BRENNAN CENTER FOR JUSTICE

NATIONAL SECURITY AND LOCAL POLICE

Michael Price

Brennan Center for Justice *at New York University School of Law*

ABOUT THE BRENNAN CENTER FOR JUSTICE

The Brennan Center for Justice at NYU School of Law is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. We work to hold our political institutions and laws accountable to the twin American ideals of democracy and equal justice for all. The Center's work ranges from voting rights to campaign finance reform, from racial justice in criminal law to Constitutional protection in the fight against terrorism. A singular institution — part think tank, part public interest law firm, part advocacy group, part communications hub — the Brennan Center seeks meaningful, measurable change in the systems by which our nation is governed.

ABOUT THE BRENNAN CENTER'S LIBERTY AND NATIONAL SECURITY PROGRAM

The Brennan Center's Liberty and National Security Program works to advance effective national security policies that respect Constitutional values and the rule of law, using innovative policy recommendations, litigation, and public advocacy. The program focuses on government transparency and accountability; domestic counterterrorism policies and their effects on privacy and First Amendment freedoms; detainee policy, including the detention, interrogation, and trial of terrorist suspects; and the need to safeguard our system of checks and balances.

ABOUT THE BRENNAN CENTER'S PUBLICATIONS

Red cover | Research reports offer in-depth empirical findings.
Blue cover | Policy proposals offer innovative, concrete reform solutions.
White cover | White papers offer a compelling analysis of a pressing legal or policy issue.

ABOUT THE AUTHOR

Michael Price serves as counsel for the Brennan Center's Liberty and National Security Program, which seeks to ensure that our government respects human rights and fundamental freedoms in conducting the fight against terrorism. Before joining the Brennan Center, Mr. Price was the National Security Coordinator for the National Association of Criminal Defense Lawyers, where he provided legal assistance for the defense of detainees in the military commissions at Guantanamo Bay. Mr. Price also engaged in litigation and public advocacy on issues related to privacy, electronic searches and surveillance, and government secrecy. Mr. Price was the student research director for NYU's Center on Law and Security, an intern with the Department of Justice Civil Rights Division, a symposium editor for the Journal of International Law and Politics, and a student advocate in NYU's International Human Rights Clinic, where he represented two Yemeni nationals detained and tortured in secret CIA "black sites." He holds a J.D. from NYU School of Law and a B.A. from Columbia University in Political Science and Middle East & Asian Languages and Cultures.

ACKNOWLEDGEMENTS

The Brennan Center gratefully acknowledges The Atlantic Philanthropies, C.S. Fund, Democracy Alliance Partners, The Herb Block Foundation, Open Society Foundations, and the Security & Rights Collaborative, a Proteus Fund initiative, for their generous support of the Liberty & National Security Program.

The author would like to thank Emin Akopyan, Sadia Ahsanuddin, R. Kyle Alagood, Emanuel Arnaud, Jeremy Carp, Michael Eggenberger, Lena Glaser, Elizabeth Goitein, Elizabeth Hira, Seth Hoy, John Kowal, Rachel Levinson-Waldman, Kimberly Lubrano, Jim Lyons, Eric Opsal, Shannon Parker, Faiza Patel, Jeanine Plant-Chirlin, Desiree Ramos Reiner, Frederick A.O. Schwarz, Jr., Jeramie Scott, Madeline Snider, Amos Toh, and Michael Waldman for their invaluable input and assistance. In addition, the author greatly benefited from the advice and comments of Kara Dansky, Michael German, Patrick O'Hara, Stephen Schulhofer, Matthew Waxman, and members of the Muslim American Civil Liberties Coalition.

TABLE OF CONTENTS

Stamp's Law: "The Government are very keen on amassing statistics – they collect them, add them, raise them to the nth power, take the cube root and prepare wonderful diagrams. But what you must never forget is that every one of those figures comes in the first instance from the chowky dar *(village watchman), who just puts down what he damn pleases."*[1]

INTRODUCTION

Since the attacks of September 11, 2001, many state and local law enforcement agencies have assumed a critical but unfamiliar role at the front lines of the domestic fight against terrorism. The federal government has encouraged their participation, viewing them as a tremendous "force multiplier"[2] with approximately 800,000 officers nationwide.[3] Indeed, by collecting and sharing information about the communities they serve, police departments have been able to significantly increase the data accessible to members of the federal intelligence community.[4] At the same time, however, the headlong rush into counterterrorism intelligence has created risks for state and local agencies, with too little attention paid to how to manage them.

Although prevention of terrorist attacks is often described as a new, post-9/11 paradigm for law enforcement, the prevention of all crime has been a central tenet of modern policing since its debut nearly 200 years ago.[5] Intelligence activities, including the use of surveillance, undercover officers, and informants, have helped fulfill this mandate. But due to the potential for abuse that came to light during the 1960s and 70s, many courts and legislatures placed checks on police intelligence operations. Most importantly, they required officers engaged in intelligence activities to have reasonable suspicion that a person or group is involved in criminal activity before collecting, maintaining, or sharing information about them. Of course, this rule does not apply to most other police activities. Officers responding to an emergency, for example, may record a victim's statement or document an eyewitness account without suspecting either individual of wrongdoing. But for many police departments, reasonable suspicion became a prerequisite for creating intelligence files.[6]

Since 9/11, some police departments have established counterterrorism programs to collect and share intelligence information about the everyday activities of law-abiding Americans, even in the absence of reasonable suspicion.[7] This information is fed into an array of federal information sharing networks, creating mountains of data.[8] Whether these practices have made us safer is debatable.[9] What is clear is that they raise issues of accountability and oversight in ways that have not been given sufficient attention.

