU, and other organizations concerned about the SAR Initiative's facilitation of spying for domestic political purposes. The officials clarified that First Amendment-protected activities require additional documentation in order to be written up as SAR Reports.

The SAR Initiative gives governmental agencies a powerful tool to intimidate, monitor, spy on, or otherwise harm the rights and privacy of political activists of any stripe.

However, language in the Los Angeles and Washington, D.C. SAR policies reveals that at least some local agencies have not changed their practices in response to the new federal guidance. In fact, suspicious activity guidelines in Los Angeles and Washington, D.C. expressly draw officers' attention toward the content of speech, rather than criminal conduct.

Any guidelines targeting the content of speech clearly risk chilling free speech rights. In the words of a 1989 Senate Select Committee that examined 1980s-era government spying on the Committee In Solidarity with the People of El Salvador, "unjustified investigations of political expression and dissent can have a debilitating effect upon our political system. When people see that this can happen, they become wary of associating with groups that disagree with the government and more wary of what they say and write. The impact is to undermine the effectiveness of popular self-government."[159]

The SAR Initiative Erodes and Evades Time-Tested Civil Liberties Rules for Information Collection

The SAR Initiative's platform for prejudice rests on a fundamental weakening of key privacy and civil liberties protections. By lowering the standard for storing and sharing intelligence information generated by local police forces, the SAR initiative debases a key tenet of post-1960s intelligence reforms the requirement of a criminal predicate.

Requiring a criminal predicate for government investigations helps protect citizens from being targeted based on dissent, religion, or ethnicity, and helps to ensure that surveillance and intelligence are not used for political purposes.[160] In 2005, the National Criminal Information Sharing Plan endorsed the criminal predicate requirement for the entire ISE. Yet, inexplicably, new guidelines released by ISE officials and local SAR program standards weaken this time-tested bulwark against abuse, thus increasing the risk of civil liberties violations and prejudicial profiling.

As part of a series of law enforcement reforms, the Department of Justice issued new operating policies after Congress revealed widespread civil liberties abuses by the FBI during the 1960s and early 1970s. Local police intelligence units, or "red squads," illegally spied on antiwar and civil rights groups, and helped the FBI carry out its COINTELPRO program.[161] The red squads often abused investigative authorities for political purposes by amassing dossiers on elected officials and engaging in disruptive activities targeting union organizers, civil right advocates, and other dissidents. These domestic spying practices undermined democratic processes and were completely ineffective in meaningfully enhancing national security.

The standards contained in *28 CFR 23* are supposed to ensure that collection, storage and dissemination of criminal intelligence data are not used to violate privacy and constitutional rights. The SAR Initiative undermines and sidesteps the significant safeguards in *28 CFR 23*. The U.S. Department of Justice, Office of Justice Programs highlighted the following:

> According to the Institute for Intergovernmental Research, a nonprofit organization specializing in training law enforcement, "Today's environment of aggressive, proactive information collection and intelligence sharing is very similar to the environment that motivated Congress, in the Justice Systems Improvement Act of 1979, to require the issuance of 28 CFR Part 23 in the first place."[162] Because criminal intelligence …cannot be accessed by criminal suspects to verify that the information is accurate and complete, the protections and limitations set forth in the regulation are necessary to protect the privacy interests of the subjects and potential subjects of a criminal intelligence system.[163]

The Institute further notes, "Nothing is more critical to today's law enforcement agencies than the ability to share information. Yet history shows that to collect and share information without purpose, needs, and controls is counterproductive to law enforcement's mission and diminishes the public's trust."[164]

The National Criminal Intelligence Sharing Plan (NCISP) recommends using *28 CFR 23* regardless of whether or not an intelligence system is Crime Control Act-funded and therefore subject to the regulation.[165] The federal government's Fusion Center Guidelines also call for adopting *28 CFR 23* as the minimum standard. Furthermore, the privacy policies instituted by certain Fusion Centers, such as the Los Angeles JRIC, explicitly state that they apply *28 CFR 23*.

The devil, however, is in the details. In three critical ways, local SAR policies and national SAR standards still expressly contradict and weaken *28 CFR 23*: 1) by downgrading the reasonable suspicion requirement; 2) picking and choosing under what circumstances *28 CFR23* applies to a SAR Report; and, 3) mischaracterizing SAR Reports as "fact based information" rather than criminal intelligence.

Downgrading the Reasonable Suspicion Requirement

"Reasonable suspicion," also referred to as "criminal predicate," has been the minimum threshold necessary for submitting a criminal intelligence record to a database for the past thirty years. Reasonable suspicion is established when a trained law enforcement officer, investigator, or analyst believes there is a reasonable possibility an individual or organization is involved in criminal activity.[166] However, ISE officials have unilaterally adopted the term "reasonable indication" in an apparently deliberate attempt to water down *28 CFR 23*.

By decoupling so-called "suspicious activity" from actual crime, the definition of *reasonably indicative* information has become so broad as to make it virtually meaningless as a guide for law enforcement professionals. This not only makes it easier for reports to be based on prejudicial assumptions or political ideology — it opens the floodgates to a torrent of meaningless data. The Director of National Intelligence (ODNI) now defines a suspicious activity as "observed behavior *reasonably indicative* of pre-operational planning related to terrorism or other criminal activity."[167] A Suspicious Activity Report is "official documentation of observed behavior *reasonably indicative* of pre-operational planning related to terrorism or other criminal activity."[168] An ISE-level SAR Report (or ISE-SAR Report) is a SAR Report that "has been determined, pursuant to a two-part process, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism).[169] By failing to follow the language in *28 CFR 23*, the ODNI has indirectly revived Bush administration efforts to weaken the regulation.[170] Moreover, the ODNI effectively undermines *28 CFR 23* while avoiding the rulemaking process and the attendant public debate it entails.

While preparing the National Criminal Intelligence Sharing plan, the Global Intelligence Working Group (GIWG) recommended revising *28 CFR 23*.[171] Early drafts anticipated that *28 CFR 23*'s "reasonable suspicion" standard would be revised through rulemaking. The GIWG's interim report described an approach developed by the International Association of Chiefs of Police: "It is the policy of this agency to gather information directed toward specific individuals or organizations where there is a *reasonable indication* that said individuals or organization may be planning or engaging in criminal activities."[172] The GIWG report conceded that "The reasonable indication threshold

MILITANT PROTESTS: Even militant protests, when no laws are violated, are protected by the First Amendment.

Image Source: iStockphoto

for collecting criminal intelligence is substantially lower than probable cause. A reasonable indication may exist where there is not yet a current substantive or preparatory crime, but where facts or circumstances reasonably indicate that such a crime will occur in the future."[173] The April 2003 GIWG meeting minutes record approval for the weakening of *28 CFR 23*:

> [GIWG member] Daniel J. Oates indicated he was excited about the proposed changes to 28 CFR Part 23, specifically the area dealing with changing the reasonable suspicion collection criteria to reasonable indication. If the rule is passed, officers on the street can gather small bits of information that can be entered into an intelligence database. Under the old standard, this could not be done.[174]

Picking and Choosing When 28 CFR 23 *Applies*

Rather than seeking to modify or scrap *28 CFR 23* via rulemaking, ISE officials have taken a back door approach to weakening it by limiting its application to SAR Reports. The Concept of Operations for the Nationwide Suspicious Activity Reporting Initiative does not contain a single reference to *28 CFR 23*.[175] Version 1.5 of the SAR Functional Standards refers to *28 CFR 23* only twice. The ISE Fact Sheet on the SAR Functional Standard does not refer to *28 CFR 23* at all. And the term "reasonable suspicion" is absent from the core definition of a SAR, in a clear signal that lower standards apply.

The Program Manager for the ISE has taken a decidedly "hands-off" approach to *28 CFR 23*, leaving states and local agencies to determine when and how to apply it. The ISE Initial Privacy and Civil Liberties Analysis recommends that "agencies should clearly articulate when 28 CFR Part 23 should be applied" to suspicious activities reports. Under the current system, a SAR Report can be stored and shared on Fusion Center platforms even if it does not meet *28 CFR 23* criteria.[176]

SAR Functional Standards provide, "the ISE-SAR information may or may not meet the reasonable suspicion standard for criminal intelligence information. If it does, the information ***may also*** be submitted to a criminal intelligence information database and handled in accordance with 28 CFR Part 23."[177]

An ISE-SAR Report must meet *28 CFR 23* criteria only if an agency wants to pass the information on to a formal criminal intelligence system such as the Regional Information Sharing System (RISS). But it can be uploaded to "Shared Spaces" or stored in local systems even if it doesn't meet this standard.[178] A flow chart produced by the Program Manager for the ISE illustrates how the SAR program empowers JTTFs, local agencies, and Fusion Centers to acquire and keep data that has not yet been classified as "*28 CFR 23* Intel."[179] [See Appendix 5] That diagram also depicts a short-cut, whereby analysts are allowed to submit "terrorism-related" information to the ISE that does not meet 28 CFR 23 criteria.

Moreover, the organization mission of fighting terrorism creates a natural incentive to find reasons for sharing collective information. Once within a system designed to facilitate sharing, it strains credulity to imagine that data will be carefully safeguarded.

Because there is no uniform approach to *28 CFR 23*, agencies handle domestic intelligence inconsistently. After visits to Boston, Los Angeles, Chicago, and Miami, SAR program officials found that:

> …each agency varied in the determination of when or if SARs are passed or made available to an external agency or system such as a JTTF or Fusion Center. More important, each agency described slightly different decision processes that would determine when SAR information actually became intelligence and subsequently subject to 28 CFR Part 23 requirements.[180]

Boston's Fusion Center analyzes potential SAR Reports in-house and determines whether incident data is intelligence-related before exporting it to an "intelligence case management system" for use by the state Fusion Center.[181] By contrast, LAPD officers enter SAR Reports into a Tips and Leads database with a direct interface to the regional Fusion Center, providing multiple agencies with access to SAR Reports before a criminal predicate is established.[182] Under either system, criminal intelligence data is stored locally without *28 CFR 23* requirements having been met.

Mischaracterizing SAR Reports as "Fact Based Information"

Another way the SAR Initiative undermines civil liberties is by categorizing SAR Reports as something less than "criminal intelligence," and therefore entirely outside the reach of *28 CFR 23*. Privacy experts for the ISE deliberately misclassify SAR Reports as "fact-based information," a specific term of art under *28 CFR 23*. ISE program officials assert, "ISE-SAR information is considered fact-based information rather than criminal intelligence and may be subject to the requirements of 28 CFR Part 23."[183]

Under *28 CFR 23*, "fact-based information" refers to agencies' case management databases, records management systems, criminal history records and other non-intelligence databases. Arrest or criminal history information stored in these non-intelligence databases is not based on a reasonable suspicion that a subject is currently engaged in criminal activity.[184] Hence these "fact-based" databases are not required to comply with 28 CFR Part 23.

The following safeguards are embodied in *28 CFR 23* to help prevent a repeat of 1960s era abuses:

1) Information entering the intelligence system must meet a criminal predicate or reasonable suspicion that the individual is involved in criminal conduct and the information is relevant to that criminal conduct;
2) Information entering the system shall not include the political, religious or social views, associations, or activities of any individual or any group unless such information directly relates to criminal conduct or activity;
3) Information entering the system shall be evaluated to check the reliability of the source and validity of the data;
4) Information entering the intelligence system must not violate the reasonable expectations of privacy or civil liberties of its subjects;
5) Information maintained in the intelligence system must be updated or purged every five years;
6) Agencies must keep track of who receives the information; and
7) Information from the intelligence system must be disseminated only to those who have a right to it and need to know in order to perform a law enforcement function.

28 CFR Part 23, "Criminal Intelligence Systems Operating Policies," Executive Order 12291, 1998 Policy Clarification, 1993 Revision and Commentary.

This approach creates an enormous loophole. If SAR and ISE-SAR Reports are fact-based information (rather than criminal intelligence), then Fusion Centers can assert compliance with *28 CFR 23*, while simultaneously amassing data about people and organizations with no connection to criminal activity or enterprises. This approach ignores the fundamental nature of most SAR and ISE-SAR Reports: they are an official claim that the subject of the report is suspected of actual or potential illegal conduct or activity related to terrorism.

A Case Study of the Intelligence Cycle: Los Angeles Joint Regional Intelligence Center (JRIC)

This report examines the SAR Initiative on a national scale with specific analysis of the Los Angeles Fusion Center, called the Joint Regional Intelligence Center (JRIC). This case study is meaningful in part because the Los Angeles Police Department (LAPD) spearheaded the national SAR Initiative with its Special Order No. 11 in 2008. [See Timeline in Appendix 1]

Our investigation in Los Angeles revealed two main issues related to privacy and civil liberty concerns: 1) the accelerated and voluminous collection and retention of personal information that does not meet "nexus to terrorism" criteria; and, 2) law enforcement's unprecedented access to personal information through a myriad of government and commercial databases now available in the electronic digital age. We examine these issues through the four-stage SAR process: gathering intelligence, analysis, sharing, and review.

STAGE 1: GATHERING INTELLIGENCE — CREATING A SAR REPORT

As detailed in Section 2, the SAR process turns street officers into intelligence collectors[185] who are encouraged to vigilantly document all suspicious behavior that could indicate criminal activity associated with terrorism.[186]

In late 2008, an employee at a Los Angeles dry cleaners found a computer thumb drive — a small portable memory storage device—buried in a pile of laundry. He plugged the drive into his computer, discovered detailed photos of the Burbank airport, none with any apparent aesthetic value, and called the police. LAPD's major crimes division created a Suspicious Activity Report, opened an investigation, and interviewed the laundry employee and the owner of the thumb drive. After determining that the airport photos posed no threat, the LAPD closed the investigation.

Elsewhere in Los Angeles, during a traffic stop, a motorcycle officer noticed that the driver was extremely nervous, had trouble answering routine questions, and that his international driver's license had expired. The officer radioed the LAPD major crimes division, then filled out a SAR Report. Further investigation revealed that the vehicle was "of interest" in a burglary. In another area of the city, LAPD vice detectives found illegal gaming machines at a local laundry. They noticed the suspect was extremely nervous and agitated, and they called the SAR unit. The detectives filled out a lengthy SAR form, launched an investigation, and later arrested the suspect.

The LAPD considers these incidents "success stories" of its SAR program, created in April 2008 by LAPD Commander Joan McNamara, co-director (along with Deputy Chief Mike Downing) of the Counter Terrorism and

Criminal Intelligence Bureau (CTCIB). However, these examples also reveal the sweeping "all crimes" scope of LAPD's program, which does not require a suspicious activity to have a nexus to terrorism for it to generate an internal SAR Report.

Since it began in 2008, Los Angeles' SAR program has increased the number of SAR Reports filed. In August 2009, Cmdr. McNamara presented the following figures at the National Forum on Criminal Justice & Public Safety: [see Appendix 4 her excerpt of her Power Point]

- There were 1826 SAR Reports submitted (most by front-line officers) to the LAPD since 2008 and "due diligence is done on each and every SAR," McNamara claimed.
- The SAR program related to 529 investigations and 36 arrests. It is not known how many of the arrests related to terrorism.
- Of the total Suspicious Activity Reports, 126 were referred to the JTTF, which conducted 86 investigations. 149 were investigated by LAPD's Anti-Terrorism section, 67 by LAPD Criminal Investigation section, 230 by LAPD Criminal Conspiracy section, and 5 by the Organized Crime section.
- Of the SAR Reports referred to the FBI's eGuardian system, 66 have shown a "probable" nexus to terrorism.
- LAPD's Bomb Squad received 213 SAR Reports and made 23 arrests.
- Broken down by locale, LAX had 994 SAR Reports; Central L.A. 172; West L.A. 78; Harbor Area 54; West Valley 53. LAX clearly generated the majority of SAR Reports, which is unsurprising given its major international airport status and was once the target of convicted Algerian terrorist Ahmed Ressam, who planned to bomb LAX on New Year's Eve in 2000.

The LAPD has never released information about what happened to the 1,297 SAR Reports that did not trigger investigations. But the high number of reports suggests that the LAPD's "reasonable suspicion" and "all crimes" policy are perhaps being used, in conjunction with immigration enforcement, to justify a more extensive focus on foreigners and foreign-born U.S. citizens. The southern California chapters of the Council on American-Islamic Relations and the Islamic Shura Council have both collected numerous examples of what they consider unwarranted searches and detention.

The Los Angeles County intelligence network relies on three main sources for gathering intelligence: law-enforcement, the general public, and the private sector.

Police as Spies: Reporting by Law Enforcement Officials

LAPD's Special Order No. 11 (revised in March 2008) requires all members of the Department to document "any reported or observed activity, or any criminal act or attempted criminal act, which an officer believes *may* reveal a nexus to foreign or domestic terrorism."[187] Further, the order states: "It is the policy of the LAPD to make every effort to record information, of a criminal <u>or non-criminal nature</u>, that could indicate activity or intentions related to either foreign or domestic terrorism."[188] [See Appendix 5]

The department's expansive "all crimes" interpretation of what constitutes suspicious activity is reinforced by language contained in the latest version of national SAR guidelines. The Office of the Director of National Intelligence describes "suspicious activity" as "observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity."[189]

A confidential law enforcement source told PRA, "The program was rolled out without thinking ahead, and these reports should be connected to homeland security and terrorism, but cops are now trained to look at all suspicious activity."

Activist and former California State Senator Tom Hayden, a critic of the SAR Initiative, calls its vague reporting criteria a "blatant example of mission creep that is overflowing with due process violations." Hayden describes the SAR program as "the LAPD crash unit gone global," citing the expansion of LAPD's Cal-Gang program into an international operation. "If police arrest someone in El Salvador, that information goes into a central database that LAPD has access to. And if someone is deported, that information is fed back to the home country," says Hayden.[190]

Police are also trained to report *any incident* that occurs near critical infrastructure, regardless of whether it is inherently suspicious. For example, the head of an intelligence unit in Florida explained to us that:

> One area for a SAR [Report] is the actual place something happens. For example, activity near the port is worthy of a SAR [Report]. The idea is that if an officer pulls over someone for a routine traffic violation in the area of a port, the officer completes an SAR [Report] – because of the strategic importance of the port – and then the JTTF or the FBI or someone else culls through activity near the port to see if the same guy has been there repeatedly or has bought hazardous material near there, etc. However, a patrol officer who pulls someone over near the port probably is assigned to the port area. That means he would have to fill out extra paperwork on each of his stops, and that is just unlikely to happen.[191]

Consistent with this description of the SAR Initiative policy, LAPD Commander McNamara's August 2009 presentation referred to an oil field map with marks indicating incidents of "vehicles loitering at fence line," "suspicious photography," and "takes photos at fence line."

Under the SAR Reporting process, law enforcement respond to incident reports and then gathers more facts through personal observations, interviews, and other investigative activities. This may require further observation or engaging the subject in conversation. One textbook encourages police to cultivate a wide range of community information sources, including hotels, real estate agents, religious groups, universities, print shops, health care providers, school and office building custodians, licensing and permit agents, refuse haulers, meter readers, and taxi and delivery drivers – many from "countries of interest."[192]

Initial investigation is used to determine whether to dismiss the activity as innocent or escalate to the next step of the process. To gain a more complete picture of the activity being investigated, the officer may access data such as license and vehicle registration records; National Crime Information Center (NCIC) for warrants, criminal history, and access to the Terrorism Screening Center; Violent Gang/Terrorism Organization File (VGOTF); or the Regional Information Sharing System (RISS). Through the NCIC, officers also can access immigrant data, which is entered into NCIC even if it has not been checked for currency and accuracy.[193]

When the initial investigation is complete, the officer documents the event with a Suspicious Activity Report, which becomes the initial record for the local law enforcement records management system. At this stage, the record does not yet constitute an ISE-SAR Report. Even though this report may not evidence reasonable suspicion of criminal activity, the originating agency often shares it with the FBI and the local or state intelligence Fusion Center.