The centerpiece of this new counterterrorism architecture is a national information sharing network connecting police departments and federal agencies, known as the Information Sharing Environment (ISE). But there is little consistency regarding the types of information that local law enforcement agencies collect and share with their federal counterparts. The policies and procedures governing such activities are often opaque or unavailable to the public, while a deliberately decentralized system produces rules that vary considerably across the country. Inconsistent rules jeopardize the quality of shared intelligence and raise serious civil liberties concerns. In some jurisdictions, for example, police have used aggressive information-gathering tactics to target American Muslim communities without any suspicion of wrongdoing. Such practices have not generated investigative leads or proven especially useful in preventing potential terrorist attacks.[10] But they have strained community relations with law enforcement, thereby jeopardizing the very terrorism prevention mission they are intended to accomplish.[11]

Many state and local intelligence programs lack adequate oversight. While federal agencies operate under the watch of independent inspectors general, there is often no equivalent for state and local information sharing ventures. Very few local governments have built the kind of oversight structures that should accompany such a significant expansion of police functions.

Joint Terrorism Task Forces (JTTFs) are teams of counterterrorism investigators, analysts, and experts culled from dozens of law enforcement and intelligence agencies, including state and local police departments.[12]

Fusion centers are regional or statewide hubs where federal, state, and local agencies come together to collect and share information about national security and other threats.[13]

Local police departments often run regional fusion centers covering major urban areas while state police operate statewide fusion centers. JTTFs tend to focus on investigative work while fusion centers are geared towards information collection and analysis, but their missions are intimately related and often overlapping.

This report surveys the following police departments, fusion centers, and JTTFs:

Police Departments

- New York City Police Department (NYPD)
- Chicago Police Department (CPD)
- Los Angeles County Sheriff's Department (LASD)
- Los Angeles Police Department (LAPD)
- Philadelphia Police Department (PPD)
- Houston Police Department (HPD)
- Metropolitan Police Department (MPDC)
- Miami -Dade County Police Department (MDPD)
- Detroit Police Department (DPD)
- San Francisco Police Department (SFPD)
- Seattle Police Department (SPD)
- Miami Police Department (MPD)
- Portland Police Bureau (PPB)
- Minneapolis Police Department (MPD)
- St. Paul Police Department (SPPD)
- Dearborn Police Department (DPD)

Fusion Centers

- New York State Intelligence Center
- [Chicago] Crime Prevention and Information Center
- Illinois Statewide Terrorism and Intelligence Center
- Los Angeles Joint Regional Intelligence Center
- California State Terrorism Threat Assessment Center
- Delaware Valley Intelligence Center [Philadelphia]
- Pennsylvania Criminal Intelligence Center
- Houston Regional Intelligence Service Center
- Texas Fusion Center
- Washington [DC] Regional Threat and Analysis Center
- Southeast Florida Fusion Center [Miami-Dade]
- Florida Fusion Center
- Detroit and Southeast Michigan Information and Intelligence Center
- Michigan Intelligence Operations Center
- Northern California Regional Intelligence Center [San Francisco]
- Washington State Fusion Center
- Oregon Terrorism Information Threat Assessment Network
- Strategic Information Center [Minneapolis-St. Paul]
- Minnesota Joint Analysis Center

JTTFs

- New York City JTTF
- Chicago JTTF
- Los Angeles JTTF
- Philadelphia JTTF
- Houston JTTF
- Washington, DC JTTF
- Miami JTTF
- Detroit JTTF
- San Francisco JTTF
- Seattle JTTF
- Portland JTTF
- Minneapolis JTTF

At the state and local level, the intelligence architecture has developed along two main tracks: Joint Terrorism Task Forces (JTTFs) led by the Federal Bureau of Investigation (FBI) and "fusion centers" funded by the Department of Homeland Security (DHS) and Department of Justice (DOJ).

There is no shortage of reports describing particular aspects of this system,[14] but the overall enterprise – which includes approximately 14,600 different sub-federal law enforcement agencies,[15] 78 regional and state-run fusion centers,[16] and 103 JTTFs[17] – is difficult to map fully. This report seeks to fill this gap by describing and assessing the role played by state and local law enforcement in counterterrorism intelligence activities through the prism of 16 major police departments, 19 affiliated fusion centers, and 12 JTTFs.

The 16 police departments selected for study are among the largest in the United States. The Brennan Center chose them on the basis of three factors that made it likely that they would be most involved in the counterterrorism enterprise: (1) the number of terrorism prosecutions in their federal judicial districts; (2) the size of their American Muslim communities (which have been subject to intensive law enforcement scrutiny since 9/11) in their jurisdiction; and (3) their history of law enforcement intelligence activities. Some smaller cities, like Portland, Oregon, and Dearborn, Michigan, are included because they have large Muslim communities. The Eastern District of Michigan, which covers Dearborn and Detroit, also has the most federal terrorism indictments of any jurisdiction in the country.

The Brennan Center examined the 19 fusion centers that work with these police departments, focusing on their policies and procedures for collecting and sharing intelligence information. We also sought to understand the relationship between police departments and JTTFs, particularly where local participants were subject to different laws and policies than their federal colleagues. In addition to reviewing federal, state, and local laws, as well as departmental policies and procedures, the Brennan Center made extensive use of freedom of information requests, analyzed budgets, audits, and grant applications, conducted fusion center site visits in New York and California, and interviewed dozens of community leaders, state and local police, and fusion center officials.

We sought clarity about how state and local agencies are actually functioning in the domestic intelligence architecture. What we found was organized chaos: a federally subsidized, loosely coordinated system for sharing information that is collected according to varying local standards with insufficient quality control, accountability, or oversight.

Understanding this new system requires a brief examination of the evolution of state and local law enforcement agencies in the 12 years since 9/11, which is set out in Section I. This section shows that while no two police departments are the same, most departments covered in this survey have, to a greater or lesser extent, incorporated an "intelligence-led" approach to policing and have adopted rules to allow the collection and sharing of information through federal networks and databases. Only a handful of jurisdictions, however, have taken steps to minimize the risk to civil liberties and community relations posed by their intelligence operations.

Section II identifies the new web of information-sharing relationships among these police departments and thousands of other federal, state, and local agencies. It demonstrates that this web operates with a range of state and local rules about inputs, potentially compromising both the quality of information and constitutionally protected rights.

The Boston Marathon Bombing

The Brennan Center did not conduct an extensive review of the Boston Police Department because Boston did not meet the initial selection criteria for this survey. Nonetheless, the April 2013 Boston Marathon bombing naturally raised questions about the effectiveness of existing information sharing networks. The FBI is conducting its own investigation of the matter and Congress too has expressed concerns. As of the writing of this report, it cannot be said for certain whether the system worked as intended. Many questions relevant to such an evaluation remain unanswered. It is clear that the FBI conducted an assessment of one of the suspects, Tamerlan Tsarnaev, prior to the attack, based on a tip from Russian authorities that he planned to travel to Russia and join "underground" groups.[18] The FBI closed its assessment in June 2011, concluding that Tamerlan did not warrant further investigation. But just three months later, Tamerlan was implicated in a gruesome triple homicide occurring on September 11, 2011.[19] Were police investigators aware that the FBI had conducted an assessment of Tamerlan? Was the FBI aware of the murder investigation? Tamerlan's name was also included on a travel watch list as a result of the Russian tip. When he flew to Russia in 2012 and returned six months later, officials at the Boston Joint Terrorism Task Force received alerts. Should the FBI have reopened its assessment or questioned Tamerlan when he returned? Did the four Boston police officers assigned to the JTTF have access to the FBI's information about Tamerlan? Should the FBI have done more to bring it to their attention?[20] More broadly, were there gaps in the intelligence sharing system, or does the system need to be better tuned?[21]

Oversight of the system is spotty at the state, local, and federal levels. Section III analyzes the types of oversight models employed by police departments, concluding that most are ill suited to monitoring counterterrorism intelligence activities. A few police departments are subject to independent oversight by special counsels or inspectors general, which offer the best potential to fill this role at the municipal level. As discussed in Section IV, fusion centers have almost no independent oversight at the state or federal level. And as described in Section V, local police officers serving on JTTFs regularly operate under vague rules, often without police supervisors or local elected officials aware of their activities.

The push to increase information sharing among all levels of government was intended to safeguard the country against terrorism. But there is little data to gauge whether the system, as currently structured, has contributed to our safety.[22] DHS has spent nearly $1.4 billion on fusion centers, but it has not collected information to determine how these funds are utilized.[23] Likewise, the FBI does not track whether the information it receives from state and local agencies has helped deter terrorist threats or led to arrests and convictions.[24] At the same time, advocates have reported an increasing number of privacy and civil rights abuses.[25] And last year, a bipartisan, two-year Senate investigation concluded that fusion centers have routinely produced "irrelevant, useless or inappropriate" intelligence that endangers civil liberties and have not contributed to disrupting a single terrorist plot.[26] These revelations call into question the value of fusion centers as currently structured and, at minimum, point to the need for clearer rules on information sharing and greater oversight of state and local intelligence operations, including funding streams.

A systematic view of the involvement of local law enforcement agencies in counterterrorism operations reveals three problems that present significant challenges and potential costs from both a security and a civil liberties perspective:

- Most existing police oversight mechanisms are not equipped to monitor intelligence activities or weigh the impact of such operations on civil liberties or police-community relations.

- Information sharing among federal, state, and local agencies occurs under inconsistent rules and procedures that create a patchwork intelligence system with little in the way of quality controls or civil liberties protections.

- Independent oversight of fusion centers is virtually non-existent and compounds the risks of the decentralized form that information sharing has taken.

Section VI offers a number of recommendations for reform. Substantively, the Brennan Center recommends that state and local police departments tighten standards for collecting and sharing intelligence information in order to ensure that their efforts provide quality data and mitigate harm to community relations and civil liberties and civil rights. The various federal agencies that provide funding for these departments should encourage better standards by tying future financial assistance to reform. To ensure compliance with applicable rules, the Brennan Center recommends strengthening oversight of state and local intelligence activities at the state and local level. Additionally, fusion centers should be required to commission or consent to regular independent audits in order to verify compliance with applicable laws and policies. These reforms will help ensure that local intelligence efforts generate quality counterterrorism information while taking care not to jeopardize critical police-community relations or civil liberties and civil rights.