Neighbors as Spies: Public Reporting Through iWATCH

iWATCH, a civilian program launched by the LAPD in October 2009, works in conjunction with the SAR Initiative. "Law enforcement cannot be everywhere and see everything," notes the LAPD's blog, "iWATCH adds another tool to assist an agency's predictive and analytical capability by educating community members about specific behaviors and activities that they should report."[194]

iWATCH was developed under the direction of LAPD Commander McNamara, and can be used in any community anywhere in the United States. Miami and Boston have similar *See Something, Say Something* campaigns. iWATCH lists nine types of suspicious behavior the public should look for, assuring tipsters, "this service is truly anonymous." William Bratton described iWATCH as "the 21st century version of Neighborhood Watch." In an NPR interview, Bratton provided this rationale:

> Any street cop will tell you that crime prevention occurs best at the local level and terrorist-related crime prevention is no different. The problem has always been that individuals have varying thresholds at which they feel compelled to notify authorities when the activity is not overtly terrorist related. The iWATCH program is a giant leap toward overcoming this problem and literally provides millions of new eyes and ears in the terrorism prevention effort.[195]

iWATCH, then, encourages the public to file a report even if people are not convinced that witnessed behavior is criminal. "Let the experts decide," cajoles a Public Service Announcement.[196] In this interview, Former Chief Bratton appeared dismissive of concerns that iWATCH would invite racial profiling, saying, "No, I think we're a more mature society than that."[197] In addition to iWATCH, LAPD's new Chief Charlie Beck and Sheriff Lee Baca launched yet another public tips program in December 2009 called Crime Stoppers, a collaboration of 25 Los Angeles County law enforcement agencies solicit public assistance in solving crimes."[198]

iWATCH encourages the public to file a report even if people are not convinced that witnessed behavior is criminal. "Let the experts decide," warns a Public Service Announcement.

Both iWATCH and Crime Stoppers are disturbingly similar to the controversial TIPS (Terrorist Information and Prevention System), an initiative created by the Bush administration to recruit one million volunteers in 10 cities across the country. TIPS encouraged volunteers to report suspicious activity that might be terrorism-related. TIPS came under intense criticism by various news media outlets in July 2002 for providing the United States with a higher percentage of citizen spies. According to an editorial in the *Washington Post*:

> Americans should not be subjecting themselves to law enforcement scrutiny merely by having cable lines installed, mail delivered or meters read. Police cannot routinely enter people's houses without either permission or a warrant. They should not be using utility workers to conduct surveillance they could not lawfully conduct themselves.[199]

TIPS was officially canceled in 2002 when Congress enacted the Homeland Security Act. However, iWATCH and Crime Stoppers seem to be virtually identical to the failed TIPS program.

Private Sector Feeding Fusion Centers: Infragard

A third source of potential SAR Reports for Fusions Centers like the Los Angeles JRIC is a private sector partnership called InfraGard. Through InfraGard membership, the private sector is urged to contact the FBI and JRIC if they "note suspicious activity or an unusual event." Today, "more than 23,000 representatives of private industry are working quietly with the FBI and the Department of Homeland Security," writes Matthew Rothschild in *The Progressive*'s March 2008 issue.[200] Rothschild found that:

> The members of this rapidly growing group, called InfraGard, receive secret warnings of terrorist threats before the public does—and, at least on one occasion, before elected officials. In return, they provide information to the government, which alarms the ACLU. But there may be more to it than that. One business executive, who showed me his InfraGard

> card, told me they have permission to 'shoot to kill' in the event of martial law.[201]
>
> "We are the owners, operators, and experts of our critical infrastructure, from the CEO of a large company in agriculture or high finance to the guy who turns the valve at the water utility," says Schneck, who by day is the vice president of research integration at Secure Computing. And he said they could sick the FBI on "disgruntled employees who will use knowledge gained on the job against their employers. InfraGard is a great program."

The ACLU is not so sanguine: "There is evidence that InfraGard may be closer to a corporate TIPS program, turning private-sector corporations—some of which may be in a position to observe the activities of millions of individual customers—into surrogate eyes and ears for the FBI."[202]

STAGE 2: MAKING SENSE OF THE SAR REPORT — ANALYSIS

Nothing in the evolution of local policing indicates that "analysis of information to produce an intelligence end product" is a law enforcement agency core competency. However, this is the next step in the SAR process.[203] After entering the SAR Report into the local information system, analysts determine whether it constitutes a report that can be shared with the broader ISE.

The SAR Initiative does not mandate whether analysis should occur inside the local agency, in a smaller urban intelligence center, or in a state Fusion Center, so cities are developing different models.[204] Smaller agencies may do minimal processing before forwarding SAR Reports to the state or major urban Fusion Center. In major cities, trained counter-terrorism experts on staff may apply a more rigorous analytic review of the initial reports and filter out those that can be determined not to have a potential terrorism nexus. Even when agencies examine SAR Reports in-house, the initial report is being stored in a local system and possibly shared with other agencies, such as the FBI, if the city participates with a Joint Terrorism Task Force.

LAPD consolidates SAR Reports and potential SAR Reports with all crime and incident data, which are first collected and processed through the department's Consolidated Crime Analysis Database (CCAD) system. In addition to historical crime data warehousing, CCAD is used to route potential SAR Reports from front-line police officers through the counter-terrorism bureau, which classifies the SAR incident based on specific criteria codes.[205] Each SAR is coded based on as many as 65 to 200 variables, such as time, location, vehicles involved, and descriptions of those involved. It can also include personal information such as names, addresses, driver's license number, scars, or tattoos.

Applying Criteria for Suspicious Activity

The *SAR Initiative Concept of Operations* lays out a two-part review process to determine whether a report meets the ISE-SAR threshold and can be shared through the system. First, officials at a Fusion Center or from a federal agency review the reported suspicious activity against the criteria for an ISE-SAR Report. The Terrorist Screening Center is also contacted to determine if there is valuable information in the Terrorist Screening Database. The analyst reviews the input against all available knowledge and information for linkages to other suspicious or criminal activity. Fusion Centers have the capacity to compare the information stored in numerous government and commercial databases, such as credit reports, court filings, license information, and insurance claims.[206]

In the second step, the officer or analyst applies his or her professional judgment to determine whether the information has a potential nexus to terrorism. If the officer or analyst cannot make this explicit determination, the report will not be accessible by the ISE although it may be retained in the local Fusion Center or federal agency files in accordance with established retention policies and business rules.[207] If an analyst determines that the information has a potential nexus to terrorism, it is classified as an official ISE-SAR Report. Once this classification is made, the information becomes an ISE-SAR Report, is formatted in accordance with ISE-FS-200 (the ISE-SAR functional standard), and then shared with appropriate ISE participants.

Vagueness, Innocent Behavior, and the SAR Standards

What constitutes a SAR Report and whether it has a nexus to terrorism continues to be debated between the top ranks of the LAPD and the Sheriff's Department. Special Order No. 11 directs officers to document innocent and innocuous behavior like taking pictures or video of a facility or infrastructure, showing unusual interest in a facility, or monitoring the activity of people, facilities, processes, or systems.[208] A Los Angeles Sheriff's Department (LASD) officer who works at the JRIC (the Los Angeles-area Fusion Center) revealed his opinion that "SAR [Reports] should have a narrower focus, and a report should have an established nexus to terrorism. Otherwise, you can get overwhelmed with information, all of which must be vetted and analyzed."[209]

Vagueness and subjectivity are inherent in defining what constitutes suspicious activity. According to John Cohen, a spokesperson for the Program Manager of the ISE, "A police officer sees a group of people photographing a piece of critical infrastructure, such as a bridge. The officer approaches and asks them why they are taking pictures. They explain that they are tourists and that they are sightseeing. If the officer finds this credible, no SAR [Report] is filed. If, however, the officer detects deception, he would file a SAR [Report]."[210]

It is clear from PRA's interview with LASD Cmdr. Mike Grossman, a co-manager of the JRIC, that the Sheriff's Department has a more narrow definition than LAPD of what should constitute a SAR Report. [Cmdr. Grossman declined to discuss this difference, referring us to LAPD.] As with the JRIC, whose original DHS mandate related to terrorism, "we were overwhelmed with that kind of potential information," explained Grossman:

> …but the effort now is to go to an all crimes approach because terrorism is all crimes . . . ID theft, money laundering, trademark violations, counterfeiting. Terrorism is not just the operational piece, logistics, support and some of the crimes that are occurring may be benign but are generating millions of dollars to support terrorism around the world. This is extremely complex and the more we learn, the more difficult it gets, it gets more and more complex and takes more resources to be doing what we now know we should be doing and we don't have the budget to keep adding what we need. So there's a concern over that.[211]

All personal information collected via a SAR Report is inputted (and then retained) in an LAPD database *before* a determination is made that it has a nexus to terrorism or criminal activity, at which point it is sent to the JRIC. The individual who is the focus of the report is often identified in reports by identifying characteristics such as: Full name, address, aliases, monikers, date of birth, social security number, citizenship, driver's license, physical description, and distinguishing marks. "Such broad information collection and dissemination obviously exceed limitations imposed by 28 CFR Part 23," the ACLU has written, "yet the federal government actively encourages the violation of the regulation and encourages Fusion Centers to broaden their sources of data beyond criminal intelligence, to include federal intelligence as well as public and private sector data."[212]

STAGE 3: SHARING AND DISSEMINATING SAR REPORTS IN SHARED SPACES AND EGUARDIAN

Shared Spaces and eGuardian are the two main mechanisms for sharing and disseminating SAR Reports. Both systems are used at the Los Angeles JRIC. Once the determination of a potential terrorism nexus is made, the information becomes an ISE-SAR Report, is formatted in accordance with standards formats, and it can then be shared through IT systems with various agencies involved in counter-terrorism. The SAR Initiative relies on databases housed in the agencies where they were created, so they can be more readily updated, corrected, removed, controlled, and audited.[213] The ISE-SAR Report is stored in the Fusion Center or other federal agencies' ISE virtual electronic "Shared Space" where it can be accessed by other ISE participants, including JTTFs through eGuardian.[214]

Shared Spaces: A New Form of National Intelligence Database

ISE's Shared Spaces architecture creates a virtual federal database of SAR data. Once an ISE-SAR Report enters this space, the FBI posts it to its own national database and also sends it to FBI headquarters. Similarly, DHS saves the report in its system and sends it to the DHS Office of Intelligence Analysis.

Huge privacy concerns loom regarding users' access to Shared Spaces and their ability to browse personal data contained in its holdings. In 2007, the Center for Democracy and Technology (CDT) issued a scathing criticism of the ISE's official guidelines, stating:

> Nowhere do the guidelines or accompanying material ever actually say what privacy is. The title and text of the guidelines refer to "other legal protections," but never explain what those are either. The guidelines never mention the First Amendment or free speech. . . . [T]here is no engagement with the challenges of applying the Fair Information Practices in the terrorism context. Government officials confused about what "privacy" means in the counterterrorism context will receive no guidance form these guidelines.[215]

Following the release of CDT's critique, the ISE Program Manager and the Department of Justice gradually produced more detailed templates for implementing "fair information practices," regarding controlling access, correcting errors, and expanding local auditing procedures.

These limited measures may improve privacy protections, but massive challenges persist. In June 2009, ISE leadership admitted to Congress that 12 out of 15 federal departments involved in the ISE had not completed their written privacy protection policies, as required by ISE Privacy Guidelines, Section 12(d).[216] Los Angeles did not formally adopt ISE's suggested privacy policies until August 2009, more than a year into the SAR pilot project.

To date, evaluations or audits of the Los Angeles system have not been released to the public.

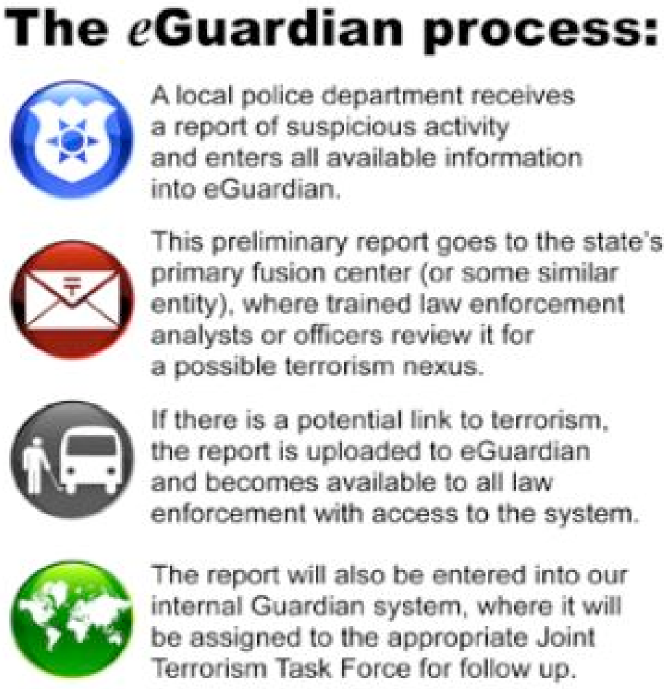
FBI eGuardian

Los Angeles' Joint Regional Intelligence Center uses the FBI's eGuardian system, an unclassified extension of an earlier FBI system called Guardian that provides access to a much broader set of government agencies.[217] eGuardian is a centralized database that is designed to enable state and local law enforcement authorities to share Suspicious Activity Reports with the FBI's Joint Terrorism Task Force at a "nonsecret" level. The Department of Defense also uses eGuardian as its repository of ISE-SAR Reports.

eGuardian is different from Shared Spaces in that a report remains in draft mode while it resides on the FBI server.[218] By granting them electronic "administrative rights," the FBI enables users from nonfederal agencies to enter their initial reports in draft mode. FBI can then access ISE-SAR Reports and incorporate them into their own ultra-secret eGuardian system. eGuardian offers a flexible data retention policy to accommodate state and local laws that may be more stringent than federal regulations.[219]

Through a secure internet portal named Law Enforcement Online (LEO), more than 18,000 agencies will be able to run searches of eGuardian. As of June 2009, the eGuardian user base surpassed 1,000 accounts, drawing participants from all parts of the country. In one four-month period, 346 incidents were reported to eGuardian, of which 280 fell into the category of suspicious activity. Of these, only 15 were determined to have a potential terrorism nexus; 107 were determined to have none.[220]

In 2009, the Department of Defense identified one eGuardian success story: the theft of U.S. Marine uniforms initially reported to a local police department and later submitted to eGuardian by a Fusion Center.[221]



The *e*Guardian process:

A local police department receives a report of suspicious activity and enters all available information into eGuardian.

This preliminary report goes to the state's primary fusion center (or some similar entity), where trained law enforcement analysts or officers review it for a possible terrorism nexus.

If there is a potential link to terrorism, the report is uploaded to eGuardian and becomes available to all law enforcement with access to the system.

The report will also be entered into our internal Guardian system, where it will be assigned to the appropriate Joint Terrorism Task Force for follow up.

EGUARDIAN LIST: eGuardian is a centralized database designed to enable state and local law enforcement authorities to share suspicious activity reports with the FBI's Joint Terrorism Task Forces at nonsecret levels. Law enforcement agencies enter their initial Suspicious Activity Reports (SAR Reports) in draft mode; the FBI can access the reports and incorporate them into its own secret eGuardian system.

Image Source: FBI Website.

Depending on privacy policies and procedures established for the SAR Initiative as a whole or by agencies responsible for individual ISE Shared Spaces, requestors may only be able to view reports in a summary ISE-SAR Information format, with data in privacy fields invisible. But requestors can always contact the submitting organization to discuss details of an ISE-SAR Report or request access to information in its privacy fields.[222]

STAGE 4: REVIEWING AND RETAINING DATA

The formal SAR process relies on multiple levels of review to filter out reports without a potential terrorism nexus. A 2006 official review of existing reporting processes found that local agencies focused on the front end (gathering and processing) but neglected the critical last steps (documenting, analyzing, and sharing) required to fully realize an effective, meaningful information-sharing system. For this reason, federal officials advocate that Fusion Centers formally review and "[weed] out reports that may appear to be 'suspicious' at the local level but are resolved as unimportant after a more in-depth review."[223]

The Commanding Officer of LAPD's Counter Terrorism and Criminal Intelligence Bureau is responsible for monitoring compliance with LAPD Special Order No. 11 and designating a privacy officer. LAPD's 2008 SAR guidelines call for "tips and leads" based on "reasonable suspicion," rather than the lower "reasonable indication," standard offered by the federal program but former Los Angeles FBI Agent Tom Parker, a 23-year veteran still worries that, "This wording is as vague as it gets. The vagueness of this policy would never have been allowed during my time at the bureau. Anyone can call in anything and a report is created. What happens to that information? What are the criteria for purging information or leaving it in the system? It leaves a lot of room for mistakes."[224] To date, evaluations or audits of the Los Angeles system have not been released to the public.

SAR Initiative officials optimistically claim that due to repeated review and re-evaluation of SAR Reports, "reports in the ISE shared spaces… can be presumed by federal, state, and local analysis personnel to be terrorism-related."[225] However, experience shows that feedback and evaluation processes do not always function as intended.

For example, when the Office of the Inspector General (OIG) evaluated the FBI's Guardian system in 2008, it found that the FBI needed to address shortcomings in the accuracy, timeliness, and completeness of information in its database.[226] FBI policy requires a supervisor to review and close each threat assessment or suspicious incident in Guardian. The OIG found that in 12 percent of the 218 incidents tested, supervisory reviews were not performed. Additionally, FBI personnel did not consistently include supplementary information in the Guardian system. The Inspector General found that this incomplete data could cause users performing searches or trend analyses to generate inaccurate threat assessments. The OIG also found that 28 percent of the 218 Guardian incidents tested were not resolved within 30 days — the FBI's standard timeframe. Some Guardian incidents remained unresolved in the threat tracking system for months.

Gaps in the review and evaluation process at a single agency are likely to be multiplied a hundredfold in the SAR Initiative's complex, procedurally diverse system, which holds SAR Reports in Fusion Center and police department databases around the country. For example, the Massachusetts Commonwealth Fusion Center had data-sharing agreements in place with fifteen difference state and regional agencies as of 2008, not including federal departments. Multiply that by seventy-two fusion centers nationwide, plus all of the agencies tapped into the FBI's eGuardian system, and literally thousands of agencies can access potentially erroneous or biased information contained in SAR Reports.

The retention of information gathered through the SAR Initiative poses another potential civil liberties problem. Regardless of the final disposition of a SAR Report (whether it is transmitted to the electronic shared space; leads to an investigation and arrest by the JTTF or the LAPD's Counter Terrorism and Criminal Intelligence Bureau (CTCIB); or proves to be a bogus lead with no connection whatsoever to criminal activity), the personal and identifying information embedded in a Suspicious Activity Report is inputted *and retained* in CTCIB's internal database for an *indefinite period of time*.

The personal and identifying information embedded in a Suspicious Activity Report is inputted and retained in CTCIB's internal database for an indefi-

"When do you really know if something is over? That's the argument," says L.A. Sheriff's Dept. Sgt. Scott Anger. Loose, inconsistent data retention rules and practices — and the fact that individuals can never know for sure if false information about them has been corrected, or if a report has actually been purged — seriously threaten our civil liberties. This issue is indirectly addressed in LAPD's August 2009 Major Crimes Division Order No. 15, obtained through a PRA information request:

> All ISE-SAR information in the Shared Space shall be reviewed for record retention (validation or purge) within 5 years of entry into the Shared Space. Information which does not reach the reasonable suspicion standard of *28 CFR Part 23* will be retained for up to one year to permit the information to be validated or refuted and its credibility and value to be assessed. If the information continues to have credibility and value at the end of one year, it may be retained for an additional year with approval of the Commanding Officer. When ISE-SAR information has no further value or meets the applicable criteria for purge, it will be removed from the Shared Space or the temporary file closed.[227]

The lack of transparency and outside oversight hinders individuals' ability to know or challenge the presence of their information in such records, so such systems are of marginal utility.

Rather than impose a single retention standard for all ISE-SAR Reports nationwide, the architects of the federal SAR Initiative allow submitting organizations to control the retention of the ISE-SAR Reports they generate, store, and upload. Therefore, Los Angeles' records retention policies may differ from that of other agencies in the nationwide system.

Conventional thinking among SAR officials seems to be that SAR information must be purged after one year or, in some cases, after five years at most. Federal ISE-SAR guidelines state that within those time periods, information must be *reviewed* and a decision made on whether to retain or purge it. "It's generally, though, the FBI's view that ten years down the road we may need to refer to particular information to make sure we're connecting all the dots," said a JTTF agent.[228]

Conclusions & Recommendations

As we approach the tenth anniversary of the terror attacks of September 11, a reevaluation of our domestic security infrastructure and practices is in order. The SAR Initiative's broad criteria encourages reporting of routine, perfectly legal activities, or incidents that "just don't seem right." This enables people to fall back on personal biases and engrained stereotypes of what a terrorist looks or acts like when deciding whether to report a "suspicious activity" to police. When following up on or sharing Suspicious Activity Reports, some police will likely, perhaps unconsciously, consider subjects' racial, ethnic, religious, and/or ideological characteristics. As a result, potentially biased tips can travel from a neighborhood police substation through Fusion Centers and into nationwide info-spheres.

The SAR Initiative's concern with "extremist" language gives police license to conflate free speech of dissidents with potential terrorism, inviting surveillance of people and organizations across the political spectrum whose views may be unpopular or unusual.