I. NEW ROLES FOR LOCAL LAW ENFORCEMENT: PHILOSOPHY, ORGANIZATION, AND NEW RULES

The attacks of September 11, 2001, sparked a massive overhaul of the federal intelligence and counterterrorism infrastructure. Terrorism was not a new problem, but it had not been a domestic priority until 2001,[27] especially for state and local law enforcement agencies. The 9/11 Commission Report emphasized that prevention of future attacks would require effective sharing of information throughout all levels of law enforcement: federal, state, and local.[28]

In response, Congress combined 22 federal agencies to form the Department of Homeland Security,[29] now the third largest agency in the federal government.[30] The FBI recast its priorities as well: preventing terrorism took precedence over its regular crime fighting responsibilities.[31] The Attorney General paved the way for more terrorism-related intelligence work by easing restrictions on the gathering of information about religious and political activities.[32] By 2004, the newly minted Office of the Director of National Intelligence (ODNI) was responsible for coordinating the entire intelligence community, consisting of 17 separate federal agencies, including the Central Intelligence Agency (CIA), the FBI, and parts of DHS and the Department of Defense.[33] At the same time, Congress created the National Counterterrorism Center (NCTC) to begin integrating information from all sources.[34]

As part of this transformation, the federal government sought to "leverage" the information gathering abilities of state and local law enforcement.[35] A flood of money flowed from the federal government to support local police in their new and unfamiliar job as the "eyes and ears" of the U.S. intelligence community.[36] Major cities such as New York and Los Angeles, which faced a heightened risk of attack, significantly altered the mission and structure of their police departments.[37] Smaller departments were equally eager to receive federal funding and build their intelligence capacities, even if counterterrorism was not a local priority.

As a result, many police departments changed the way they did business. Philosophically, there was a shift toward "intelligence-led policing," which seeks to collect information about possible perpetrators and intervene *before* a crime is committed.[38] In the counterterrorism context, proponents of intelligence-led policing believe that analyzing even innocuous or disparate pieces of information can help "connect the dots" and reveal potential terrorist plots.[39] According to David Cohen, the NYPD's Deputy Commissioner of Intelligence, "to wait for an indication of crime before investigating is to wait far too long."[40] Consequently, increased resources were devoted to intelligence gathering, especially by larger police departments. Rules, or the interpretation of them, were changed to permit greater latitude in the collection, storage and sharing of intelligence reports.

The utility of this approach is hotly debated.[41] What is not debatable is that police departments, and the local lawmakers charged with their supervision, have not always paid sufficient attention to the risks associated with this turn towards counterterrorism intelligence. As a result, reports of abuses have emerged, including departments accused of targeting American Muslim communities[42] and social protest movements, such as Occupy Wall Street and its local manifestations.[43]

But violations of civil rights are not the only risks posed by these changes. Losing the trust of its community is easy for a police department that strays far from its longstanding mission of serving the public. This can be counterproductive for both crime fighting and counterterrorism.

Community cooperation is essential to both. According to a 2010 study by the Institute for Homeland Security Solutions, tips from the public accounted for nearly a third of all actionable information leading to foiled terrorist plots.[44] Decades of policing research show that perceptions of fairness directly influence the willingness of communities to cooperate with the police. But community resentment and distrust can build if local law enforcement trawls for information with little rationale, discouraging engagement with the police. This is especially true where intelligence operations single out ethnic or religious communities for scrutiny. A study recently cited by the Department of Justice[45] found that individuals with potentially valuable information will be more reluctant to engage with police, even though they may be staunchly opposed to violence to achieve political ends.[46] And, as intelligence experts have concluded, sweeping surveillance programs will almost inevitably produce a mountain of irrelevant information that makes identifying genuine threats more difficult.[47] Like a Google search, the results are only as good as the query. If police officers do not have a focused and well-founded reason for collecting and sharing information, the resulting "white noise" may complicate and distort the intelligence process.[48]

Philosophy: Toward "Intelligence-Led Policing"

When it comes to fighting terrorism, many local law enforcement agencies have adopted the idea of "intelligence-led policing."[49] There are differing definitions of the term,[50] but a central tenet is the collection and analysis of information, often covertly, for the purpose of top-down decision-making aimed at crime prevention.[51]

The Brennan Center's research found that 12 of the 16 police departments surveyed utilize elements of an intelligence-led approach.[52] The extent to which a police department embraces this philosophy depends on many factors, including the perceived likelihood of a terrorist attack; force size; funding; and the opportunity cost of shifting resources to counterterrorism.

No department has embraced intelligence-led policing as fully as the New York City Police Department (NYPD).[53] In the aftermath of 9/11, Police Commissioner Raymond Kelly dedicated 1,000 officers to counterterrorism duties and recruited David Cohen, a 35-year CIA veteran, to run the Intelligence Division.[54] The NYPD's intelligence operations extend to bordering states as well as overseas.[55] No other local police department has a comparable program.