The lack of a consistent, uniform legal framework governing the overall SAR Initiative exacerbates the potential for prejudices to be operative throughout the system. Masses of data have been funneled to Fusion Centers across the country. Although federal standards have narrowed the criteria for suspicious activities reporting, they remain inconsistent with time-tested civil liberties safeguards. Flawed assumptions about the efficacy of data-mining to identify terror plots, plus other myths used to justify the SAR Initiative are fueling an unwise and risky strategy that targets innocuous lawful activity, rather than concentrating national resources on criminal activity and terrorism.

America's counter-terror effort should enable local agencies to share incidents of *reasonably suspicious* criminal activity with intelligence agencies. The country has made enormous strides in developing that sharing capacity and connectivity. The SAR Initiative, however, promotes procedures that can ultimately undermine national security, individual safety, and civil liberties. It clogs the intelligence system with bad intelligence; erodes Constitutional protections & invites racial, ethnic, and religious profiling; and evades public oversight and accountability, thereby denying Americans knowledge of whether this program is lawful, effective, and worthy of continued public investment.

RECOMMENDATIONS

1. Congress Should Hold Hearings on the SAR Initiative Prior to National Deployment. Americans have a right to know whether these programs actually fulfill their mandate to keep the population safe. Congress should evaluate the effectiveness, lawfulness, and consistency of the SAR Initiative before it can be deployed and periodically thereafter. This evaluation should be required as a condition for all information-based counter-terrorism programs. Public opinion polls reflect the distressing reality that many Americans have been willing to compromise liberty for the promise of security. All who fall under the protection of the U.S. Constitution – whether or not they accept that bargain – deserve an honest accounting of whether the government has delivered on that promise.

2. Rigorously Oversee All Suspicious Activity Reporting. Since Fusion Centers are run by state and local agencies, State lawmakers should not wait for Congress to take action. States should immediately monitor local domestic intelligence practices. The history of internal surveillance in the United States demonstrates that lax oversight leads to abuses that undermine democratic civil society. External checks and balances on Fusion Centers, which process SAR Reports, are virtually non-existent; most supervision is done by law enforcement itself. Advocates should consider following the lead of the ACLU of Massachusetts in crafting state-level independent oversight mechanisms for all Fusion Center activities to ensure compliance with Constitutional safeguards.

DETAINED: August 22, 2008 – Antiwar protestors march through the streets in downtown Denver. Denver Police Department officers remove and detain a peaceful protestor.

Image Source: photo by Thomas Cincotta

3. Fill Seats on the Privacy and Civil Liberties Oversight Board. Vigorous oversight is desperately needed to counterbalance the government's enormous capacity to share information and spy on innocent persons. To ensure that far-reaching surveillance technologies track terrorists rather than innocent people, Congress formed the Privacy and Civil Liberties Oversight Board. Since taking office, President Obama has allowed the board to languish, and its 2010 budget allocation sits unspent. The President should move quickly to fill all of the Board's seats with strong representation from affected communities and experienced civil liberties advocates.

4. Congress Should Pass the End Racial Profiling Act (ERPA). Passing the proposed ERPA – without a national security exemption – is a critical step to ensuring safety for all of our communities. This Act would bar certain law enforcement agencies from using racial profiling as an investigatory tool. Lengthy detentions, unwarranted scrutiny and/or harassment by government agents have unduly harmed people who have done nothing illegal. Profiling violates Constitutional guarantees and international human rights norms and distracts law enforcement from real terrorist suspects, putting everyone at risk. Further, the harm created by targeting ethnic communities only provides more ideological fodder for foreign terrorists that seek to recruit supporters within our borders.

5. Remove Non-Criminal Activity from SAR Report Criteria. SAR Programs lower the Constitutional threshold for information gathering and sharing. In its current form, the SAR Initiative will likely lead police to increasingly stop, question, and even detain individuals engaged in First Amendment-protected activity, including harmless legal conduct like photography, or on the basis of racial, ethnic, or religious characteristics. The Justice Department should amend the civil liberties safeguard *28 CFR 23* to stipulate that Suspicious Activity Reports constitute "criminal intelligence" which may only be stored if data meets the long-utilized standard of reasonable suspicion of criminal conduct. Failing that, at a minimum, the Justice Department must revise suspicious activity criteria to completely bar photography, protest gatherings, demonstrations, political lectures and other First Amendment activities as indicators of suspicious conduct. Such changes will reduce the amount of irrelevant data and increase safety and security; they should be made compulsory for any agency that wishes to participate in the Information Sharing Environment.

6. Regulate new "Shared Spaces" Information Sharing Infrastructure. Congress and the Justice Department should take regulatory action and enact legislation to make "Shared Spaces" – a new form of intelligence database – officially subject to the Constitutional safeguards embodied in *28 CFR 23*.

7. Expose Domestic Surveillance. Excessive secrecy limits public knowledge of local intelligence practices. Litigators defending the rights of political dissenters should routinely request records maintained in the SAR Initiative system. City, county and state governments should require local law enforcement and Fusion Center officials to detail their surveillance and documentation practices. Community activists should demand that public officials answer questions like:

- Who is responsible for the collection of intelligence information?
- What information is being collected and for what purpose?
- With whom will the information be shared?
- How long will it be retained?
- How accurate and reliable is the information?
- How will the data be secured against loss or unauthorized access?
- Will individuals know the basis for decisions affecting them, such as searches, detentions, or an intimidating knock on the door?
- How are surveillance cameras contributing to this network?
- How will individuals be able to respond to false and erroneous information?
- Are procedures in place to purge inaccurate and irrelevant data?
- Who audits the system?
- Which agencies have which missions?
- What is the role of the military in domestic intelligence?

8. Restore Constitutional Checks and Balances. Legislators should enlist courts as a critical check and balance for the new nationwide intelligence apparatus by requiring judicial permission before agencies can access personal identifying information in SAR Reports. Lawmakers should require a judicial determination whenever the government seeks to unveil the names of persons identified through data collection or mining.

9. Enhance Privacy Protections in Information-Sharing Systems. The Markle Foundation's Task Force on National Security in the Information Age and the Center for Democracy and Technology developed detailed recommendations concerning privacy protections that should be built into information sharing systems. They clearly identify steps to bring privacy laws into the 21st Century. Policymakers should refer to these guides to ensure that systems are structured appropriately. Some recommendations have already made it into law. Policy leaders need to recognize that while architects of SAR Initiative policies often claim that SAR programs abide by safeguards, the fact that standard operating procedures call for collecting non-criminal data strongly suggests that SAR practices do not adhere to the law.

10. Revisit the Need for Fusion Centers in the Post-September 11 Bureaucracy. With 72 new Fusion Centers, an intelligence net is being cast inward, bringing more of us under the government's watchful eye. The FBI's Joint Terrorism Task Forces (JTTF), which operate under the clearly-defined authority and oversight of the Department of Justice, already take the lead in investigating and stemming potential terrorist plots across the country. The redundancy of certain activities and the lack of Congressional oversight of Fusion Centers warrant the attention of public interest researchers, journalists, and policy makers. It is worth considering whether the public might be better served by relocating the Fusion Centers' data fusing function to JTTFs, thereby achieving increased of public accountability while also streamlining the bureaucracy.

11. Reject Intelligence-Led Policing in favor of Community Policing and Traditional Law Enforcement. Our research fails to find a justification for mandating that local law enforcement adopt a pre-emptive policing model. The term "intelligence-led policing" masks the fact that it is really *pre-emptive* policing, which raises serious Constitutional issues. Should police have the right to investigate non-criminal behavior indefinitely, with no limits—or built-in safeguards? Endless tracking of individuals such as outspoken political activists or religious leaders in any community to maintain "situational awareness" of alleged potential terrorism chills First Amendment rights and erodes public trust.

Pre-emptive policing is a concern not only for civil libertarians and affected communities, but also for law enforcement executives. The International Association of Chiefs of Police should reject the functional re-classification of officers as intelligence agents. Law enforcement agencies around the country have raised questions about the value of deputizing local cops as immigration agents because doing so makes certain people afraid to report crime, jeopardizing public safety. Chiefs of police should seriously consider whether it is useful to reassign officers as intelligence analysts, removing them from community problem-solving and crime response. Supervisors should take into account the detrimental effects of the intelligence-gathering approach, such as the sowing of mistrust, especially within communities that are preemptively targeted. A traditional law enforcement approach to deterring terrorism—rather than an intelligence paradigm—would allow police to focus on their core competencies and actionable leads, rather than casting a broad net and wasting resources by monitoring many innocent activities.

Appendix 1

TIMELINE OF THE INSTITUTIONALIZATION OF NATIONWIDE SUSPICIOUS ACTIVITY REPORTING INITIATIVE

Mar 2002 International Association of Chiefs of Police (IACP) meets to explore their own intelligence sharing initiatives at the Criminal Intelligence Sharing Summit. IACP calls for amending *28 CFR 23* to reduce the threshold of "reasonable suspicion" to "reasonable indication." Based on IACP recommendations and funded by the DOJ, the Global Intelligence Working Group formed to write National Criminal Intelligence Sharing Plan later that year.

2003 National Criminal Information Sharing Plan calls for *28 CFR 23* to be used by all agencies in Information Sharing Environment.

July 2004 9/11 Commission Report does not use the term "Suspicious Activity Reporting," but is replete with examples of opportunities lost because available information was inaccessible due to "human or systemic resistance to sharing information."

Dec. 2004 Congress passes Intelligence Reform and Terrorism Prevention Act (IRTPA) directing President to establish the Information Sharing Environment (ISE), an approach that facilitates the sharing of terrorism and criminal information, but also includes immigration and other personal data. IRTPA § 1016 requires president to appoint a program manager to work with Information Sharing Council to foster an Information Sharing Environment among all appropriate entities and the private sector.

Fall 2005 Counter-terrorism Security Group, an arm of the National Security Council, tasks NCTC to work with the counter-terrorism community to develop options for improving the value of SAR to preventing terrorism.

2006 An interagency working group on SAR processes formed under auspices of the Program Manager for the ISE in the Office of the Director of National Intelligence. The SAR Support and Implementation Project team includes: 1) law enforcement experts from all levels, 2) Bureau of Justice Assistance, 3) Major Cities Chiefs Association, 4) DOJ's Global Justice Information Sharing Initiative, 5) Criminal Intelligence Coordinating Council, and 6) DHS.

Oct. 2007 President Bush issues National Strategy for Information Sharing to unify efforts to advance the sharing of terrorism-related information. Calls for federal support to develop a nationwide capacity for gathering, documenting, processing, analyzing, and sharing terrorism-related SAR Reports in a manner that rigorously protects the privacy and civil liberties of Americans.

Jan. 2008 PM-ISE (through the Common Terrorism Information Sharing Standards Committee of the Information Sharing Council) releases Version 1 of the ISE-SAR Functional Standard including common definition for Suspicious Activities Reports, set of SAR data elements, a business process, and initial set of criteria for determining when a report should be designated as one with a potential terrorism nexus.

Mar. 2008 Los Angeles Police Department (LAPD) mandates a department-wide SAR process with Special Order No. 11, spearheading the national SAR initiative.

Sep. 2008 Privacy and Civil Liberties Analysis for the ISE-SAR Functional Standard and Evaluation Environment issued.

May 2009 Program Manager for the ISE revises the Functional Standard for Suspicious Activity Reporting (Version 1.5). Civil liberties advocates had raised concerns about SAR Initiative, arguing it targeted legal activities and had inadequate protections against racial/ethnic/religious profiling.

Sept 2009 The ISE-SAR Evaluation Environment concluded. A final report documenting "Lessons-Learned" and "Best Practices" was set for the end of 2009.

Appendix 2

DATA MINING PROGRAMS SINCE SEPTEMBER 11, 2001

Program	*Description / Purpose*	*Status*	*Problems*
Total Information Awareness » Terrorism Information Awareness (TIA)	Originally named "Total Information Awareness," the name of the program was quickly changed to "Terrorism Information Awareness." Goal was to find signatures of terrorist activity patterns by mining individuals' financial, medical, travel, place/event entry, transportation, education, housing, and communications transactions. TIA was created by the Defense Advanced Research Projects Agency (DARPA) in 2002.	Congress terminated funding for the program on September 25, 2003, except for "processing, analysis, and collaboration tools for counter-terrorism foreign intelligence," specified in a classified annex to the Act. The language makes clear that TIA-like activities may continue through hidden research projects and programs.	Name change was prompted by the strongly negative reaction of the American public to the threat it posed to informational privacy and overbroad surveillance. Program could generate high numbers of false positives and access personally identifiable data of U.S. persons who did nothing to warrant suspicion.
National Intelligence Program	Can only use research against non-Americans within the United States.	Congress transferred some of the funding, which was previously going to the TIA, to the National Intelligence Program.	There is no check on the government from expanding the program to American citizens at a later date.
Evidence Extraction and Link Discovery	Program goal is to design systems with the ability to extract data from multiple sources (text messages, social networking sites, financial records, web pages, etc.) Designed to link items relating to potential "terrorist" groups and scenarios, and to learn patterns of different groups or scenarios to identify new organizations and emerging threats.	Still in operation.	Surviving TIA programs include some of the 18 data-mining projects that are collectively known as "Evidence Extraction and Link Discovery" within DARPA's Information Awareness Office.
Novel Intelligence from Massive Data	Program of the National Security Agency that is supposed to extract information from databases including text, audio, video, graphs, images, maps, equations, and chemical formulae. The mission was to help the nation avoid "strategic surprise," which was defined as unanticipated events critical to national security.	Its current operations can not be confirmed.	This type of early warning approach may involve a significant increase in domestic surveillance. There is much overlap between NIMD and the TIA program, and some experts stated that the NIMD is the controversial TIA program in a slightly different form.

Quantum Leap	Program of the CIA that enables an analyst to get quick access to all classified and unclassified information about virtually anyone.	Began to be used in 2003, but its present use can not be confirmed.	Deputy Chief Information Officer Bobby Brady stated that the program is "so powerful it's scary" and in the wrong hands, "{it} could be Big Brother."
Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement (ADVISE)	Situated within the Department of homeland Security's "Threat and Vulnerability Testing and Assessment" portfolio. The system is meant to collect both corporate and public online information and cross-reference it against law enforcement and intelligence records. Goal was to illuminate terrorist motives and intentions.	The DHS TVTA portfolio was set up in 2003, and it received $47 million in funding in 2006. The program was ended in September 2007 by orders from the agency's internal Inspector General.	The Inspector General scrapped the program in 2007 after it found that pilot testing of the system had been performed using data on real people without the required privacy safeguards in place.
Multi-State Anti-Terrorism Information Exchange (MATRIX)	MATRIX was based on a "high terrorism factor" scoring system. Source data would include criminal histories, driver's license data, vehicle registration records, and public data record entries. Other data was thought to include credit histories, driver's license photographs, marriage and divorce records, social security numbers, dates of birth, and the names/addresses of family members, neighbors and business associates. ACLU noted that the type of data compiled could be expanded to include information in commercial databases.	Contract for the program was won in May 2003, and it was terminated in May 2005. Before the official termination, at least 11 of the 16 states that participated in the MATRIX pilot program pulled out.	ACLU's Freedom of Information Act requests from 2003 revealed that MATRIX would perform an almost identical function to the previously banned TIA program. Federal funding was cut amid concerns over privacy and state surveillance.
Computer Assisted Passenger Prescreening System (CAPPS II)	Counter-terrorism system in place in the U.S. air travel industry. It is designed to use algorithms to sort through Passenger Name Records (full name, address, etc.) and other information in order to "risk score" all airline passengers. Risk scores determined level of screening the person must go through, and sometimes whether they would be able to travel where they wanted to go or not.	This second generation of the CAPPS system was proposed in 2003 by the Transportation Security Administration. The CAPPS II program was cancelled by the TSA in the summer of 2004, only to be modified.	The TSA claimed that it had not used any real-world data in the testing of CAPPS II, but this later turned out to be false. The program also contained no mechanism by which a passenger could challenge his/her score.

Secure Flight	Airline passenger pre-screening program that covers all passengers traveling to, through, or within the country. The program will match passenger information against federal government watch lists. The program will serve to prevent certain individuals from boarding an aircraft, while subjecting others to enhanced screenings.	Announced in 2004 as the modification to the previous CAPPS II system. TSA suspended the program in February 2006 after discovering the database was accessible to hackers. Implementation began in August of 2009 by the TSA.	Congress dictated that Secure Flight was to forgo the use of private sector data and risk scoring, both of which were employed by the previous CAPPS II program. Reports in July 2005, however, revealed that the TSA did actually link passenger information to commercial databases. Also, the program was deemed as developing into something much more complex than what was originally described; it would compile dossiers on passengers in order to score their likelihood of being a terrorist.

Appendix 3

LAPD SPECIAL ORDER NO. 11

This directive has been typeset and reformatted for this report.

OFFICE OF THE CHIEF OF POLICE

SPECIAL ORDER NO. 11MARCH 5, 2008

SUBJECT: REPORTING INCIDENTS POTENTIALLY RELATED TO
FOREIGN OR DOMESTIC TERRORISM

PURPOSE:

Current anti-terrorism philosophy embraces the concept that America's 800,000 law enforcement officers fill a critical position in the area of terrorism prevention. Law enforcement authorities must carry out their counter-terrorism responsibilities within the broader context of their core mission of providing emergency and non-emergency services in order to prevent crime, violence and disorder. In support of this, the Department's Counter-Terrorism and Criminal Intelligence Bureau (CTCIB) is engaging in an effort to more thoroughly gather, analyze and disseminate information and observations, of either a criminal or suspicious nature, which may prove critical to the intelligence cycle.

This Order establishes Department policy for investigating and reporting crimes and non-criminal incidents that represent indicators of potential foreign or domestic terrorism, and incorporates within the Department Manual a procedure for gathering and maintaining information contained in such reports.

POLICY:

It is the policy of the Los Angeles Police Department to make every effort to accurately and appropriately gather, record and analyze information, of a criminal or noncriminal nature, that could indicate activity or intentions related to either foreign or domestic terrorism. These efforts shall be carried out in a manner that protects the information privacy and legal rights of Americans, and therefore such information shall be recorded and maintained in strict compliance with existing federal, state and Department guidelines regarding Criminal Intelligence Systems (28 Code of Federal Regulations (CFR), Part 23 and applicable California State Guidelines).

PROCEDURE:

I. DEFINITIONS.

A. Suspicious Activity Report. A Suspicious Activity Report (SAR) is a report used to document any reported or observed activity, or any criminal act or attempted criminal act, which an officer believes may reveal a nexus to foreign or domestic terrorism. The information reported in a SAR may be the result of observations or investigations by police officers, or may be reported to them by private parties.

Incidents which shall be reported on a SAR are as follows:

- Engages in suspected pre-operational surveillance (uses binoculars or cameras, takes measurements, draws diagrams, etc.)
- Appears to engage in counter-surveillance efforts (doubles back, changes appearance, evasive driving, etc.);
- Engages security personnel in questions focusing on sensitive subjects (security information, hours of operation, shift changes, what security cameras film, etc.);
- Takes measurements (counts footsteps, measures building entrances or perimeters, distances between security locations, distances between cameras, etc.);
- Takes pictures or video footage (with no apparent esthetic value, i.e. camera angles, security equipment, security personnel, traffic lights, building entrances, etc.);
- Draws diagrams or takes notes (building plans, location of security cameras or security personnel, security shift changes, notes of weak security points, etc.);
- Abandons suspicious package or item (suitcase, backpack, bag, box, package, etc.);
- Abandons vehicle (in a secured or restricted location i.e. the front of a government building, airport, sports venue, etc.);
- Attempts to enter secured or sensitive premises or area without authorization (i.e. "official personnel," closed off areas of airport, harbor, secured areas at significant events such as appearances by politicians, etc);
- Engages in test of existing security measures (i.e. "dry run", security breach of perimeter fencing, security doors, etc., creating false alarms in order to observe reactions, etc.);
- Attempts to smuggle contraband through access control point (airport screening centers, security entrance points at courts of law, sports games, entertainment venues, etc.);
- Makes or attempts to make suspicious purchases, such as large amounts of otherwise legal materials (i.e. pool chemicals, fuel, fertilizer, potential explosive device components, etc);
- Attempts to acquire sensitive or restricted items or information (plans, schedules, passwords, etc);
- Attempts to acquire illegal or illicit explosives or precursor agents;
- Attempts to acquire illegal or illicit chemical agent (nerve agent, blood agent, blister agent, etc.);
- Attempts to acquire illegal or illicit biological agent (anthrax, ricen, Eboli [sic], small pox, etc.);
- Attempts to acquire illegal or illicit radiological material (uranium, plutonium, hospital x-ray discards, etc.);
- In possession, or utilizes, explosives (for illegal purposes);
- In possession, or utilizes, chemical agent (for illegal purposes, i.e. dry ice bomb, chlorine, phosgene, WMD attack, etc);
- In possession, or utilizes, biological agent (for illegal purposes, i.e. terrorist device, WMD or a tool of terrorism, etc.);
- In possession, or utilizes, radiological material (for illegal purposes, i.e. as a weapon, etc.);
- Acquires or attempts to acquire uniforms without a legitimate cause (Service personnel, government uniforms, etc);
- Acquires or attempts to acquire official or official-appearing vehicle without a legitimate cause (i.e. emergency or government vehicle, etc.);
- Pursues specific training or education which indicate suspicious motives (flight training, weapons training, etc);

- Stockpiles unexplained large amounts of currency;
- In possession of multiple passports, identifications or travel documents issued to the same person;
- Espouses extremist views (verbalizes support of terrorism, incites or recruits others to engage in terrorist activity, etc.); Brags about affiliation or membership with extremist organization ("white power", militias, KKK, etc.);
- Engages in suspected coded conversations or transmissions (i.e. email, radio, telephone, etc., i.e. information found during a private business audit is reported to police);
- Displays overt support of known terrorist networks (posters of terrorist leaders, etc.);
- Utilizes, or is in possession of, hoax/facsimile explosive device;
- Utilizes, or is in possession of, hoax/facsimile dispersal device;
- In possession of, or solicits, sensitive event schedules (i.e. Staples Center);
- In possession of, or solicits, VIP Appearance or Travel Schedules;
- In possession of, or solicits, security schedules;
- In possession of, or solicits, blueprints to sensitive locations;
- In possession of, or solicits, evacuation plans;
- In possession of, or solicits, security plans;
- In possession of, or solicits, weapons or ammunition;
- In possession of, or solicits, other sensitive materials (passwords, access codes, secret government information, etc.); and,
- In possession of coded or ciphered literature or correspondence.

B. Involved Party (IP). An involved party (IP) is an individual that has been observed engaging in suspicious activity of this nature, when no definitive criminal activity can be identified, thus precluding their identification as a suspect.

II. REPORTING AND INVESTIGATING.

A. Employees - Responsibilities. Any Department employee receiving any information regarding suspicious activity of this nature shall:

Investigate and take appropriate action, to include any tactical response or notifications to specialized entities.

Note: This section does not preclude, in any way, an employee taking immediate action during the commission of a criminal act, or in circumstances which require the immediate defense of life, regardless of the nature or origin.

If the activity observed is not directly related to a reportable crime, officers shall record the information collected from the person reporting, or their own observations, on an Investigative Report (IR), Form 03.01.00, titled "Suspicious Activity" in accordance with the following guidelines:

If the person reporting (R) is willing to be contacted by investigators, they shall be listed within the Involved Persons portion of the IR. Officers shall consider utilizing a "Request for Confidentiality of Information," Form 03_02.00, to ensure confidentiality. If absolutely necessary, officers can enter "Anonymous" for person reporting. Any desire by a person reporting to remain anonymous does not exempt officers from the requirement to complete a TR.

- If the potential target of the activity can be identified, such as a government building or official being surveilled, that location or individual shall be listed within the "Victim" portion of the IR. Otherwise the "City of Los Angeles" shall be listed as the victim.
- If the information includes an involved party (IP), officers shall identify or fully describe IPs within the narrative (page 2) of their report, along with any vehicle descriptions or other pertinent information. If the information is related to a regular criminal investigation (such as a bomb threat, criminal threats, trespassing, etc.), the officers shall complete the criminal investigation, make any appropriate arrests and complete any related reports. The officers shall include any additional information

that provides the nexus to terrorism within the narrative of the crime or arrest report.

Should officers come across information that indicates possible terrorism-related activity while investigating an unrelated crime or incident (e.g., such as officers conducting a domestic violence investigation observe possible surveillance photographs and a map of the region surrounding a government facility), or should they conduct an impound or found property investigation which is suspicious in nature, the officers shall make no mention of this potential terrorism-related material or activity within the impound, property, crime or arrest report. Under these circumstances, the officers shall complete a separate SAR in addition to the crime or arrest report, and shall note the criminal investigation, impound or found property investigation as their source of their activity.

Officers shall note on the left margin of any arrest face sheet or IR that the report is to be sent to CTCIB, Major Crimes Division.

> **Note:** The Investigative Report is currently being revised to include "SAR" and "Original to CTCIB, Major Crimes Division" boxes to be checked when appropriate. The revised IR will also include additional entries for involved parties and involved vehicles.

- Notify Major Crimes Division (contact Real-Time Analysis and Critical Response [RACR] Division for off hours notification) for guidance or if the report involves an arrest or a crime with follow-up potential.
- Notify the Watch Commander, Area of occurrence.

Upon approval by the Watch Commander, ensure the Area Records Unit is made aware of the report, immediately assigns a DR number and forwards the original report to MCD.

> **Note:** Nothing in this Order alters existing .policies regarding notifications to required specialized units such as Bomb Squad, Hazardous Materials Unit, Criminal Conspiracy Section or RACR Division.

B: Hazardous Materials and Devices Section, Emergency Services Division - Responsibility. Personnel assigned to the Bomb Squad, Hazardous Materials/ Environmental Crimes, or Airport K-9 Bomb Detection Unit shall ensure that a SAR is completed on all incidents on which they respond where a potential nexus to terrorism exists. Suspicious Activity Reports completed by personnel assigned to these units shall be processed through a geographic Area Records Unit as directed below.

C. Watch Commanders Responsibilities. Upon notification that officers have received information regarding suspicious activity, the Watch Commander shall:

- Ensure the information supports the completion of a SAR report and that no greater law enforcement response or notifications to MCD are currently needed;
- Review the report for completeness; and,
- Ensure the Area Records Unit immediately assigns a DR Number and forwards the original report to MCD.

D: Major Crimes Division Responsibility. Upon receiving a telephonic notification of suspicious activity, MCD personnel shall, when appropriate, conduct immediate debriefs of arrestees, or provide the appropriate guidance to patrol officers. Upon receiving a SAR report forwarded to MCD, assigned personnel shall follow established protocols regarding the processing of such information.

E. Records Personnel - Responsibilities. Upon receipt of a SAR-related incident, crime or arrest report, records personnel shall:

- Enter the information into the CCAD system, including any appropriate CTCIB-related codes; and,
- Send the original report to "CTCIB/Major Crimes Division, Stop 1012" as soon as practicable, but no later than 24 hours after the report is taken. No copies of the report shall be maintained at the Area.

F. Area Detectives Personnel - Responsibilities. Upon receipt of a SAR-related crime or arrest report Area detectives shall:

- Ensure the report has been screened by MCD personnel and referred back to the geographic Area for investigation; and,
- Complete the investigation per normal policies and guidelines.

Note: If the report is a SAR-related incident only, or a crime or arrest report which arrives at an Area Detective Division without having been reviewed by MCD personnel, Area detectives shall immediately forward the report to MCD (no copies shall be retained at the Area).

G. Counter-Terrorism and Criminal Intelligence Bureau -Responsibility. Counter-Terrorism and Criminal Intelligence Bureau (CTCIB) is responsible for providing Department personnel with training pertaining to the proper handling of suspected terrorism-related activity and ensuring adherence to the guidelines established regarding developmental information and intelligence systems. **AMENDMENTS:** This Order adds section 4/271.46 to the Department Manual_

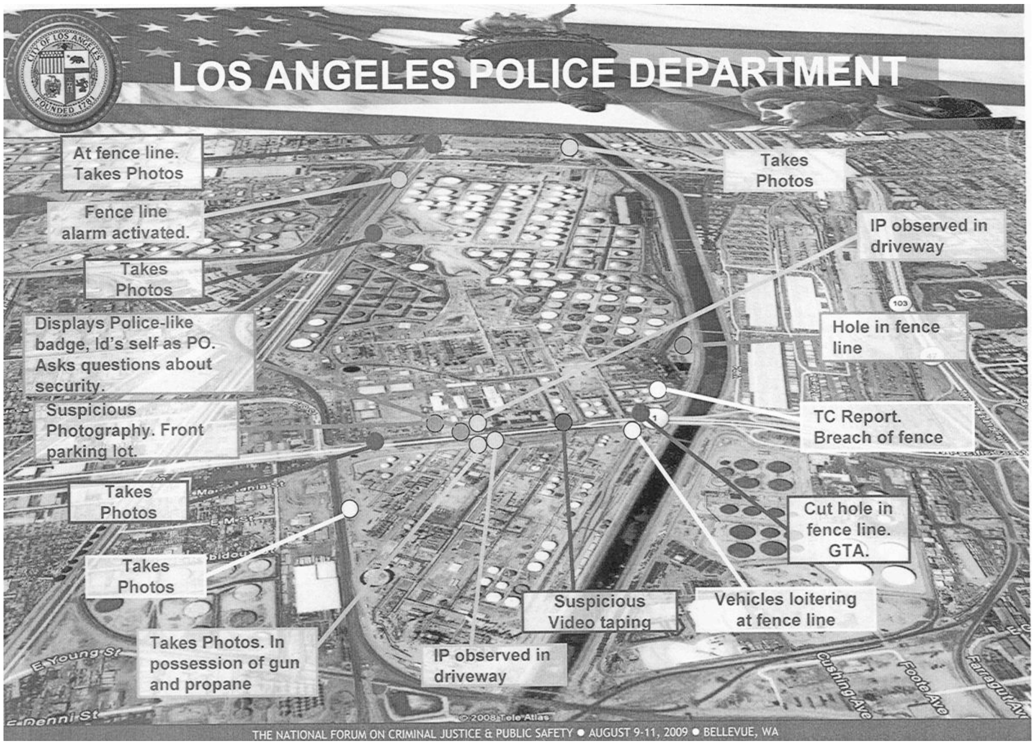
AUDIT RESPONSIBILITY: The Commanding Officer, Counter Terrorism and Criminal Intelligence Bureau, shall monitor compliance with this directive in accordance with Department Manual Section 0/080.30 and shall ensure that all information is collected and maintained in strict compliance with existing federal, State and Department guidelines regarding Criminal Intelligence Systems (28 C.F.R., Part 23 and applicable California State Guidelines).

WILLIAM J. BRATTON Chief of Police

DISTRIBUTION “D”

Appendix 4

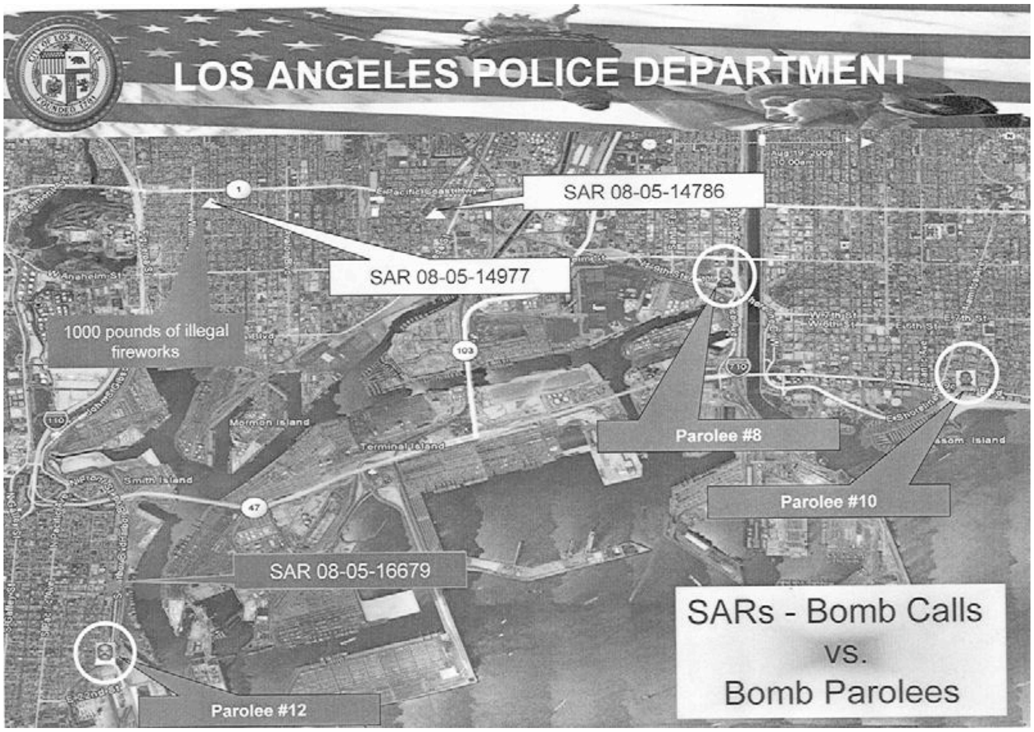
IMAGES FROM LAPD SLIDESHOW PRESENTATION OF HYPOTHETICAL INCIDENTS



LOS ANGELES POLICE DEPARTMENT

At fence line. Takes Photos
Fence line alarm activated.
Takes Photos
Displays Police-like badge, Id's self as PO. Asks questions about security.
Suspicious Photography. Front parking lot.
Takes Photos
Takes Photos
Takes Photos. In possession of gun and propane
IP observed in driveway
Suspicious Video taping
Vehicles loitering at fence line
Cut hole in fence line. GTA.
TC Report. Breach of fence
Hole in fence line
IP observed in driveway
Takes Photos
E Young St
E Denni St
Cushing Ave
Foote Ave
Farragut Ave
© 2008 Tele Atlas

THE NATIONAL FORUM ON CRIMINAL JUSTICE & PUBLIC SAFETY ● AUGUST 9-11, 2009 ● BELLEVUE, WA

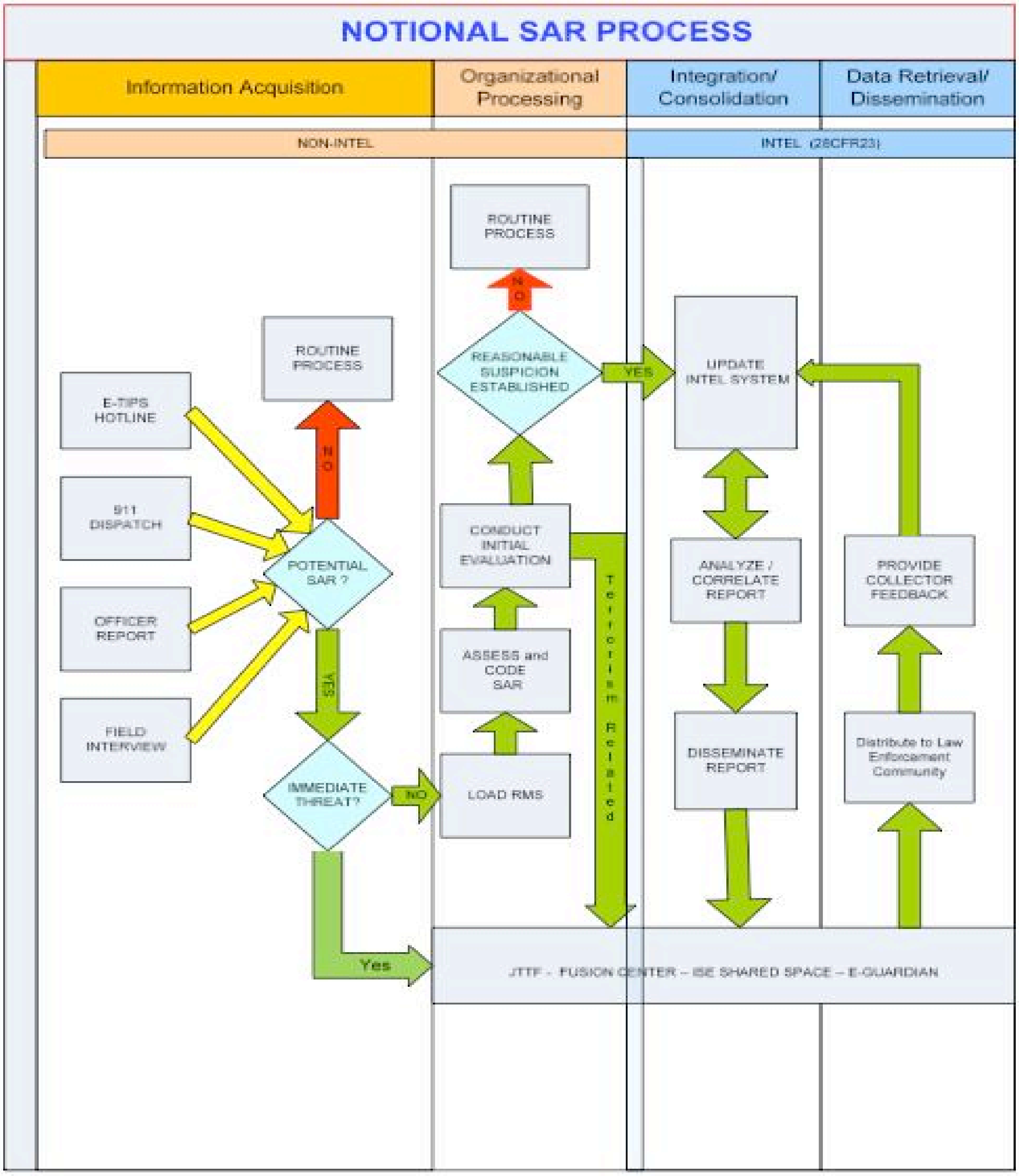


LOS ANGELES POLICE DEPARTMENT

SARs - Bomb Calls
vs.
Bomb Parolees

Appendix 5

GRAPHIC FROM SAR INITIATIVE'S PILOT PROJECT'S FINDINGS AND RECOMMENDATIONS


NOTIONAL SAR PROCESS
Information Acquisition
Organizational Processing
Integration/ Consolidation
Data Retrieval/ Dissemination
NON-INTEL
INTEL (28CFR23)
E-TIPS HOTLINE
911 DISPATCH
OFFICER REPORT
FIELD INTERVIEW
ROUTINE PROCESS
NO
POTENTIAL SAR ?
YES
IMMEDIATE THREAT?
NO
Yes
LOAD RMS
ASSESS and CODE SAR
CONDUCT INITIAL EVALUATION
REASONABLE SUSPICION ESTABLISHED
NO
ROUTINE PROCESS
YES
Terrorism Related
UPDATE INTEL SYSTEM
ANALYZE / CORRELATE REPORT
DISSEMINATE REPORT
PROVIDE COLLECTOR FEEDBACK
Distribute to Law Enforcement Community
JTTF – FUSION CENTER – ISE SHARED SPACE – E-GUARDIAN

About the Editorial Team & Civil Liberties Project Team

STAFF TEAM

Project Director **Thomas Cincotta** heads PRA's nationwide investigation of regional counterintelligence strategies. A criminal defense lawyer, he coordinated the Denver chapter of the National Lawyers Guild (NLG) in support of peace groups and other dissidents during the 2008 Democratic National Convention. He connected progressive lawyers with other community efforts around sentencing reform, immigrant rights, and police misconduct. He also represented migrant farm workers and served on the board of El Centro Humanitario, Denver's first day laborer center. Cincotta currently serves on the NLG's national executive board and international committee. Before becoming a lawyer, Cincotta worked as a labor representative for UNITE HERE Local 217 in Providence, Rhode Island.

Tarso Luís Ramos is Executive Director of Political Research Associates, a role he assumed after serving as PRA's research director for three years. As research director, he focused on anti-immigrant groups and the rise of "colorblind" ideology. He also launched three new research projects-on civil liberties, right-wing attacks on mainline churches, and Islamophobia and antisemitism on college campuses. Before joining PRA, he served as founding director of Western States Center's racial justice program, which resists racist public policy initiatives and supports the base-building work of progressive people of color-led organizations. As director of the Wise Use Public Exposure Project in the mid-'90s, he tracked the Right's anti-union and anti-environmental campaigns.

Senior Analyst **Chip Berlet**, at PRA since 1982, has written, edited, and co-authored numerous articles on civil liberties, surveillance, and government repression for publications as varied as the New York Times, Boston Globe, Utne Reader, and Amnesty Now.. He serves as a vice president of the Defending Dissent Foundation. Berlet spent several years as a paralegal investigator for lawsuits filed by the American Civil Liberties Union, National Lawyers Guild and other groups against the FBI, CIA, Military Intelligence, and local police Red Squads. His article on "Violence and Public Policy" appeared in the journal of Criminology and Public Policy special issue on terrorism. He also wrote the entry on "Surveillance Abuse" for the Encyclopedia of Crime and Punishment. Berlet is co-author, with Matthew N. Lyons, of *Right-Wing Populism in America: Too Close for Comfort* published by Guilford Press (2000).

PRA INVESTIGATORS

Mary Fischer - Los Angeles

Fischer is an award-winning investigative reporter and editor with twenty-three years of experience covering criminal justice, law enforcement, medical and government agency (FBI, BOP, DEA) stories for national and regional magazines, including GQ, Men's Journal, The Daily Journal, New York, Life, Oprah, Rolling Stone, ELLE, Los Angeles Times, and Los Angeles Magazine. Mary is known for her high-impact, in-depth research that often generates national media attention and on-air interviews.