The NYPD's intelligence operations have been highly controversial. A 2011 Pulitzer Prize-winning Associated Press (AP) investigation documented the NYPD's surveillance of Muslim communities because of their religion.[56] In brief, documents released by the AP show: the police "Demographics Unit" mapped and monitored New York's Muslim neighborhoods;[57] the NYPD sent informants and undercover officers into mosques to listen in on religious and political discussions, which were then recorded in police files;[58] and the NYPD routinely monitored the activities of Muslim Student Associations at colleges and universities in New York, New Jersey, Connecticut, and Pennsylvania.[59] These activities are the basis of three ongoing federal lawsuits challenging their legality.[60] The approach has

also come at the cost of community trust, which experts agree is essential to the success of counterterrorism efforts.[61] Since the extent of the NYPD's intelligence operations became public, there has been a noticeable cooling of relations between the police and many community leaders. Muslims have boycotted "outreach" events hosted by the city,[62] protested against the NYPD, and organized reform efforts.[63]

Other police departments that are also strong proponents of intelligence-led policing have rejected some of the tactics used by the NYPD. For example, in 2007, the Los Angeles Police Department (LAPD) dropped a plan to "map" Muslim communities following grave concerns expressed by religious and civil rights groups.[64] And after details of the NYPD's surveillance operations emerged in 2011, the Chicago police chief (who previously served in the NYPD) affirmed that his department "does not and will not conduct blanket surveillance and profiling of any community in the city of Chicago."[65] The Chicago police also promptly expanded prohibitions against "bias-based policing" and religion-based intelligence investigations.[66]

This does not mean, however, that either Los Angeles or Chicago does not collect intelligence. Indeed both police forces operate broad counterterrorism intelligence programs that are permitted to collect information even where there is no suspicion of criminal or terrorist activity. Nonetheless, publically available information suggests that neither department targets particular religious or ethnic groups for active, wholesale surveillance. Rather, both departments rely heavily on their officers reporting "suspicious activity" that they encounter in the course of their normal duties. This information is then shared with state and regional "fusion centers," as detailed in Section II.

The Los Angeles County Sheriff's Department (LASD), the fourth largest local law enforcement agency in the country, follows a somewhat different approach. While it collects intelligence, it prohibits its officers from retaining any intelligence files unless they contain reasonable suspicion that an individual or group is involved in criminal activity.[67] It also employs a robust community outreach strategy, but segregates outreach programs from police counterterrorism or intelligence units.[68]

All of the police departments in this survey (and others like them) conduct community outreach. Some combine community outreach with intelligence collection, while others keep the two ventures separate. The LASD, for example, says it does not provide outreach information to counterterrorism or intelligence units, focusing instead to build "long-term, trusted relationships" with the community.[69] Muslim community leaders in Los Angeles take a generally positive view of the LASD's outreach efforts and do not believe local police are being duplicitous, although some lament that the relationship is based on homeland security concerns.[70] By contrast, many Muslim New Yorkers suspect that the NYPD uses outreach activities such as youth cricket leagues and mosque visits as a cover for intelligence collection.[71] As a result, prominent community leaders have developed a pronounced distrust of NYPD outreach efforts, perceiving them as little more than a public relations tool for the department.[72]

Overall, many police departments have strengthened their intelligence collection operations and explicitly shifted toward intelligence-led strategies in the years since 9/11. There are, however, significant variations in how police view this mission. While some, such as the NYPD, have whole-heartedly embraced an aggressive approach, others have sought to balance counterterrorism imperatives with their traditional mandate to serve and build trust with communities.

Organization: Counterterrorism Intelligence Units

The Brennan Center's review of 16 police departments shows a direct correlation between the overall size of a department, the degree to which it relies on intelligence-led policing, and the amount of resources it has devoted to counterterrorism intelligence units. Intelligence-led counterterrorism strategies require additional resources because local police departments cannot simply abandon their obligation to fulfill traditional law enforcement responsibilities such as crime investigation and neighborhood patrols.[73] Consequently, many police departments have found ways to incorporate counterterrorism intelligence responsibilities into more traditional police operations. Department missions to preserve "homeland security" often describe a diverse set of functions, by no means limited to (or even explicitly inclusive of) counterterrorism. In this context, counterterrorism intelligence may be secondary to broader "criminal intelligence" responsibilities geared toward prevention and interdiction of a range of threats to public safety.[74]

Before 9/11, police intelligence units fought organized crime, narcotics, and gangs. Only New York, which had a terrorist attack in 1993, and Los Angeles had dedicated counterterrorism personnel.[75] Today, more than 80 percent of the departments in this report have sworn personnel with specific counterterrorism intelligence duties, not including officers assigned to state or federal operations.[76] Seven of these departments have officers whose sole function is counterterrorism while six have more generalized intelligence units that include counterterrorism in their mandate. Only cash-strapped Detroit,[77] which has been forced to trim its police force despite having one of the nation's highest violent crime rates,[78] and the community policing bastions of Dearborn[79] and Portland,[80] do not have any such personnel.