Trevor Aronson – Miami

A Florida native, Aaronson is a freelance journalist who writes about government, criminal justice, globalization and technology in the United States and abroad. He has won more than two dozen national and regional awards for his work, including recognition from the Society of Professional Journalists and the National Association of Black Journalists. In addition, Aaronson was a finalist for the 2005 Livingston Awards for Young Journalists for a series about corruption at the Hollywood (Fla.) Police Department that led to federal indictments and convictions of four high-ranking officers.

NATIONAL ADVISORS

Heidi Boghosian, National Lawyers Guild, Executive Director

Eileen Clancy, iWitness Video

David Cunningham, Brandeis University, Professor of Sociology

Aziz Huq, University of Chicago Law School, Lecturer in Constitutional Law

Hussein Ibish, Hala Salaam Maksoud Foundation, Executive Director

National Police Accountability Project

Tram Nguyen, Journalist

Chip Pitts, Bill of Rights Defense Committee, President of Board of Directors

Carol Rose, ACLU Massachusetts, Executive Director

Shakeel Syed, Islamic Shura Council, Los Angeles Chapter, Executive Director

Sue Udry, Defending Dissent Foundation, Executive Director

Manisha Vaze, Families for Freedom, Anti-Deportation Organizer

Glossary

28 CFR Part 23 – This is legal shorthand for a portion of a federal document: 28 Code of Federal Regulations (CFR) Part 23 (*28 CFR 23*) is a regulation designed to ensure that police intelligence operations are properly focused on illegal behavior by requiring that criminal intelligence systems "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." This rule is a constitutional safeguard that governs inter-jurisdictional and multi-jurisdictional criminal intelligence systems operated by or on behalf of state and local law enforcement agencies and funded with certain federal funds. Many state Fusion Centers and local intelligence units have voluntarily adopted *28 CFR 23* guidelines, although auditing and oversight of compliance is wholly inadequate.

COINTELPRO – An acronym for the "Counterintelligence Program," operated secretly by the Federal Bureau of Investigation from 1956 through 1971.

Functional Standards – The Office of the Director of National Intelligence, in coordination with the Department of Justice and Department of Homeland Security, developed and promulgated common standards for preparing terrorism information for "maximum distribution and access" of terrorism information within the Information Sharing Environment. Functional Standards are rules, conditions, guidelines, and characteristics of data products set forth by the ODNI. The Functional Standards do not have the force of law or official regulation; they are not adopted by Congress or published in the Federal Register. This report addresses Functional Standards, but not the Technical Standards, which are the specific methodologies used to facilitate information exchange.

Information Sharing Environment (ISE) – Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 called for the creation of an Information Sharing Environment (ISE), defined as "an approach that facilitates the sharing of terrorism and homeland security information, which may include any method determined necessary and appropriate for carrying out this section." The ISE includes State and major urban area intelligence Fusion Centers and their law enforcement, homeland security, and other information-sharing partners at the federal, state, local, and tribal levels. Executive Order 13388 and the Presidential Information Sharing Guidelines released in 2005 further refined the definition of the ISE. The National Strategy for Information Sharing (NSIS) issued on October 31, 2007 by President Bush, outlined the goals and challenges in improving terrorism-related information sharing.

Intelligence – Intelligence in this context has come to mean information that has been selected and collected, and then analyzed, evaluated and distributed to meet the unique policy-making needs of one particular enterprise.

Intelligence Abuse – Intelligence activities that violate laws and constitutional protections, especially, in the United States, the First and Fourth Amendments.

ISE Shared Space – A local repository of Suspicious Activity Reports that theoretically have a "potential nexus" with terrorism. ISE Shared Spaces are networked data repositories used to make standardized terrorism-related information, applications, and services accessible to all ISE participants (across the law enforcement, intelligence, homeland security, foreign affairs, and defense communities). The term describes a functional concept, not a specific technical approach. Agencies locally hold and control SAR data and make that data easily and securely (we are told) viewable by other agencies. SAR data in the ISE Shared Spaces is accessible via secure networks by users authorized by the Department of Justice Trusted Broker technology using a federated search tool hosted at www.ncirc.gov

ISE-Suspicious Activity Report (ISE-SAR Report) – An ISE-SAR Report is a Suspicious Activity Report (as defined below) that has been determined by intelligence analysts at the local level to have a potential terrorism nexus. The standard for determining whether a suspicious activity has a potential terrorism nexus is if it is "reasonably indicative" of criminal activity associated with terrorism. "Reasonably indicative" is a vague standard that has not been defined by Congress or the courts, in contrast to the commonly adopted term, "reasonable suspicion." Under rules promulgated by the Office of the Director of National Intelligence (ODNI), a Suspicious Activity Report (SAR) becomes an ISE-SAR Report when the potential terrorism nexus is established and the SAR is shared with the nationwide Information Sharing Environment where multiple agencies can access the information and "look for patterns and trends."

Nationwide Suspicious Activity Reporting Initiative ("SAR Initiative" or NSI) – The Nationwide SAR Initiative is one of several efforts to institutionalize interagency sharing of terrorism-related information. It develops and promotes common standards, architecture, and legal and policy guidance for reporting incidents determined to have a potential nexus to terrorism. This initiative is based on the ISE-SAR Functional Standard established by the Office of the Program Manager for the Information Sharing Environment. The SAR Initiative "establishes a process and a technology infrastructure whereby information can be shared to detect and prevent criminal activity, including that associated with domestic and international terrorism." It is led by the FBI, Global Justice Information Sharing Initiative of the Department of Justice, Department of Homeland Security, Information Sharing Environment, National Sheriff's Association, Major County Sheriff's Association, Department of Defense, International Association of Chiefs of Police, and Major Cities Chiefs of Police Association.

National Criminal Intelligence Sharing Plan (NCISP) – A subtitle of the Homeland Security Act of 2002, called the Homeland Security Information Sharing Act, requires the president to develop new procedures for sharing classified information, as well as unclassified but otherwise sensitive information, with state and local police. This charge was addressed in May 2002 when the International Association of Chiefs of Police, Department of Justice, FBI, Department of Homeland Security, and other law enforcement endorsed the NCISP.

Program Manager for the Information Sharing Environment (PM-ISE) – In 2004, Congress required the President to designate a Program Manager with government-wide authority to manage the Information Sharing Environment (ISE) and establish an Information Sharing Council to advise the President and Program Manager on the development of ISE policies and to ensure coordination among all agencies participating in the ISE. Under the Obama Administration, the Information Sharing Council functions under the auspices of the Executive Office of the President. The acting Program Manager (PM) is Susan B. Reingold, who served as Deputy Program Manager since 2005. However, the SAR Initiative was moved from the PM-ISE to a new Program Management Office housed in the Department of Justice Bureau of Justice Assistance in December 2009, which will be led by Thomas O'Reilly.

Suspicious Activity – Defined by the intelligence community as "observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity."

Suspicious Activity Report (SAR Report) – Official documentation of observed behavior "reasonably indicative" of pre-operational planning related to terrorism or other criminal activity.

Bibliography

Alexander, Col. Blair C. 2005. "Strategies to Integrate America's Local Police Agencies into Domestic Counterterrorism," Strategy Research Paper, U.S. Army War College, 18 March.

Ali, Kazim. 2007. "Culture of Fear: Poetry Professor Becomes Terror Suspect," *New America Media*, 24 April. Online at http://www.alternet.org/rights/50939/ (February 23, 2010).

Ambinder, Marc. 2010. "NCTC Was Slated for Deep Budget Cuts," *The Atlantic*. Online at http://politics.theatlantic.com/2010/01/nctc_was_slated_for_deep_budget_cuts.php (February 23, 2010).

American Civil Liberties Union of Massachusetts. 2005. *Mass Impact*. www.aclum.org/pdf/mass_impact.pdf

Andrea, Elliott. 2006. "After 9/11, Arab-Americans Fear Police Acts, Study Finds," *The New York Times*, 12 June.

Bain, Ben. 2008. "Feds take counterterrorism local," *Federal Computer Weekly*. Online at http://www.kms.ijis.org/traction?type=single&proj=Public&rec=3261&drafts=f (February 23, 2010).

Bain, Ben. 2009. "Stimulus Bill has $250m for Fusion Centers," *Federal Computer Weekly*. Online at http://fcw.com/Articles/2009/02/02/senate-stimulus.aspx (February 23, 2010).

Berkowitz, Bruce. "Homeland Security Intelligence: Rationale, Requirements and Current Status." In *Analyzing Intelligence, Origins, Obstacles, and Innovations* ed. Roger Z. George and James Bruce, 289. Washington D.C.: Georgetown University Press.

Blue Ribbon Rampart Review Panel. *Rampart Reconsidered: The Search for Real Reform Seven Years Later* (2006). http://www.lapdonline.org/assets/pdf/Rampart Reconsidered-Full Report.pdf

Boghosian, Heidi. 2007. "Punishing Protest: Government Tactics That Suppress Free Speech," National Lawyers Guild. Online at: http://www.nationallawyersguild.org/punishing.htm (February 23, 2010).

Bratton, William J. "The Need for Balance." Subject to Debate (April 2006).

Brian Jackson, ed. 2009. *The Challenge of Domestic Intelligence in a Free Society*, 31. New York: RAND Corp., (internal citation omitted). Online at: http://www.rand.org/pubs/monographs/2009/RAND_MG804.pdf

Brooks, Bob. 2010. "Civilian courts no place for terrorists," *Ventura County Star,* 5 January. Online at: http://www.vcstar.com/news/2010/jan/05/civilian-courts-no-place-for-terrorists/ (February 23, 2010)

Bures, Frank. 2001. "City's split: fear for safety vs. fear for rights," *Christian Science Monitor*, 17 October.

Business Executives for National Security, "Untangling the Web: Congressional Oversight and the Department of Homeland Security," A White Paper of the CISS-BENS Task Force on Congressional Oversight (Dec. 2004).

Carter, David L. "Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies," *U.S. Department of Justice, Office of Community Oriented Policing Services*. Online at http://www.scribd.com/doc/24325790/DOJ-Law-Enforcement-Intelligence-Guide-for-State-Local-Tribal-Law-Enforcement-Agences-2d-Ed-May-2009 (February 23, 2010).

Carter, David L., and Jeremy G. Cater. 2009. "Intelligence-Led Policing: Conceptual and Functional Considerations for Public Policy," *Criminal Justice Policy Review,* 20(3), 1 September.

Casey, James. 2004. "Managing Joint Terrorism Task Force Resources," *FBI Law Enforcement Bulletin,* 73:1.

Center for Democracy & Technology. "CDT Analysis of Privacy Guidelines for the Information Sharing Environment for Terrorism Information." www.cdt.org/security/20070205iseanalysis.pdf (February 2, 2007).

Center for Democracy & Technology. 2008. "Investigative Guidelines Cement FBI Roles as Domestic Intelligence Agency, Raising New Privacy Challenges," 29 October. Online at: http://www.cdt.org/policy/investigative-guidelines-cement-fbi-role-domestic-intelligence-agency-raising-new-privacy-cha (February 23, 2010).

Chertoff, Michael. "Remarks at the 2006 Bureau of Justice Assistance," U.S. Department of Justice and SEARCH symposium on Justice and Public Safety Information Sharing. (March 14, 2006).

Cook-Pritt, Jennifer. 2009. Interview of Florida Department of Law Enforcement Agent by PRA Investigator Lisa Ruth, 19 October.

Cope, Nina. 2004. "Intelligence led policing or policing led intelligence?", *British Journal of Criminology* 44:188-203.

Corn, David. 2006. "The 9/11 Investigation," *The Nation*, 4 August.

Council of State Governments. 2006. "The Impact of Terrorism on State Law Enforcement: Adjusting to New Roles and Changing Conditions."

CRS Report for Congress. 1976. "The FBI: Past, Present, Future, at 25; U.S. Senate, United States Select Committee to Study Government Operations, Church Committee Report," Vol. 7, Covert Action, Book II: Intelligence Activities and the Rights of Americans. Washington, D.C.: The Library of Congress, 289.

Dillon, Dana R. 2002. "Breaking Down Intelligence Barriers for Homeland Security," *Heritage Foundation Backgrounder* 1536. Online at http://www.heritage.org/Research/HomelandSecurity/BG1536.cfm (February 23, 2010).

Donner, Frank. 1981. *The Age of Surveillance: The Aims and Methods of America's Political Intelligence System*. New York: Vintage Books.

Donner, Frank. 1990. *Protectors of Privilege: Red Squads and Police Repression in Urban America*. Berkeley and Los Angeles: University of California Press.

Donofrio, Joel. 2008. "Pastor: St. Pius Incident a simple Misunderstanding," *Quad Cities Online*. Online at http://qconline.com/archives/qco/display.php?id=375937 (February 23, 2010).

English, Richard. 2009. *Terrorism: How to Respond*. New York: Oxford University Press.

Federal Bureau of Investigation (FBI). "Strategic Plan 2004-2009," p. 19. Retrieved from http://www.fbi.gov/publications/strategicplan/strategicplanfull.pdf (February 23, 2010).

Federal Bureau of Investigation, Press Room. 2008. "Connecting the Dots: Using New FBI Technology." Available at http://www.fbi.gov/page2/sept08/eguardian_091908.html (February 23, 2010).

Fein, Bruce. 2009. "Statement before the Subcommittee on Intelligence Sharing & Terrorism Risk Assessment Committee on Homeland Security," 1 April. Online at: http://www.afterdowningstreet.org/node/41360 (February 23, 2010).

Fitzgerald, Paul. 2009. Interview with Deputy Superintendent of Boston Regional Intelligence Center conducted by PRA Investigator Andrea Simakis, 30 May.

Fredrickson, Caroline. 2009. "Statement before the Senate Committee on the Judiciary," 1 April. Online at: www.**aclu.org**/files/images/asset_upload_file33_39415.pdf (March 15, 2010).

Fuller, John Randolph. 2009. *Criminal Justice: Mainstream and Crosscurrents*. New Jersey: Prentice Hall.

George, Roger Z. and James Bruce, Eds. 2008. *Analyzing Intelligence: Origins, Obstacles, and Innovations*. Washington, D.C.: George Washington Press.

German, Michael and Jay Stanley. 2007. "What's Wrong With Fusion Centers," ACLU. Online at http://www.aclu.org/technology-and-liberty/whats-wrong-fusion-centers-executive-summary> (February 23, 2010).

Hass, Jeffrey. 2009. *The Assassination of Fred Hampton: How the FBI and Chicago Police Murdered a Black Panther*. Chicago: Lawrence Hill Books.

Hess, Karen M. 2008. *Introduction to Law Enforcement and Criminal Justice*. Kentucky: Cengage Learning.

Heymann, Philip B., and Juliette Kayyem. 2005. *Protecting Liberty in an Age of Terror*. Cambridge: MIT Press.

Hsu, Spencer, and Johnson, Carrie, "Documents Show DHS Improperly Spied on Nation of Islam in 2007," *Washington Post*, 17 December, A09.

Hylton, Hilary. 2010. "Fusion Centers: Giving Cops Too Much Information?", *TIME Magazine*, 9 March. Online at http://www.time.com/time/nation/article/0,8599,1883101,00.html (February 23, 2010).

Information Sharing Environment, Program Manager. 2008. "Federal Segment Architecture Methodology (FSAM) Case Study: Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Evaluation Environment (EE)," 9 December.

Information Sharing Environment, Program Manager. 2008. "Information Sharing Environment (ISE) Functional Standards, Suspicious Activity Reporting (SAR), ISE-FS-200," January.

Information Sharing Environment, Program Manager. 2008. "National Suspicious Activity Reporting Initiative Concept of Operations, Version 1," December. Online at: http://www.ise.gov/pages/sar-initiative.aspx. (February 23, 2010).

Information Sharing Environment, Program Manager. 2009. "Fact Sheet: Update to Suspicious Activity Reporting Functional Standard Provides Greater Privacy and Civil Liberties Protections."

Information Sharing Environment, Program Manager. 2009. "Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5," May. Online at http://www.ise.gov/docs/ctiss/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf (February 23, 2010).

Information Sharing Environment, Program Manager. 2009. "Progress and Plans Annual Report to the Congress," June, Appendix B, p. 52.

Information Sharing Environment, Program Manger. 2008. "Initial Privacy and Civil Liberties Analysis," September 2008. Online at: http://www.ise.gov/pages/sar-initiative.aspx (February 23, 2010).

Information Sharing Environment. "Interagency Threat Assessment and Coordination Group." http://www.ise.gov/pages/partner-itacg.html (February 23, 2010).

Information Sharing Environment. 2008. "Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project." Online at http://www.ise.gov/pages/sar-initiative.aspx (February 23, 2010).

International Association of Chiefs of Police. 2002. "IACP Criminal Intelligence Sharing Report." Washington, D.C.: IACP.

Johnson, Kevin. 2005. "FBI Gets Local Police in the Loop," *USA Today*, 2 August. Online at http://www.usatoday.com/news/nation/2005-08-01-dc-fbi-information-sharing_x.htm (February 23, 2010).

Kaplan, David E., Monica M. Ekman, and Angie C. Marek. 2006. "Spies Among Us: Despite a troubled history, police across the nation are keeping tabs on ordinary Americans," *US News & World Report*, 8 May.

LaPlante, Matthew D. 2009. "Vast spy data center in Salt Lake City – too much stuff to digest?", *Salt Lake City Tribune*, 23 October.

Lombardi, Kristen. 2004. "Idling while Brown," *Boston Phoenix*, September 3-9. Online at http://www.bostonphoenix.com/boston/news_fe atures/other_stories/multipage/documents/04097838.asp (February 23, 2010).

Loyka, Stephan A.; Faggiani, Donald A.; and Karchmer, Clifford. 2005. "Protecting Your Community from Terrorism: Strategies for Local Law Enforcement," *Volume 4: The Production and Sharing of Intelligence*. Washington, D.C.: Community Oriented Policing Services and the Police Executive Research Forum.

Markle Task Force on National Security. 2002. "Protecting America's Freedom in the Information Age," October. Online at http://markletaskforce.org/ (February 23, 2010).

Markowitz, Michael W. and Jones-Brown, Delores D. 2000. *The System in Black and White*. Westport, CT: Praeger Publishers.

Martin, Kate. 2004. "Domestic Intelligence and Civil Liberties," *SAIS Review,* Winter/Spring Issue.

McNamara, Joan T. 2009. "Suspicious Activity Reporting, Testimony of the Subcommittee on the Intelligence, Information Sharing and Terrorism Risk Assessment, U.S. House of Representatives." Online at www.fas.org/irp/congress/2009_hr/031809mcnamara.pdf (February 23, 2010).

Miller, Jason. 2009. "TSC growing in role as information sharing bridge," *Federal News Radio*. Online at http://www.federalnewsradio.com/index.php?nid=110&sid=1692926 (February 23, 2010).

Murphy, John. 2009. Interview of Intelligence Manager for the Broward County Sheriff's Office conducted by PRA Investigator Lisa Ruth, 17 September.

O'Harrow, Robert. 2006. *No Place to Hide*. New York: Free Press.

O'Harrow, Robert. 2008. "Centers Tap into Databases: State Groups Were Informed After 9/11," *Washington Post*, 2 April.

Office of Justice Programs, Department of Justice Bureau of Justice Assistance. 2005. "Intelligence-Led Policing: The New Intelligence Architecture," September.

Office of the Inspector General. 2007. "Follow-Up Audit of the Terrorist Screening Center," Audit Report 07-41, September.
Online at:
http://www.justice.gov/oig/reports/FBI/a0741/final.pdf

Office of the Inspector General. 2008. "The Federal Bureau of Investigation's Terrorist Threat and Suspicious Incident Tracking System," Audit Report 09-02, November.

Office of the Inspector General. 2008. "The Federal Bureau of Investigation's Terrorist Threat and Suspicious Incident Tracking System." Audit Report 09-02, November.
Online at
http://www.justice.gov/oig/reports/FBI/a0902/exec.htm

Peterson, Marilyn. 2005. "Intelligence-Led Policing: The New Intelligence Architecture," NCJ 210681. Washington, D.C.: U.S. Department of Justice, Bureau of Justice Assistance.

PR Newswire. 2009. "Presidential Task Force on Controlled Unclassified Information Releases Report and Recommendations," *PR Newswire*, 15 December. Online at: http://www.prnewswire.com/news-releases/presidential-task-force-on-controlled-unclassified-information-releases-report-and-recommendations-79312237.html. (February 23, 2010).

Pusey, Allen. 2007. "Every Terrorism Case Since 9/11," *ABA Journal*, September, p. 16.