As noted, the NYPD has developed a vast and unique counterterrorism apparatus. It has devoted approximately 1,000 officers to the Counterterrorism Bureau and the Intelligence Division with annual combined budget of more than $100 million.[81] The Intelligence Division receives approximately two-thirds of these resources.[82] Funding for the department's counterterrorism operations comes not only from the city, state, and federal governments, but also from two private foundations. The New York City Police Foundation pays for the NYPD's overseas intelligence operations, which span 11 locations around the world.[83] The NYPD Counter-Terrorism Foundation raised nearly $300,000 to pay Marc Sageman, a former CIA officer, to become the department's first "scholar-in-residence."[84]

Police departments outside of New York spend far less on counterterrorism intelligence operations. The LAPD formed a Counterterrorism and Special Operations Bureau to house its long-standing Anti-Terrorist Intelligence Section, which is responsible for receiving, analyzing, and disseminating information about potential terrorist activity.[85] The entire Bureau consists of five divisions, with 750 people and has an annual budget of approximately $77 million.[86] While official figures are unavailable, news reports indicate that it devotes roughly 300 people and $24 million to counterterrorism.[87] Similarly, the D.C. police department created a Homeland Security Bureau with a total budget of $53 million and roughly 300 officers, 63 of which are responsible for intelligence work at a cost of $7 million.[88] In addition, in late 2011, Chicago began the process of reorganizing its police department, consolidating counterterrorism functions under a single unit.[89] In 2012, the Chicago Police Department employed 327 counterterrorism officers in 6 sections with a combined budget of $25 million.[90] But by 2013,

Chicago moved its counterterrorism intelligence operations under the command of a new "Office of Crime Control Strategies," reduced their budget to approximately $8 million, and cut the number of officers to 100.[91] Given that the city recorded a shocking 506 murders during 2012,[92] the Chicago police have naturally been keen to focus their resources on more traditional policing.[93]

The LASD is one of six police departments in this survey that has officers with counterterrorism intelligence duties but does not have a dedicated counterterrorism intelligence unit. Instead, counterterrorism is the responsibility of the Major Crimes Bureau, which is also charged with investigating a host of other offenses ranging from organized crime to gang activity to health care fraud.[94] Similarly, the Miami Police Department has an Intelligence and Terrorism Unit that provides protection for visiting dignitaries and is responsible for investigating organized crime and money laundering in addition to terrorism.[95]

This division of resources is typical of mid-sized police departments that do not follow a strict intelligence-led philosophy. Fiscal constraints have also prompted some departments to reconsider and curtail their counterterrorism intelligence operations to instead fund routine crime prevention and investigation.[96] Without dedicated counterterrorism intelligence units, these departments often rely on regional or state-run fusion centers and federal Joint Terrorism Task Forces, as discussed in Section II.

Departments without a dedicated counterterrorism intelligence unit or full-time counterterrorism intelligence officers can still play a critical role in identifying and protecting critical infrastructure, educating and increasing community awareness about potential threats, conducting outreach to vulnerable segments of the population, and preparing emergency response plans.[97] Unlike covert intelligence operations, protecting critical infrastructure and building partnerships with local businesses and communities is in line with traditional policing priorities and poses far fewer risks to civil liberties and community relations. Officers assigned to ports and airports, for example, can simultaneously protect against terrorism, improve drug interdiction capabilities, and decrease other crime.[98] In fact, the Miami-Dade Police Department reported a "spillover effect" due to increased police presence at the airport resulting in an 80 percent reduction in theft over time.[99]

As a result of this dynamic, many of the smaller departments studied by the Brennan Center, and particularly those that emphasize community policing, have focused almost entirely on what DHS calls "hometown security," also known as community protection.[100] The Dearborn Police Department exemplifies this approach, tending to view the primary responsibility for counterterrorism intelligence as the province of state and federal agencies. In addition to its community outreach work, Dearborn focuses on preventive patrols for possible terrorist targets (i.e., increased police presence in strategic locations), general target hardening (i.e., increased physical security at vulnerable locations), investigating suspicious packages, and improving emergency response capabilities.[101] Such activities are often outside the mandate of federal authorities but are particularly well suited to local law enforcement agencies because of their presence in the community and their preexisting patrol and response capacity.[102]

Overall, only large police departments facing a significant threat of terrorism may be able to afford big, dedicated counterterrorism intelligence units. However, such an approach carries known risks. Without sufficient rules and oversight, these units risk violating civil rights and civil liberties and can alienate large swaths of the community, which in turn may prove counterproductive. They also detract

resources from traditional crime fighting obligations. Smaller police departments do not have personnel dedicated to counterterrorism intelligence, but their day-to-day criminal intelligence work will often include a counterterrorism component. An emphasis on community outreach and partnership can also enhance public trust and open lines of communication, although it is important not to exploit this relationship or to substitute it for actionable intelligence. Moreover, when police intelligence efforts support patrols, target hardening, and the investigation of "precursor" crimes, they are likely to mitigate the danger of abuse and the deterioration of community relations while performing critical counterterrorism functions.

New Rules: Untethering Intelligence Activities from the Reasonable Suspicion Requirement

The decentralized nature of American policing has allowed for the proliferation of an array of philosophies and structures. This has produced wildly different rules on how police departments collect, store, and share intelligence information. Until 9/11, police departments had limited authority to gather information on innocent activity, such as what people say in their houses of worship or at political meetings. Police could only examine this type of First Amendment-protected activity if there was a direct link to a suspected crime. But the attacks of 9/11 led law enforcement to turn this rule on its head.[103] Some departments, such as New York and Chicago, loosened restrictions for monitoring First Amendment-protected activity, under the theory that acts of terrorism are preceded by many legal activities that could be detected by giving police freedom to spy on religious or political organizations.[104] Others started participating in Suspicious Activity Reporting (SAR) programs, which are based on the premise that police officers may come across activity that is not indicative of a crime, but is still "suspicious" and should be recorded. Notably, some police departments decided that they could prevent terrorism perfectly well under existing rules and did not embrace these changes. These choices have tremendous implications for the liberty and security of everyone in the United States.