Randol, Mark A. 2009. "Terrorism Information Sharing and Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress," *Congressional Research Service*.
Online at
http://assets.opencrs.com/rpts/R40901_20091105.pdf (February 23, 2010).

Relyea, Harold C. 2008. "Privacy and Civil Liberties Oversight Board: New Independent Agency Status," *CRS Report for Congress,* 20 February. Online at: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA477136

Ridgeway, Greg. RAND Corporation. 2007. *New York: Analysis of Racial Disparities in New York City Police Department's Stop and Frisk Practices*.
http://www.rand.org/pubs/research_briefs/RB9325/index1.html

Robert S. Mueller, III, Director, Federal Bureau of Investigation, 2005. "Testimony Before the

Senate Committee on Intelligence of the U.S. Senate," 16 February.

Ronczkowski, Major Michael R. 2007. "Prepared Statement of Testimony before the Committee on Homeland Security and Governmental Affairs," U.S. Senate, 30 October.

Sanchez, Phillip L. 2009. "Increasing Information Sharing Among Independent Police Departments," Thesis for Naval Postgraduate School, March.

Sather, Katherine. 2004. "Photo Student Draws Attention of Authorities," *Seattle Times*, 14 July. Online at http://seattletimes.nwsource.com/html/localnews/2001979027_locks14m.html (February 23, 2010).

Savage, Charlie and Scott Shane. 2009. "Intelligence Improperly Collected on U.S. Citizens," *New York Times*, 17 December.

Savelli, Lou. 2004. *A Proactive Law Enforcement Guide for the War on Terrorism*. New York: Looseleaf Law Publications.

Schmitt, Eric. 2009. "Surveillance Effort Draws Civil Liberties Concern," *New York Times*, 28 April. Online at http://www.nytimes.com/2009/04/29/us/29surveil.html?pagewanted=all (February 23, 2010).

Schulz, G.W. 2008. "Homeland Security Pays Dividends for Alaska," *Truthdig*, 31 October. Online at http://centerforinvestigativereporting.org/articles/homelandsecuritypaysdividendsforalaska (February 23, 2010).

Schulz, G.W. 2009. "Assessing RNC Police Tactics," *Minnpost.com*, 1 September. Online at http://www.centerforinvestigativereporting.org/articles/assessingrncpolicetacticspart1of2 (February 23, 2010).

Serrao, Stephen G. 2009. "Suspicious Activity Reporting," *Lawofficer.com*. Online at http://www.lawofficer.com/news-and-articles/articles/online/2009/serrao_suspicious_activity_reporting.html (February 23, 2010).

Siegel, Larry J. 2008. *Essentials of Criminal Justice*. Kentucky: Wadsworth Publishing.

Singel, Ryan. 2009. "Newly Declassified Files Detail Massive Data Mining Project," *Wired*, 23 September, online edition.

Smith, Rogers M. 2005. "Civil Liberties in the Brave New World of Antiterrorism," *Radical History Review* 93:170-185.

Solomon, John, and Ellen Nakashima. 2007. "White House Edits to Privacy Board's Report Spur Resignation," *Washington Post*, 15 May.

Stanley, Jay. 2009. "Enforcing Privacy: Building American Institutions to Protect Privacy in the Face of New Technology and Government Powers," ACLU. Online at http://www.aclu.org/technology-and-liberty/enforcing-privacy-building-american-institutions-protect-privacy-face-new-tec (February 23, 2010).

Stedman, John C., Lt., Los Angeles County Sheriff's Department. 2005. "Counterfeit Goods: Easy Cash for Criminals and Terrorists," Testimony to the U.S. Senate Committee on Homeland Security and Government Affairs,25 May.

Straw, Joseph. 2009. "Connecting the Dots, Protecting Rights," *Security Management*. Online at http://www.securitymanagement.com/article/connecting-dots-protecting-rights-005945 (February 23, 2010).

Treverton, Gregory F. 2008. "Reorganizing U.S. Domestic Intelligence: Assessing the Options," *RAND Corporation*. Online at http://www.rand.org/pubs/monographs/MG767/ (February 23, 2010).

Tu, Janet I. 2008. "Does Course on Islam Give Law Enforcers Wrong Idea?" *Seattle Times.* (May 26, 2008).

U.S. Department of Homeland Security, Directorate of Information Analysis and Infrastructure Protection (IAIP). "Homeland Security Operations Morning Briefings from September 27, 2004 - January 14, 2005." Online at: http://cryptome.org/hsomb/hsomb.htm.

U.S. Department of Homeland Security. "DHS Secretary Napolitano, Missouri Governor Nixon Address Annual National Fusion Center Conference," Online at http://www.dhs.gov/ynews/releases/pr_1236792314990.shtm (February 23, 2010).

U.S. Department of Justice, Bureau of Justice Statistics. 2008. "Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI): NIEM Standards in Action." Online at http://www.niem.gov/request/SARInitiativeNSI.pdf (February 23, 2010).

U.S. Department of Justice, Office of Justice Programs. "199 Revision and Commentary to 28 CFR Part 23 on Sept. 16, 1993." Online at: www.iir.com/28cfr/pdf/1993RevisionCommentary_28CFRPart23.pdf (February 23, 2010).

U.S. Department of Justice. "Fact Sheet: Terrorist Screening Center." Online at: http://www.fbi.gov/pressrel/pressrel03/tscfactsheet091603.htm (February 23, 2010).

U.S. Department of Justice. 2004. "Law Enforcement: A Guide for State, Local, and Tribal Law Enforcement Agencies." Washington, D.C.: Office of Community Oriented Policing Services.

U.S. Department of Justice. 2006. "Fusion Center Guidelines, Executive Summary," Online at http://www.fas.org/irp/agency/ise/guidelines.pdf (February 23, 2010).

U.S. Government Accountability Office. 2007. "Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information-Sharing Initiatives." Online at: www.gao.gov/new.items/d07455.pdf (February 23, 2010).

U.S. National Commission on Terrorist Attacks Upon the United States. 2004. "Final Report of the National Commission on Terrorist Attacks Upon the United States (The 9/11 Commission Report)." Washington, D.C.: GPO.

Voegtlin, Gene. 2005. "From Hometown Security to Homeland Security: IACP's Principles for a Locally Designed and Nationally Coordinated Homeland Security Strategy." International Association of Chiefs of Police White Paper, 27 July. Online at: http://www.theiacp.org/PublicationsGuides/TopicalIndex/tabid/216/Default.aspx?id=624&v=1

Washington Post Editorial Board. 2002. "What is Operations TIPS?" *Washington Post,* 13 July.

Webb, Maureen. 2007. *Illusions of Security: Global Surveillance and Democracy in the Post-9/11 World*. San Francisco: City Lights.

Webster, Stephen. 2009. "Fusion center declares nation's oldest universities a possible threat," *The Raw Story*, 6 April. Online at http://rawstory.com/news/2008/Virginia_terror_assess-ment_targets_enormous_crosssection_0406.html (February 23, 2010).

Wyllie, Doug. 2009. "American cops are force multipliers in counterterrorism," *PoliceOne.com*. Online at http://www.policeone.com/columnists/doug-wyllie/articles/1816539-technology-isnt-the-biggest-problem-for-information-sharing-in-le/ (February 23, 2010).

Wyllie, Doug. 2009. "Technology isn't the (biggest) problem for information sharing in law enforcement," *PoliceOne.com*. Online at http://www.policeone.com/columnists/doug-wyllie/articles/1816539-technology-isnt-the-biggest-problem-for-information-sharing-in-le/ (February 23, 2010).

Endnotes

[1] The Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) mandates the creation of a "decentralized, distributed, and coordinated [information sharing] environment . . . with 'applicable legal standards relating to privacy and civil liberties.'"

[2] See Gregory F. Treverton, *Reorganizing U.S. Domestic Intelligence: Assessing the Options* (RAND Corporation: 2008), p. 112.

[3] See Treverton, *Reorganizing U.S. Domestic Intelligence*, p. 112.

[4] Rogers M. Smith, "Civil Liberties in the Brave New World of Antiterrorism," *Radical History Review* Issue 93 (Fall 2005), p. 173. For a visual presentation of this vast matrix, see Gregory F. Treverton, *Reorganizing U.S. Domestic Intelligence: Assessing the Options* (RAND Corporation: 2008) http://www.rand.org/pubs/monographs/MG804/

[5] Karen M. Hess, *Introduction to Law Enforcement and Criminal* Justice. Ninth Edition. (Jan. 2008), p. 376. These include: 1) the presidentially appointed Information Sharing Council, 2) a Joint Intelligence Community Council (consisting of the Director of National Intelligence and the secretaries of State, Treasury, Defense, Energy and Homeland Security, along with the Attorney General, 3) a Homeland Security Council that includes the Secretary of Defense, Director of Homeland Security, and the Attorney General, and 4) the National Counter-terrorism Center, a central integrating institution in charge of analyzing threats and planning antiterrorism operations. The Director of Central Intelligence defines national intelligence needs under the guidance of the President and National and Homeland Security Advisors. The Attorney General and the Director of the FBI also participate in formulating these requirements.

[6] In response to the 9/11 Commission's report, Congress created a new director of national intelligence (DNI) with broad budgetary and personnel authority to serve as the principal intelligence advisor to the president and manage sixteen intelligence agencies. The DNI's duties include establishing objectives and priorities for the collection, analysis, production, and dissemination of national intelligence.

[7] President Bush previously signed Executive Order 13228 establishing the Department of Homeland Security on October 8, 2001.

[8] J. Randolph Fuller, *Criminal Justice: Mainstream and Crosscurrents*. Second Edition. (Prentice Hall: 2009), p. 543. The author speculates that DHS did not include CIA and FBI because they could have lost their authority to decide how best to deploy their resources. Another reason is political. These are mature agencies that, over the years, have developed networks with politicians, a large number of loyal alumni, and their own organizational culture. Placing them under DHS would have required more of a political battle than was desired after September 11, 2001. Others have argued that the Bush administration did not want to create a national intelligence agency. See, e.g., Bruce Berkowitz, "Homeland Security Intelligence: Rationale, Requirements and Current Status," in *Analyzing Intelligence*, Roger Z. George and James Bruce, Eds. (George Washington Press: 2008), pp. 289-291.

[9] U.S. Department of Homeland Security, "DHS Secretary Napolitano, Missouri Governor Nixon Address Annual National Fusion Center Conference," (March 11, 2009). See also, Ben Bain, "Stimulus Bill has $250m for Fusion Centers," *Federal Computer Week* (Feb. 2, 2009). Available at: http://fcw.com/Articles/2009/02/02/senate-stimulus.aspx

[10] Hess, p. 373.

[11] Federal guidance recommends that Fusion Centers obtain access to at least seventeen available networks that provide homeland security, terrorism-related, or law enforcement information. These networks cost taxpayers $830.5 million to develop, operate, and maintain in fiscal years 2005 and 2006. U.S. Government Accountability Office, *Information Technology: Numerous Federal Networks Used to Support Homeland Security Need to Be*

Better Coordinated with Key State and Local Information-Sharing Initiatives (GAO-07-455) (April 2007), p. 2.

[12] Federal guidance recommends that Fusion Centers obtain access to at least seventeen available system and network resources that provide homeland security, terrorism-related, or law enforcement information. These networks cost taxpayers $830.5 million to develop, operate, and maintain in fiscal years 2005 and 2006. U.S. Government Accountability Office, *Information Technology: Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information-Sharing Initiatives* (GAO-07-455) (April 2007), p. 2.

[13] Hilary Hylton, "Fusion Centers: Giving Cops Too Much Information?" *Time* (March 9, 2009). Available at: http://www.time.com/time/nation/article/0,8599,1883101,00.html

[14] The National Guard is prohibited from performing domestic intelligence by the Posse Comitatus Act. However, the Guard participates in Fusion Centers under an exception for drug interdiction activity. The precise manner of how the Guard's role in Fusion Centers is limited to that arena is not fully explained in current literature. For a copy of the Guard's Memorandum of Agreement with the Massachusetts Commonwealth Fusion Center, obtained by the ACLU of Massachusetts, see: www.stopspying.us/wiki.

[15] Hess, p. 371

[16] Hess, p. 371, citing Shane, Scott and Bergman, Lowell, "FBI Struggles to Reinvent Itself to Fight Terror," *The New York Times* (October 10, 2006).

[17] For example, the National Threat Center Section (NTCS) in the FBI's Counter-terrorism Division is the focal point for all threat information, preliminary analysis, and assignment for immediate action of all emerging International Terrorism and Domestic Terrorism threats incoming to the FBI. Within NTCS, the Threat Monitoring Unit (TMU) has primary responsibility for supporting the FBI's role in defending the United States against terrorism threats. Through coordination with FBI Field Offices, the TMU collects, assesses, disseminates, and memorializes all threat information collected or received by the FBI. See: http://foia.fbi.gov/eguardian_threat.htm

[18] Trevorton, op cit, p. 9.

[19] See: Department of Justice, *Fact Sheet, Terrorist Screening Center*; see also Office of the Inspector General, *Follow-Up Audit of the Terrorist Screening Center*, Audit Report 07-41 (September 2007), for an explanation of TSC processes and how it relates to the NCTC.

[20] Jason Miller, "TSC growing in role as information sharing bridge," *Federal News Radio* (June 9, 2009). http://www.federalnewsradio.com/index.php?nid=110&sid=1692926

[21] JTTFs fall under the auspices of the FBI Counterterrorism Division (CTD) and the FBI's National Security Bureau. The task forces coordinate their efforts largely through the interagency National Joint Terrorism Task Force (NJTTF), established in 2002, which operates out of the National Counter Terrorism Center (NCTC).

[22] By comparison, domestic intelligence agencies in Canada, Australia, and England do not have the power to make arrests.

[23] James Casey, "Managing Joint Terrorism Task Force Resources," *FBI Law Enforcement Bulletin*, v. 73, no. 1 (2004), p. 1.

[24] Hess, p. 371, quoting Federal Bureau of Investigation (FBI), *Strategic Plan 2004-2009*, p. 19. http://www.fbi.gov/publications/strategicplan/strategicplanfull.pdf

[25] See Center for Democracy & Technology, *Investigative Guidelines Cement FBI Roles as Domestic Intelligence Agency, Raising New Privacy Challenges* (October 29, 2008). http://www.cdt.org/policy/investigative-guidelines-cement-fbi-role-domestic-intelligence-agency-raising-new-privacy-cha

[26] The City of Portland withdrew (and later re-established) its participation in the FBI's JTTF because it could not monitor whether local officers participating in the agency would abide by state law prohibiting the monitoring of free speech activity without reasonable suspicion. Anderson, Jennifer, "New Council Inherits Task Force Decision," *Portland Tribune* (Dec. 21, 2004); Bures, Frank, "City's split: fear for safety vs. fear for rights," *Christian Science Monitor* (Oct. 17, 2001). http://www.portlandcopwatch.org/PPR28/pjttfppr28.html

[27] For a listing of JTTF activities directed at political activists, see the website of the Bill of Rights Defense Committee: http://www.bordc.org/resources/jttf-activities.php See also Frank Donner, *The Age of Surveillance: The Aims & Methods of America's Political Intelligence System,* (New York: Vintage Books, 1981). Civil liberties lawyer and historian Frank Donner argued, on the topic of political repression, that the unstated yet actual primary goal of surveillance and political intelligence gathering by government law enforcement agencies and their private allies is not amassing evidence of illegal activity for criminal prosecutions, but punishing critics of the *status quo* or the state in order to undermine dissident movements for social change.

In Colorado, evidence emerged that Denver police assigned to a JTTF monitored local human rights groups. In response to a lawsuit, Denver police adopted a new policy 2001 forbidding surveillance based on political views. Yet, after Denver instituted this policy, the local JTTF apparently continued the spying. Printouts made in April 2002 by the Denver Intelligence Unit contained a JTTF "Active Case List" with material from the Colorado Campaign for Middle East Peace, AFSC, Rocky Mountain Independent Media Center, and the Human Bean Company. For more see ACLU Colorado: http://www.aclu-co.org/docket/200406/200406_description.htm

[28] Trevorton, op cit, p. 52, 57. In August 2004, the National Counter Terrorism Center absorbed the Terrorist Threat Integration Center that had been created in May 2003 but never made fully operational. Although DHS has the legal mandate for assembling counter-terrorism intelligence, the NCTC has taken that role in practice. The federal Interagency Threat Assessment and Coordination group (ITAGC) is also integrated into the NCTC, where it supports the efforts of the NCTC to produce "federally coordinated" intelligence reports on terrorism threats to help improve sharing with state, local and private sector individuals. *Information Sharing Environment: Interagency Threat Assessment and Coordination Group*. http://www.ise.gov/pages/partner-itacg.html (accessed on January 5, 2010).

[29] Marc M. Binder, "NCTC Was Slated for Deep Budget Cuts," *The Atlantic* (Jan. 5, 2010). http://politics.theatlantic.com/mt-42/mt-tb.cgi/19682

[30] David E. Kaplan, Monica M. Ekman, Angie C. Marek, "Spies Among Us: Despite a troubled history, police across the nation are keeping tabs on ordinary Americans," *US News & World Report*, (May 8, 2006), p. 40.

[31] Larry J. Siegel, Essentials of Criminal Justice (Sixth Ed.), p. 111.

[32] Trevorton, ob cit, p. 67.

[33] Siegel, p. 115.

[34] ACLU, *Enforcing Privacy: Building American Institutions to Protect Privacy in the Fact of New Technology and Government Powers* (November 2009), pp. 4-5. See also, Harold C. Relyea, "Privacy and Civil Liberties Oversight Board: New Independent Agency Status," *CRS Report for Congress* (Feb. 20, 2008).

[35] U.S. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington, DC: GPO, 2004), p. 395.

[36] See, e.g., John Solomon and Ellen Nakashima, "White House Edits to Privacy Board's Report Spur Resignation," *Washington Post* (May 15, 2007), p. A5. http://washingtonpost.comwp-dyn/content/article/2007/05/14/AR2007051402198_pf.html

[37] ACLU, "Enforcing Privacy," p. 13.

[38] Kevin Johnson, "FBI Gets Local Police in the Loop." *USA Today* (Aug. 2, 2005). http://www.usatoday.com/news/nation/2005-08-01-dc-fbi-information-sharing_x.htm

[39] Robert O'Harrow, "Centers Tap into Databases: State Groups Were Informed After 9/11." *Washington Post* (April 2, 2008). http://www.washingtonpost.com/wp-dyn/content/article/2008/04/01/AR2008040103049.html

[40] Paul Fitzgerald, Deputy Superintendent of Boston Regional Intelligence Center. Interview by PRA Investigator Andrea Simakis (May 30, 2009).

[41] Doug Wyllie, *Technology isn't the (biggest) problem for information sharing in law enforcement*, PoliceOne.com (April 30, 2009). http://www.policeone.com/columnists/doug-wyllie/articles/1816539-technology-isnt-the-biggest-problem-for-information-sharing-in-le/

[42] Dana R. Dillon, "Breaking Down Intelligence Barriers for Homeland Security," *Heritage Foundation Backgrounder #1536* (April 10, 2002) (emphasis added). http://www.heritage.org/Research/HomelandSecurity/BG1536.cfm

[43] United States Coast Guard, "America's Waterway Watch." http://www.americaswaterwaywatch.us/

[44] "Three wise boaters to Report Hearing, Seeing or Speaking Evil," *Shiptalk Newsletter* (April 2006). http://www.shiptalk.com/newsletters_06/april_06_text_only.html.

[45] Joseph Straw, "Smashing Intelligence Stovepipes," Security Management (March 2008), retrieved from http://www.securitymanagement.com/print/3708.

[46] "Police: 3 Men 'Suspiciously' Videotaping At Santa Monica Pier." http://prisonplanet.com/Pages/Aug05/110805suspicious.htm

[47] Boston Police Department Rules and Procedures, "Field Interrogation, Observation, Frisk, and/or Search Report, Rule 323, § 5 (June 3, 2005).

[48] Ibid.

[49] Information Sharing Environment, Program Manager, National Suspicious Activity Reporting Initiative Concept of Operations, Version 1 (December 2008), p. 12. http://www.ise.gov/pages/sar-initiative.aspx. (February 23, 2010), p. 12.

[50] Responsibility for coordinating the initiative will move from the Program Manager of the Information Sharing Environment to the new Program Management Office that will be staffed by a variety of ISE participants and stakeholders.

[51] See Philip B. Heymann and Juliette Kayyem, *Protecting Liberty in an Age of Terror* (MIT Press: 2005).