Consent Decrees: New York, Chicago, and Los Angeles

In theory, the authority of local law enforcement agencies to conduct intelligence operations rests entirely on their statutory mandate to enforce criminal law.[105] It follows that there should be some criminal predicate, some fact-based reason to suspect criminal activity, to justify intelligence gathering activities by local police.[106] In 1968, the Supreme Court established this basic principle – the "reasonable suspicion" requirement – to govern "stop and frisk" encounters.[107] Today, cadets in every police academy in the United States learn it. To satisfy the requirement, "an officer 'point[s] to specific and articulable facts which, taken together with rational inferences from those facts, evince more than an inchoate and unparticularized suspicion or hunch of criminal activity.'"[108]

The reasonable suspicion standard is not a particularly high bar to clear. But history shows that when police departments deviate from this principle, there are abuses. In the 1960s and 70s, for example, the NYPD engaged in widespread surveillance of political activists and organizations, including anti-war demonstrators, gay rights advocates, and other "activist" groups.[109] In Chicago, the police operated a "Red Squad" that monitored political and social activities for decades, targeting everyone from alleged anarchists and communists to the American Civil Liberties Union (ACLU) and the National Association for the Advancement of Colored People (NAACP).[110] And in Los Angeles, the police department's Public

Disorder Intelligence Division infiltrated anti-war groups, monitored unions and student groups, spied on the city's mayor, and reported on City Council members who criticized the LAPD.[111]

Subsequent lawsuits led to court orders, known as consent decrees, requiring these police departments to demonstrate reasonable suspicion of criminal conduct in order to collect intelligence involving lawful First Amendment activities.[112] The NYPD, in particular, remains subject to a consent decree stemming from a 1971 lawsuit called *Handschu v. Special Services Division*.[113] The decree consists of a set of guidelines, known as the Handschu Guidelines (Guidelines), which regulate NYPD investigations related to political activity. Initially, the Guidelines prohibited the NYPD from investigating a person or group engaged in political activity unless it had "specific information" that the person or group was involved in criminal conduct.[114] However, after 9/11, the NYPD won permission to loosen this restriction for the purpose of combating terrorism, as did the LAPD and Chicago police.[115]

The NYPD now claims the authority to collect information through informants and undercover officers, attend public events without disclosing their presence as police officers, and conduct general topical and online research, all without reasonable suspicion of criminal activity.[116] The most restrictive remaining element of the Guidelines is a prohibition on keeping information obtained at public events that does not relate to unlawful activity.[117] But in a recent deposition, Assistant Chief Thomas Galati cast doubt on whether the Intelligence Division has been following even this rule.[118] Galati testified that none of the information collected and maintained by the Demographics Unit has given rise to an indication of unlawful or terrorist activity that would trigger an investigation,[119] suggesting that the information retained by the NYPD is not about criminal activity and is likely a violation of the *Handschu* consent decree.[120] In February 2013, counsel for *Handschu* plaintiffs sought to enjoin the NYPD's surveillance of Muslim communities and install a court-appointed monitor to oversee NYPD compliance with the consent decree.[121] A declaration by Paul Chevigny, an attorney for the *Handschu* plaintiffs, stated that the NYPD continues to violate the rule against keeping information unrelated to criminal activity as well as rules governing the use of informants to infiltrate and investigate organizations.[122] The litigation is ongoing.

Suspicious Activity Reports

After public criticism caused the LAPD to abandon its plans for NYPD-style community mapping,[123] the department developed a new theoretical construct. Known as a Suspicious Activity Report (SAR), its central feature is information generated from observations by police officers in the normal course of their duties. In other words, police compile information not through targeted surveillance or informants, but from what they see or hear while conducting their usual work. Given the rarity of terrorist attacks in the United States, this may well reflect a pragmatic choice about best practices for resource allocation. Nevertheless, this model too carries risks. Vague and expansive definitions of "suspicious activity" can open the door to a flood of irrelevant information. They can also lead to bias-based reporting as well as an influx of reports on political and religious activity protected by the First Amendment.

From a law enforcement perspective, the appeal of SARs is obvious. A SAR program reduces the opportunity costs of intelligence-led counterterrorism work because officers on the street continue to perform their traditional crime-fighting duties. They can follow protocols for reporting suspicious activity that is potentially related to threats with no substantial diversion from their "core mission of

providing emergency and non-emergency services in order to prevent crime, violence and disorder."[124] SARs also reinforce the notion that every cop is the "eyes and ears" of the national counterterrorism effort. Consequently, both the Justice Department and DHS have encouraged police to adopt standardized SAR programs through the National SAR Initiative (NSI).[125]

Although the notion of SARs has proliferated, only seven of the 16 police departments in the Brennan Center survey have established a formalized SAR program through the NSI. Departments that do not have an official SAR program still collect terrorism-related "tips and leads" and may share that information with a JTTF or fusion center that participates in the NSI. The NYPD, for example, does not participate in the NSI, but it certainly collects "suspicious" information. It has also implemented a public "See Something, Say Something" campaign and has enlisted private businesses in a counterterrorism information-sharing network dubbed "NYPD SHIELD."[126]

Figure 1 identifies which police departments have signed on to participate in the NSI and whether their local rules require officers to suspect wrongdoing before generating intelligence files.