[52] Mark A. Randol, Congressional Research Service. *Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress*. (November 5, 2009), p. 2. http://assets.opencrs.com/rpts/R40901_20091105.pdf

[53] Randol, p.2, citing Markle Task Force on National Security, *Protecting America's Freedom in the Information Age* (October 2002), p. 28. http://markletaskforce.org/ See also, Robert O'Harrow, *No Place to Hide* (New York, Free Press: 2006), pp. 99-102.

[54] Ibid.

[55] Mark A. Randol, Congressional Research Service. *Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress*. (November 5, 2009), pp. 2, 6.

[56] Colleen Rowley. Interview with PRA Investigator Mary Fischer, September 2009.

[57] National Research Council of the National Academies. *Protecting Individual Privacy in the Struggle Against Terrorists*. Washington, D.C.: National Academies Press (2008), pp. 3-4. This report was prepared a committee of 21 people with a broad range of expertise in scientific, government, and private sector communities and co-chaired by former Defense Secretary William J. Perry and Charles M. Vest of the National Academy of Engineering. The nonpartisan committee also found no scientific consensus on whether behavioral surveillance techniques are ready for use at all in counter-terrorism; at most they should be used for preliminary screening, to identify those who merit follow-up investigation. Further, they have enormous potential for privacy violations because they will inevitably force targeted individuals to explain and justify their mental and emotional states.

[58] Ibid.

[59] See Thomas Cincotta, "Intelligence Fusion Centers: A De-Centralized National Intelligence Agency," *The Public Eye* (Winter 09/Spring 10), Sidebar ("Torrance: A Genesis Fable for Fusion"). http://www.publiceye.org/magazine/v24n4/intelligence-fusion-centers.html

[60] In Chicago alone, the local police intelligence unit amassed files on over 200,000 citizens and groups ranging from the PTA to the Communist Party. Chip Berlet, Political Research Associates, "Government Surveillance: Not a track record to boast about." http://www.publiceye.org/media/privacy_online_85/Privacy_PC-08.html See also Frank Donner, *Protectors of Privilege: Red Squads and Police Repression in Urban America* (Berkeley and Los Angeles: University of California Press, 1990), pp. 47, 143, 205-06.

[61] Gene Voegtlin. "From Hometown Security to Homeland Security: IACP's Principles for a Locally Designed and Nationally Coordinated Homeland Security Strategy." International Association of Chiefs of Police white paper, July 27, 2005. http://www.theiacp.org/PublicationsGuides/TopicalIndex/tabid/216/Default.aspx?id=624&v=1

[62] Joan T. McNamara, "Suspicious Activity Reporting," *Testimony of the Subcommittee on the Intelligence, Information Sharing and Terrorism Risk Assessment, U.S. House of Representatives* (March 18, 2009). www.fas.org/irp/congress/2009_hr/031809mcnamara.pdf

[63] William J. Bratton. "The Need for Balance." *Subject to Debate* (April 2006), p. 2.

[64] Hess, op cit, p. 378. "The keys to combating terrorism lie with the local police and the intelligence they can provide to federal authorities, how readily information is shared between agencies at different levels, and the interoperability of communications systems should an attack occur."

[65] Richard English, *Terrorism: How to Respond* (New York, Oxford University Press: 2009), pp. 89-117.

[66] Randolph Fuller, p. 541

[67] *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project.* (June 2008), p.2. http://www.ise.gov/pages/sar-initiative.aspx

[68] Paul Fitzgerald, Deputy Superintendent of Boston Regional Intelligence Center. Interview by PRA Investigator Andrea Simakis (May 30, 2009).

[69] Hess, pp. 387, 389, *citing* Stephan A. Loyka; Donald A. Faggiani; and Clifford Karchmer, *Protecting Your Community from Terrorism: Strategies for Local Law Enforcement. Volume 4: The Production and Sharing of Intelligence.* (Washington, DC: Community Oriented Policing Services and the Police Executive Research Forum, February 2005), p. 7. See also, John C. Stedman, Lt., Los Angeles County Sheriff's Department, "Counterfeit Goods: Easy Cash for Criminals and Terrorists," *Testimony to the U.S. Senate Committee on Homeland Security and Government Affairs* (May 25, 2005), explaining how detectives served a search warrant at a clothing store in Los Angeles County. During the course of the search, thousands of dollars in counterfeit clothing were recovered as were two unregistered firearms. The suspect was later found to have a tattoo of the Hezbollah flag on his arm. Also in 2004, detectives served a multi-location search warrant. During the course of the investigation, detectives located a photo album with dozens of pictures of attendees at a fundraising event for the Holy Land Foundation, an alleged "terrorist funding operation" that largely served charities in the Middle East.

[70] Council of State Governments*, The Impact of Terrorism on State Law Enforcement: Adjusting to New Roles and Changing Conditions* (Dec. 2006), pp. 27-28.

[71] Randol, p.6, quoting U.S. Congress, House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, *A Report Card on Homeland Security Information Sharing*, Statement of John McKay, Former U.S. Attorney for the Western District of Washington, 110th Cong., 2nd sess., September 24, 2008. Local police also stopped two other September 11 hijackers – Mohammed Atta and Ziad Samir Jarrah. Like Hanjoor, both were in violation of their immigration status. Ziad Jarrah, hijacker of the plane that crashed in Shanksville, Pennsylvania, was stopped by police in Maryland for speeding. He was driving 90 mph in a 65 mph zone. He was issued a ticket and released. An officer pulled Mohammed Atta over for speeding in Florida. This officer was not aware that Atta had an outstanding arrest warrant for failing to pay a ticket in Tamarac, Florida for driving without a valid license. Four months later, he hijacked and piloted the plane that crashed into the north tower of the World Trade Center.

[72] Lou Savelli, *A Proactive Law Enforcement Guide for the War on Terrorism*. (Flushing, NY: Looseleaf Law Publications, 2004), p. 65.

[73] Major Michael R. Ronczkowski, Prepared Statement of Testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate (October 30, 2007), p. 4.

[74] Local police came face-to-face with three of the September 11 hijackers before the attack. Hani Hanjoor hijacked and piloted Flight 77 and crashed it into the Pentagon, killing 289 persons. Six weeks prior, Hanjoor was issued a speeding ticket by Arlington, Virginia police for speeding and released. He paid the ticket so he would not have to show up in court.

[75] *IACP Criminal Intelligence Sharing Report* (Washington DC: IACP, August 2002) pp. 12-16. The NCISP was born at the Criminal Intelligence Sharing summit organized by the International Association of Chiefs of Police (IACP) in March 2002. The IACP brought together law enforcement executives and intelligence experts from across the U.S. to explore their own intelligence sharing initiatives. *IACP Criminal Intelligence Sharing Report* (Washington DC: IACP, August 2002) p. 1. The Global Justice Information Sharing Initiative (Global), a formal advisory group funded by the Office of Justice Programs of the Department of Justice, was already in existence with the charge of developing standards to better share information across the criminal justice system. Based on these IACP recommendations and funded by the Department of Justice, Global created a new subgroup, the Global Intelligence Working Group (GIWG) in December 2002 to write the National Criminal Intelligence Sharing Plan.[75] GIWG met quarterly during 2003 and developed the NCISP, which was released and approved by the U.S. Attorney General in October 2003.

[76] David L. Carter, Jeremy G. Carter. "Intelligence-Led Policing: Conceptual and Functional Considerations for Public Policy*," Criminal Justice Policy Review* (September 2009), p. 315. See the action steps of the Information Sharing Environment Implementation Plan (Retrieved October 24, 2008). http://www.ise.gov/docs/ISE-impplan-200611.pdf

[77] U.S. Department of Justice, Bureau of Justice Assistance, *National Criminal Intelligence Sharing Plan* (October 2003). http://it.ojp.gov/documents/National_Criminal_Intelligence_Sharing_Plan.pdf

[78] Ameena Mirza Qazi, correspondence with the author, January 14, 2010.

[79] J.H. Ratcliffe, *What is intelligence-led policing*. Retrieved December 20, 2009 from http://jratcliffe.net/ilp/index.htm

[80] Ibid.

[81] David L. Carter, Jeremy G. Carter. "Intelligence-Led Policing: Conceptual and Functional Considerations for Public Policy*," Criminal Justice Policy Review* (September 2009), p. 316. This concept is currently in use by police agencies in the United Kingdom, Australia, New Zealand, and Norway – countries that do not have the constitutional protections of the First, Fourth, and Fifth Amendments to the U.S. Constitution. The UK fully implemented intelligence led policing in 2000.

[82] Col. Blair C. Alexander. *Strategies to Integrate America's Local Police Agencies into Domestic Counterterrorism*. Strategy Research Paper, U.S. Army War College (March 18, 2005), p. 25. Requiring local police agencies to take on the time consuming and expensive task of intelligence-led policing could result in performance shortfalls in preventing both traditional crime and terrorism, while simultaneously jeopardizing civil liberties.

[83] Ronczkowski, p. 4.

[84] The Office of Justice Programs' Core Criminal Intelligence Training Standards call for only forty hours of training for analysts or intelligence officers.

[85] Janet I. Tu, "Does Course on Islam Give law Enforcers Wrong Idea?" *Seattle Times*, May 26, 2008. See also, Profile of Solomon Bradman, SSI CEO, Right Web (March 23, 2010). http://www.rightweb.irc-online.org/profile/bradman_solomon

[86] ACLU, "Fusion Center Encourages Improper Investigations of Lobbying Groups and Anti-War Activists," *ACLU* (Feb. 25, 2009). http://www.aclu.org/technology-and-liberty/fusion-center-encourages-improper-investigations-

lobbying-groups-and-anti-war For a useful leaflet describing a variety of domestic surveillance violations by the FBI, police, and Fusion Centers, see: http://aclum.org/sos/aclu_domestic_surveillance_what_we_know.pdf

[87] ACLU, "Fusion center encourages improper investigations of lobbying groups and anti-war activists" (February 25, 2009). *http://www.commondreams.org/newswire/2009/02/26*

[88] *See* Stephen Webster, "Fusion center declares nation's oldest universities possible threat," *The Raw Story* (April 6, 2009). *http://rawstory.com/news/2008/Virginia_terror_assessment_targets_enormous_crosssection_0406.html*

[89] Charlie Savage and Scott Shane, "Intelligence Improperly Collected on U.S. Citizens," *New York Times* (Dec. 17, 2009).

[90] Spencer Hsu and Carrie Johnson, "Documents Show DHS Improperly Spied on Nation of Islam in 2007," *Washington Post* (Dec. 17, 2009), A09.

[91] Sam Rohrer (R-PA), "Government Intimidation Destroys a Free Society," *Address to Annual Freedom 21 Conference* (Aug. 14, 2009). http://axiomamuse.wordpress.com/2009/12/31/government-intimidation-destroys-a-free-society/

[92] Brian Jackson, ed., *The Challenge of Domestic Intelligence in a Free Society,* (New York: RAND Corp., 2009), p. 76.

[93] Schulhofer, 2002, p. 52, quoted in Jackson, op cit, p. 76.

[94] Jackson, *The Challenge of Domestic Intelligence in a Free Society* (2008), p. 76.

[95] Ibid., p. 75, citing Bergman et al., 2006.

[96] Jackson, *The Challenge of Domestic Intelligence in a Free Society* (2008), p. 75

[97] National Research Council of the National Academies. *Protecting Individual Privacy in the Struggle Against Terrorists*. Washington, D.C.: National Academies Press (2008), pp. 3-4.

[98] Jackson, *The Challenge of Domestic Intelligence in a Free Society* (2008), p. 75.

[99] Jackson, *The Challenge of Domestic Intelligence in a Free Society*, p. 76, citing Ellen Nakashima, "FBI Plans Initiative to Profile Terrorists," *Washington Post* (July 11, 2007). http://www.washingtonpost.com/wp-dyn/content/article/2007/07/10/AR2007071001871.html http://www.rand.org/pubs/monographs/2009/RAND_MG804.pdf

[100] Bruce Fein, Statement before the Subcommittee on Intelligence Sharing & Terrorism Risk Assessment Committee on Homeland Security (April 1, 2009). *http://www.afterdowningstreet.org/node/41360*

[101] Michael W. Markowitz and Delores D. Jones-Brown, eds., 2000, *The System in Black and White*, pp. 66-68. See also, Piliavin and S. Briar, "Police Encounters with Juveniles," *American Journal of Sociology*, vol. 70 (1964), pp. 206-214; J.H. Skolnick, 1966, *Justice Without Trial: Law Enforcement in Democratic Society*.

[102] Greg Ridgeway, RAND Corporation, *New York: Analysis of Racial Disparities in New York City Police Department's Stop and Frisk Practices* (February 1, 2007).

[103] Blue Ribbon Rampart Review Panel, *Rampart Reconsidered: The Search for Real Reform Seven Years Later* (2006). http://www.lapdonline.org/assets/pdf/Rampart Reconsidered-Full Report.pdf

[104] Hess, p. 390, quoting Heather J. Davies and Gerard R. Murphy, *Protecting Your Community from Terrorism: The Strategies for Local Law Enforcement Series Vol. 2: Working with Diverse Communities*. (Washington, DC: Office of Community Oriented Policing Services and Police Executive Research Forum, 2004), p. 1.

[105] See, e.g., Chuck Hustmyre, "In Defense of Profiling," *American Thinker* (Feb. 10, 2010) http://www.americanthinker.com/2010/01/in_defense_of_profiling.html; Jeffrey H. Smith, Former general counsel of the CIA in "What to Make of the Failed Terrorist Attack," *Washington Post* (Dec. 29, 2009) http://www.washingtonpost.com/wp-dyn/content/article/2009/12/28/AR2009122802418.html ; Neil Livingstone, "How Obama Can Really Get Serious on Terrorism," *www.thedailybeast.com* (Jan. 28, 2010) (calling on Pres. Obama to "ditch political correctness") http://www.thedailybeast.com/blogs-and-stories/2010-01-28/how-obama-can-really-get-serious-on-terrorism/?cid=hp:originalslist3 ; Jeff Jacoby, "Tell the Sept 10 people that the war against radical Islam is far from over," www.aish.com (January 2010) http://www.aish.com/ci/s/80401017.html

[106] For example, evidence strongly suggested that the U.S. airport security system resulted in widespread discrimination against Arab and Muslim travelers from 1996 to 2002, but did not prevent the September 11, 2001 attacks. See American-Arab Anti-Discrimination Committee Research Institute, *Reports on Hate Crimes and Discrimination Against Arab Americans* (2003). See also, Aziz Huq, "Three Reasons Racial Profiling Won't End Terrorism," *Color Lines*, (Jan. 20, 2010). Available at: http://www.colorlines.com/article.php?ID=674.

[107] U.S. Department of Justice, Civil Rights Division, "Guidance Regarding the Use of Race in Law Enforcement Agencies." (2002) http://www.usdoj.gov/crt/split/documents/guidance Exceptions for national security and border protection which are

so vague, however, that they permit almost any consideration of race or ethnicity.

[108] See, e.g., Tram Nguyen, We Are All Suspects Now: Untold stories from immigrant communities after 9/11 (Beacon Press, 2005); Amy Bakalian and Mehdi Bozorgmehr, Backlash 9/11: Middle Eastern and Muslim Americans Respond (Univ. of California Press, 2009); Nancy Chang, Silencing Political Dissent: How Post-September 11 Anti-Terrorism Measures Threaten Our Civil Liberties (w/ forward by Howard Zinn) (Seven Stories Press, 2002).

[109] Heymann and Kayyem, op cit, note 51, p. 108.

[110] Allen Pusey, "Every Terrorism Case Since 9/11," *ABA Journal* (Sept. 2007), p. 16 (citing a Transactional Records Access Clearinghouse of Syracuse University analysis of Justice Department data). These investigations have led to more than 4300 prosecutions and almost 3000 convictions. The average sentence has been 27 months.

[111] Attorneys General Ashcroft and Mukasey amended the guidelines governing FBI criminal investigations to make it easier for the FBI to investigate lawful political or religious activities of Americans. On the slightest hint of a connection to a foreign entity, the FBI is required to share that information with the CIA, which is free to include it in secret databases.

[112] Hess, p. 390, citing Andrea Elliott, "After 9/11, Arab-Americans Fear Police Acts, Study Finds." *The New York Times* (June 12, 2006).

[113] Gathering Marbet, "Police Boost Anti-Terrorist Measures on Pier After Suspicious Videotaping," *Surf Santa Monica* (August 11, 2005). http://www.mail-archive.com/osint@yahoogroups.com/msg14379.html

[114] Joel Donofrio, "Pastor: St. Pius incident a simple misunderstanding," *Quad Cities Online* (February 2008). http://qconline.com/archives/qco/display.php?id=375937

[115] Redacted copies of the Department of Homeland Security (DHS) Directorate of Information Analysis and Infrastructure Protection (IAIP) publication the *Homeland Security Operations Morning Brief* (September 27, 2004 to January 14, 2005) Available at: http://cryptome.org/hsomb/hsomb.htm and http://www.tcuec.com/hsomb/

The Massachusetts State Police has responded to reports of suspicious persons concerning the security perimeter around LNG tankers entering and leaving the harbor involving "foreign nationals taking pictures of the tanker, security detail, and the Tobin Bridge." "An LNG Security and Cost Primer," *Fishermen's Voice* (December 2004) (excerpt from "Report of Findings, LNG Security Procedures of an LNG Site in Everett, Mass."), available at: http://www.fishermensvoice.com/archives/lngprimer.html

[116] (AFOSI Talon 102-23-09-04-2297; 23 Sep 04; HSOC 3579-04) Source: Homeland Security Operations Morning Brief 27 September 2004. Available at: http://cryptomes.org/hsomb/hsomb.htm

[117] (COGARD Southwest Harbor; 23 Sep 04; HSOC 3577-04) Source: Homeland Security Operations Morning Brief 27 September 2004. Available at: http://cryptomes.org/hsomb/hsomb.htm

[118] (COGARD FIST Seattle, 28 Sep 04; HSOCT 3657-04) Source: Homeland Security Operations Morning Brief 30 September 2004. Available at: http://cryptomes.org/hsomb/hsomb.htm

[119] (Illinois State Police STIC, 25 Oct 04; HSOC 4065-04) Source: Homeland Security Operations Morning Brief 26 October 2004. Available at: http://cryptomes.org/hsomb/hsomb.htm

[120] (USSS; 19 Nov 04; HSOC 4434-04) Source: Homeland Security Operations Morning Brief 22 November 2004. Available at: http://cryptomes.org/hsomb/hsomb.htm

[121] (Patriot Report: Concerned Citizen Call-in 20 Dec 04; HSOC 4833-04) Source: Homeland Security Operations Morning Brief 21 December 2004. Available at: http://cryptomes.org/hsomb/hsomb.htm

[122] (Patriot Report: Concerned Citizen Call-in, 20 Dec 04; HSOC 4847-04) Source: Homeland Security Operations Morning Brief 21 December 2004. Available at: http://cryptomes.org/hsomb/hsomb.htm

[123] ISE, Program Manager, Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5, "Part B: ISE-SAR Criteria Guidance" (May 2009), p. 29, fn. 11. (requiring that "race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion (except if used as part of a specific suspect description)"). See also: Fact Sheet: Update to Suspicious Activity Reporting Functional Standard Provides Greater Privacy and Civil Liberties Protections, available at: www.ise.gov

[124] ISE, Program Manager, ISE Report to Congress (June 2009) (PAGE #); ISE, Initial Privacy and Civil Liberties Analysis, p. 14.

[125] ISE, Program Manager, ISE, Program Manager, ISE, Initial Privacy and Civil Liberties Analysis (Sept. 2008), p. 14, citing 5 U.S.C. 552a(e)(7).

[126] ISE, Program Manager, ISE, Initial Privacy and Civil Liberties Analysis (Sept. 2009), p. 29.

[127] Department of Justice, *Privacy and Civil Liberties Policy Development Guide and Implementation Templates* (Nov. 2, 2009). Available at: http://it.ojp.gov/default.aspx?area=globalJustice&page=1238

[128] Richard Winton, Teresa Watanabe, Greg Kikorian. "LAPD Defends Muslim Mapping Effort," *Los Angeles Times*. (November 10, 2007). Retrieved from

http://www.latimes.com/news/local/la-me-lapd10nov10,0,3960843.story on December 22, 2009.

[129] Secretary of Homeland Security Michael Chertoff, *Remarks at the 2006, Bureau of Justice Assistance, US Dept of Justice and SEARCH symposium on Justice and Public Safety Information Sharing* (Mar 14, 2006). www.dhs.gov

[130] Doug Wyllie, "American cops are force multipliers in counter-terrorism," PoliceOne (October 1, 2009)

[131] For example, an analyst at Washington's state Fusion Center (WAJAC) looks out for what he calls "pre-operational indicators" of possible terrorist activity when he examines police reports. On one occasion, he noticed an unremarkable police report filed by a young officer who had been called to an area dollar store early in 2007 on a report of suspicious activity. The store clerk told him that a man had come to the store on consecutive days to purchase large quantities of liquid chlorine bleach and ammonia. The relatively inexperienced officer filed a report and closed the case. For this analyst, the two substances were a red flag because they could produce deadly chlorine gas if combined. He filed a report with WAJAC about the pattern of suspicious activity. It turned out that the chemical buyer was a local golf course groundskeeper struggling amid a state ban on gopher traps. To eliminate the pests, he poured homemade, heavier-than-air chlorine gas into their holes. Joseph Straw, "Smashing Intelligence Stovepipes," Security Management (March 2008), retrieved from http://www.securitymanagement.com/print/3708.

[132] ISE, Program Manager, Information Sharing Environment Functional Standard Suspicious Activity Reporting (SAR) Version 1.0 (Jan. 2008), Part B, "ISE-SAR Criteria Guidance," p. 27.

[133] Los Angeles Police Department Terrorism-Related CCAD Codes, attached as Appendix C to the Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project (June 2008), pp. 43-48. District of Columbia Metropolitan Police, General Order, *Suspicious Activity Reporting Program* (GO-HSC-802.06) (Jan. 16, 2009).

[134] See Miami Police Department Emergency Management & Homeland Security, "Miami Shield" Powerpoint presentation, p. 39. Photography reports accounted for fifteen percent of incoming tips to Miami's intelligence division from January 1 to July 2008, though only a small fraction met the criteria for further investigation by the FBI.

[135] Randol, p. 8.

[136] Mazda, p. 6, "War on People," posted to Flickr (September 25, 2007). http://www.flickr.com/photos/85625337@N00/1440772777/

[137] Carols Miller, "Amtrak photo contestant arrested by Amtrak policy in NYC's Penn Station," *Photography is Not a Crime* (December 27, 2008). http://carlosmiller.com/2008/12/27/amtrak-police-arrest-photographer-participating-in-amtrak-photo-contest/ For a clever treatment of Mr. Kerzic by comedian Stephen Colbert, see http://vimeo.com/3064587

[138] Eric Schmitt, "Surveillance Effort Draws Civil Liberties Concern," *The New York Times* (April 28, 2009). http://www.nytimes.com/2009/04/29/us/29surveil.html?pagewanted=all

[139] Ibid.

[140] Associated Press, "Lawsuit claims NYPD harasses photographers, filmmakers," *First Amendment Center* (December 7, 2007). http://www.firstamendmentcenter.org/news.aspx?id=19418 Other instances of abuse include:

In April 2005, photographer Alex Williams was confronted by a King County (Seattle, WA) Sherriff's deputy while taking pictures inside a public bus tunnel. Despite Williams' offering to delete the digital photos, the deputy confiscated his flash cards. Taking pictures at that location was not prohibited, as later stated by a spokesman for the Sheriff's office. Molly Shen, "Police Seize Pictures of Seattle Bus Tunnel," *Komo News* (April 11, 2005). http://www.komonews.com/news/archive/4149371.html

Award-winning documentarian Rakesh Sharma was detained in 2005 after he was spotted filming on a Manhattan sidewalk with a handheld camera. Carol DiOrio, "Suit spurs new rules for NYC filming," *Hollywood Reporter* (May 24, 2007). http://www.hollywoodreporter.com/hr/content_display/business/news/e3i100bdf32d950877fe8f85fc34fea1d67

Brian Gotter, local weatherman in Milwaukee, WI, was pulled over by local authorities after being seen taking photos of a municipal building and public library. Even though Gotter was conducting his routine photographing of local communities to use as backdrops to his forecast and he was ultimately allowed to proceed driving off with his family, authorities stated that taking photographs of public buildings is in itself suspicious behavior sufficient to give authorities the right to stop and detain anyone partaking in such behavior. Jeff Wagner, "Brian Gotter Tracked and Jacked: The War on Terrorism Comes to Franklin," *620 WTMJ* (September 26, 2009). http://www.620wtmj.com/shows/jeffwagner/61877667.html

Also, in 2004, the Massachusetts ACLU documented a case where an elderly couple were using binoculars to birdwatch at a reservoir in western Mass when they were detained by authorities. See ACLU of Massachusetts, *MASS IMPACT* (2004). http://www.aclum.org/pdf/mass_impact.pdf

[141] ACLU of Massachusetts, *Mass Impact* (2005), p. 17. www.aclum.org/pdf/mass_impact.pdf

[142] In July 2008, the Department of Justice proposed extending the retention period from five years to a maximum of ten years without a review and validation of the information. Federal Register, Vol. 73, No. 148 (July 31, 2008) [Docket No. OJP 1473]. The proposed rule changes were not adopted.

[143] Jennifer Cook-Pritt, Florida Department of Law Enforcement Agent. Interview by PRA Investigator Lisa Ruth (October 19, 2009).

[144] ISE, Program Manager, Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5, ISE-FS-200 (April 2009), Part B – "ISE-SAR Criteria Guidance," p. 29.

[145] Ibid., fn. 11.

[146] http://www.iir.com/28cfr/FAQ.htm#q1

[147] Donner (1981), op cit, note 27, p. xv.

[148] See *Brandenburg v. Ohio*, 395 U.S. 444 (1960), holding that the government cannot punish inflammatory speech unless it is directed to inciting and likely to incite imminent lawless action, and striking down an Ohio statute that broadly prohibited the mere advocacy of violence.

[149] District of Columbia Metropolitan Police, General Order, *Suspicious Activity Reporting Program* (GO-HSC-802.06) (Jan. 16, 2009), subsections III, A, 7 aa, bb, and dd. http://www.mpdc.org/GO/GO/GOHSC80206.pdf

[150] Los Angeles Police Department, *Special Order No. 11*, "Terrorism-Related CCAD Codes," (2008)

[151] See, e.g., Robert S. Mueller, III, Director, Federal Bureau of Investigation, Testimony Before the Senate Committee on Intelligence of the U.S. Senate (February 16, 2005): "law enforcement officials must also contend with an ongoing threat posed by domestic terrorists based and operating strictly within the U.S. Domestic terrorists motivated by a number of political or social agendas -- including white supremacists, black separatists, animal rights/environmental terrorists, anarchists, anti-abortion extremists, and self-styled militia -- continue to employ violence and criminal activity in furtherance of these agendas". http://www.fbi.gov/congress/congress05/mueller021605.htm

[152] Carter, p. 322.

[153] Donner (1981), p. 12.

[154] Jeffrey Haas, *The Assassination of Fred Hampton: How the FBI and Chicago Police Murdered a Black Panther,* (Lawrence Hill, Nov. 1, 2009).

[155] Luis A. Fernandez, *Policing Dissent: Social Control and the Anti-Globalization Movement* (Rutgers U. Press, 2008).

[156] G.W. Schulz, "Assessing RNC Police Tactics" *Minnpost.com* (September 1, 2009). http://www.centerforinvestigativereporting.org/articles/assessingrncpolicetacticspart1of2

[157] Heidi Boghosian, *Punishing Protest: Government Tactics That Suppress Free Speech* (National Lawyers Guild, 2007). http://www.nationallawyersguild.org/punishing.htm

[158] Lisa Rein, "Federal Agency Aided Md. Spying," *Washington Post* (February 17, 2009). http://www.washingtonpost.com/wp-dyn/content/article/2009/02/16/AR2009021601131.html

[159] Heymann and Kayyem, op cit, note 51, p. 94, quoting Senate Select Committee on Intelligence, the FBI and CISPESm S. Rep. No. 101-46 at 102 (1989) (quoting United States v. U.S. District Ct. for E. Dist. of Micigan, 407 U.S. 297, 314 (1972)).

[160] Kate Martin. *Domestic Intelligence and Civil Liberties*. SAIS Review, vol. XXIC, no. 1. (Winter-Spring 2004), p. 9.

[161] See Donner, op cit, note 51.

[162] http://www.iir.com/28cfr/FAQ.htm#q1

[163] U.S. Department of Justice, Office of Justice Programs, 199 Revision and Commentary to 28 CFR Part 23 (Sept. 16, 1993). www.iir.com/28cfr/pdf/1993RevisionCommentary_28CFRPart23.pdf

[164] Institute for Governmental Research, "Overview," http://www.iir.com/28cfr/Overview.htm (March 17, 2010).

[165] 28 CFR Part 23 applies to any state or local law enforcement agency that operates a criminal intelligence system supported by funding from the Omnibus Crime Control and Safe Streets Act of 1968, as amended. Consequently, it applies to a very small number of criminal intelligence systems, such as the six Regional Information Sharing Systems (RISS) Intelligence Centers are programs that meet this requirement. The vast majority of agencies complying with 28 CFR Part 23 have voluntarily adopted the regulation.

[166] In order to be *reasonable*, the officer's suspicion must be supported by some specific, articulable facts that are "reasonably consistent with criminal activity." The officer's subjective suspicion must be objectively reasonable, and "an investigative stop or detention predicated on mere curiosity, rumor, or hunch is unlawful even though the officer may be acting in complete good faith." Where a

reasonable suspicion of criminal activity exists, 'the public rightfully expects a police officer to inquire into such circumstances 'in the proper exercise of the officer's duties.'" *People v. Wells*, 36 Cal.4th 1082, 1982 (2009)

[167] ISE Functional Standard, Version 1.5 (5)(h) (emphasis added); see also Version 1.5 at p.6. Program Manager, Information Sharing Environment. *Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5*. (May 2009). http://www.ise.gov/docs/ctiss/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf

[168] Version 1.5(5)(i) (emphasis added)

[169] Version 1.5 (5)(d) (emphasis added)

[170] Global Intelligence Working Group, *Global Intelligence Working Group Meeting Summary* (February 17-18, 2003) http://it.ojp.gov/default.aspx?area=globalJustice&page=1230

[171] See Michelle Kinnucan, "Big Brother Gets Bigger: Domestic Spying & the Global Intelligence Working Group," *Agenda* (Ann Arbor, MI: July-August 2003). http://www.publiceye.org/liberty/repression/big-broth-kin.html The meeting minutes for April 2003 state that the GIWG must officially communicate their support and any recommended changes to 28 CFR Part 23 to the U.S. Department of Justice (DOJ) within the prescribed comment period as noted in the Federal Register. Additionally, the minutes state that GIWG agreed to directly communicate their support of the revised 28 CFR Part 23 to Attorney Alan Fisher, General Counsel's Office, DOJ. http://it.ojp.gov/documents/IWGMeetingSummary4-03.pdf

[172] IACP National Law Enforcement Policy Center "Criminal Intelligence Model Policy "(February 1998, Revised June 2003), p. 1, attached as Appendix C to GWIC Interim Report on the Development of the National Criminal Information Sharing Plan, available at: http://www.ialeia.org/files/docs/Criminal%20Intelligence%20Sharing%20Plan.pdf (last accessed January 19, 2010).

[173] Ibid.

[174] Global Intelligence Working Group, *Meeting Summary* (April 2-3, 2003). http://it.ojp.gov/documents/IWGMeetingSummary4-03.pdf

[175] Information Sharing Environment, Program Manager, "National Suspicious Activity Reporting Initiative Concept of Operations, Version 1".

[176] Program Manger Information Sharing Environment, *Initial Privacy and Civil Liberties Analysis* (September 2008), p. 5, states "If an ISE-SAR also meets 28 CFR Part 23 criteria, [then] it may [also] be submitted to a criminal intelligence information database, and the information in the criminal intelligence system would be subject to the five year review and validation / purge requirement under 28 CFR Part 23." The maximum retention period is five years. A record must be either purged at the end of the established retention period or undergo a review-and-validation process before the end of the retention period. If a record is purged, then it must be removed from the criminal intelligence system. If a record is reviewed and validated, it will receive a new retention period of up to five years. In order for a record to be validated, the submitting agency must determine that the subject is still reasonably suspected of involvement in current criminal activity. In other words, the submitting agency must determine that the record continues to meet the 28 CFR Part 23 submission criteria. A record may be validated at any time during its retention period; however, simply updating the identifying information about the subject during the retention period is not enough, by itself, to indicate the subject is still reasonably suspected of involvement in current criminal activity. http://www.ise.gov/pages/sar-initiative.aspx

[177] ISE-SAR Functional Standards, Version 1.5, Part B, at p. 33 (italics added).

[178] Ibid. A criminal intelligence system provides a way to receive, store, and share or exchange criminal intelligence. A criminal Intelligence System includes the facilities, equipment, agreements, and procedure used for receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence.

[179] ISE, Program Manager, *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project* (October 2008), p. 24.

[180] ISE, Program Manager, *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project* (June 2008), p. 30.

[181] *Ibid.,* p. 28.

[182] *Ibid.*

[183] Program Manger, Information Sharing Environment, *Initial Privacy and Civil Liberties Analysis* (September 2008), p. 15.

[184] Institute for Governmental Research, "Overview," http://www.iir.com/28cfr/Overview.htm (March 17, 2010).

[185] Hess, p. 376, stating "Patrol operations, especially traffic officers, properly trained in what to look for and what questions to ask when interacting with citizens, can be a tremendous source of intelligence, not only for local investigators, but also for their state and federal homeland security counterparts."

[186] Program Manager, Information Sharing Environment. *Information Sharing Environment (ISE) Functional Standards, Suspicious Activity Reporting (SAR), ISE-FS-200* (January 2008). The Director of National Intelligence has

released two definitions of what constitutes a suspicious activities report. In the first version, the ODNI defined an SAR as "*observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention.*" Examples included "surveillance, photography of facilities, site breach or physical intrusion, cars parked or boats anchored at atypical locations, cyber attacks,…or other unusual behavior or incidents."

[187] Los Angeles Police Department, Special Order No. 11. [See Appendix 3 to this Report]. www.stopyspying.us/wiki

[188] Ibid.

[189] See David L. Carter, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies* (U.S. Department of Justice, Office of Community Oriented Policing Services: Jan. 2009), pp. 262-269. http://www.scribd.com/doc/24325790/DOJ-Law-Enforcement-Intelligence-Guide-for-State-Local-Tribal-Law-Enforcement-Agences-2d-Ed-May-2009

[190] Tom Hayden. Interview with PRA Investigator Mary Fischer, September 2009.

[191] John Murphy, Intelligence Manager for the Broward County Sheriff's Office. Interview by PRA Investigator Lisa Ruth (September 17, 2009).

[192] Hess, p. 382.

[193] The Privacy Act of 1974 requires the FBI to make reasonable efforts to ensure the accuracy of NCIC records, but the Justice Department exempted this system from accuracy requirements on March 24, 2003. The NCIC system provides over 80,000 law enforcement agencies with access to more than 39 million records in the blink of an eye. For more information, see http://epic.org/privacy/ncic/

[194] Los Angeles Police Department, "iWATCHLA," *LAPD Online* (retrieved February 2010). http://www.lapdonline.org/iwatchla

[195] William J. Bratton. Interview by Neil Conan, "Los Angeles' iWATCH Antiterrorism Program," National Public Radio (October 6, 2009) http://www.npr.org/templates/story/story.php?storyId=113546077

[196] See Los Angeles Police Department "iWATCH PSA" (retrieved February 2010). http://www.youtube.com/watch?v=RkmRPJv5jZE

197 Ibid.

[198] See *Crimestoppers* www.lacrimestoppers.com/howitworks.aspx

[199] Editorial, "What is Operations TIPS?," *Washington Post* (July 13, 2002).

[200] Matthew Rothschild, "The FBI Deputizes Business," *The Progressive* (March 2008). See also, Matthew Rothschild, "FBI Calls Progressive's Infragard Story Patently False, Author Responds," *The Progressive* (March 1, 2008). http://www.progressive.org/mag_wx030108

[201] Ibid.

[202] Ibid.

[203] Alexander, p. 25. For more on how local policing of immigration harms civil liberties and community safety, see *Forcing Our Blues into Great Areas: Local Police and Federal Immigration Enforcement*, A Legal Guide for Advocates. http://www.neappleseed.org/docs/local_police_and_immigration_enforcement.pdf

[204] See, e.g., *Findings and Recommendations of the Suspicious Activity Reporting (SAR) Support and Implementation Project* for October 2008 (Jan. 2009), pp. 26-28, discussing site overviews for Chicago, Boston, Miami, and Los Angeles. http://www.ijis.org/_programs/sar.html

[205] *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project*. (October 2008), p. 21. http://www.ise.gov/pages/sar-initiative.aspx

[206] ACLU, *What's Wrong with Fusion Centers* (Dec. 2007). http://www.aclu.org/technology-and-liberty/whats-wrong-fusion-centers-executive-summary

[207] Information Sharing Environment, Program Manager, National Suspicious Activity Reporting Initiative Concept of Operations, Version 1, p. 10.

[208] LAPD Special Order No. 11 (March 2008).

[209] Los Angeles Sheriff's Department (LASD) officer who works at the JRIC, unidentified. Interview with PRA Investigator Mary Fischer (September 2009).

[210] Joseph Straw, "Connecting the Dots, Protecting Rights," *Security Management* (August 2009). http://www.securitymanagement.com/article/connecting-dots-protecting-rights-005945

[211] LASD Cmdr. Mike Grossman, co-manager of the JRIC. Interview with PRA Investigator Mary Fischer (September 2009).

[212] Caroline Fredrickson, American Civil Liberties Union, "Protecting National Security and Civil Liberties: Strategies for Terrorism Information Sharing," *Statement before the Senate Committee on the Judiciary* (April 1, 2009). Available at: www.**aclu.org**/files/images/ asset_upload_file33_39415.pdf

[213] IRTPA, Section 1016. Center for Democracy & Technology, "CDT Analysis of Privacy Guidelines for the Information Sharing Environment for Terrorism Information," (Feb. 2, 2007) Available at: http://www.cdt.org

[214] Randol, p. 38.

[215] See Center for Democracy & Technology, "CDT Analysis of Privacy Guidelines for the Information Sharing Environment for Terrorism Information," (Feb. 2, 2007), p. 4. http://www.cdt.org. The privacy guidelines are online at www.ise.gov/docs/privacy/PrivacyGuidelines20061204.pdf

[216] Program Manager, Information Sharing Environment, *Progress and Plans Annual Report to the Congress* (June 2009), Appendix B, p. 52.

[217] Information Sharing Environment, Program Manager, National Suspicious Activity Reporting Initiative Concept of Operations, Version 1, "The NSI as an Integrated ISE Shared Space Environment," (Dec. 2008), Appendix B, pp. 35-38. Guardian operates at the Secret level and it still inaccessible to many federal, state, and local law enforcement agencies, while eGuardian operates at the "sensitive but unclassified" level to engender broader sharing and greater collaboration between JTTFs and local law enforcement.

[218] Ben Bain, "Feds take counterterrorism local," *Federal Computer Weekly* (October 6, 2008). http://www.kms.ijis.org/traction?type=single&proj=Public&rec=3261&drafts=f See also FBI, "eGuardian Threat Tracking System," FBI Press Room. Available at: http://foia.fbi.gov/eguardian_threat.htm

[219] Federal Bureau of Investigation, "Connecting the Dots: Using New FBI Technology," FBI Press Room (Sept. 19, 2008). http://www.fbi.gov/page2/sept08/eguardian_091908.html According to the FBI, if an incident has no probable link to terrorism, the report is deleted to ensure personal data is not being needlessly stored. If the information is deemed "inconclusive," it will remain in eGuardian for up to five years, in accordance with federal regulations.

[220] Program Manager for the ISE, *Information Sharing Environment, Progress and Plans, Annual Report to the Congress* (June 2009), p. 19. Available at: http://www.fas.org/irp/agency/ise/2009report.pdf.

[221] Ibid.

[222] Information Sharing Environment, Program Manager, National Suspicious Activity Reporting Initiative Concept of Operations, Version 1, p. 10.

[223] Ibid., p. 12.

[224] Tom Parker, Los Angeles FBI Agent. Interview by PRA Investigator Mary Fischer (September 2009).

[225] Joseph Straw, "Connecting the Dots, Protecting Rights," p. 22.

[226] Office of the Inspector General. *The Federal Bureau of Investigation's Terrorist Threat and Suspicious Incident Tracking System.* Audit Report 09-02 (November 2008). http://www.justice.gov/oig/reports/FBI/a0902/exec.htm

[227] Captain Greg Hall, Los Angeles Police Department, Major Crimes Division, Divisional Order No. 15, "Privacy Guidelines for Information Sharing Environment, Suspicious Activity Report (ISE-SAR) Evaluation Environment Initiative." (August 28, 2009). Available at: www.stopspying.us/wiki.

[228] JTTF agent who asked to remain unidentified. Interview by PRA Investigator Mary Fischer (September 2009).

PRA
Political Research Associates

1310 Broadway, Suite 201
Somerville, MA 02144-1837
Voice: 617.666.5300
www.publiceye.org