Figure 1. Police Department Involvement in SAR Initiative and Reasonable Suspicion Requirement

Police Departments	Nationwide SAR Initiative Participants[127]	Reasonable Suspicion Requirement[128]
New York City		
Chicago	✓	
Los Angeles County		✓
City of Los Angeles	✓	
Philadelphia	✓	✓
Houston	✓	
Washington, D.C.	✓	
Miami-Dade County	✓	
Detroit		✓
San Francisco		✓
Seattle	✓	✓
City of Miami		
Portland		✓
Minneapolis		✓
St. Paul		Conflicting
Dearborn		✓

Just as intelligence-led policing means different things to different departments, what is considered "suspicious activity" also varies by jurisdiction. While the federal government actively promotes SAR programs through the NSI, it has not been effective in promoting uniformity among police departments with respect to which activities they consider suspicious. Departments do not have consistent rules about whether and when the reasonable suspicion standard is required, and the federal government has not been anxious to clarify its position.[129] As a result, the police in Washington, D.C., use one list of suspicious activities while the police in Los Angeles use another. Meanwhile, the Houston police have their own criteria, which are so broad as to include "any suspicious person or event … determined as suspicious or worthy of reporting by an officer or supervisor."[130]

In Los Angeles, police use SARs to "document any reported or observed behavior/activity that may reveal a nexus to foreign or domestic terrorism."[131] But, as is true with the more intensive intelligence collection practice of New York, the "suspicious activity" recorded need not be linked to any specific plot or target. The LAPD's list of suspicious activities includes some common sense indicators such as the theft of badges or uniforms, presenting false identification, breaching protected facilities, and making threats.[132] However, it also includes such innocuous and non-criminal activities as photography, looking through binoculars, and taking notes.[133] With such a broad view of terrorism-related activities, officers are more likely to stop, detain, and report individuals exercising their First Amendment rights based on bias, which in turn increases the likelihood that irrelevant information will enter the system.[134]

The LAPD acknowledges that the First Amendment may protect these "non-criminal" behaviors, but it instructs officers to report them anyway if they are "reasonably indicative of suspicious activity associated with terrorism."[135] The "reasonably indicative" standard is not well understood, and it has been interpreted as less stringent than the "reasonable suspicion" standard, a well-established rule requiring officers to suspect criminal activity before conducting a *Terry* stop ("stop and frisk").[136] The first-ever audit of the LAPD's SAR program in 2013 defined "reasonably indicative" as "the totality of the circumstances which creates in the mind of the reasonable observer an articulable concern that the observed behavior is terrorism-related."[137] But with such an expansive list of "terrorism-related" behaviors, this standard offers little comfort or clarification.[138]

Why Reasonable Suspicion?

The absence of a reasonable suspicion requirement for documenting and sharing counterterrorism information for SARs can render a department's intelligence activities rudderless. As described by former CIA assistant director Mark Lowenthal, the operating philosophy is very often "don't let bad things happen," which is "hardly a compelling analytical doctrine."[139] If there is no suspicion of criminal activity – past, present, or future – then the basic rationale and natural focus for local police intelligence fades away. In its place are often vague or misguided conceptions of the threat posed by terrorism.[140]

In Los Angeles, for example, the city's regional fusion center determined that only 2 percent of the SARs generated by the LAPD between 2008 and 2010 had an articulable connection to terrorism.[141] Nonetheless, the LAPD retained 98 percent of the SARs in its intelligence files, purging just 66 of 2,734 records.[142]

Such broad standards can also open the door to racial and religious profiling. The ACLU raised this concern in a letter to LAPD Chief Charlie Beck, noting that "the SAR program invites officers to use their own hunches and subjective judgments about which photographers might be terrorists, judgments that will necessarily be informed by biases, even if unconsciously formed."[143] And in New York, there are now three federal lawsuits involving allegations that the NYPD's intelligence program singled out American Muslims for scrutiny for no reason other than their religion.[144]

The NYPD maintains that its surveillance of Muslims is justified because the "majority of recent terror plots have either been carried out or planned by Islamists who have been radicalized to violence."[145] But a landmark ruling against the department on its controversial "stop and frisk" program casts doubt on this defense. In the stop and frisk case, the NYPD said it encouraged officers to stop young black and Hispanic young men because doing so was consistent with the racial composition of crime suspects.[146] The court found that this program was a form of racial profiling and that it is "impermissible to subject all members of a racially defined group to heightened police enforcement because some members of that group are criminals."[147] Instead, the court reiterated that police must base their stops on reasonable suspicion, which works to remove bias from the equation by requiring officers to have "a minimal level of objective justification" for their activity.[148] One's race or religion, without more, is insufficient.

Intelligence-led policing does not – and should not – necessitate targeting communities or beliefs. The LASD, for example, relies on "criminal based intelligence."[149] According to the department's intelligence guidelines, officers cannot collect information about "political, religious, social views, associations or activities" unless it is "related directly to the criminal predicate which is the basis for focusing on the individual or group."[150]

The intent of this rule is not to hamstring law enforcement. The reasonable suspicion standard does not prevent police from responding to emergency calls or following up on the tips and leads they receive. It does not prevent officers from retaining information identifying witnesses, victims, or the location of crimes, assuming there is a criminal predicate.[151] It also does not apply to other types of records regularly maintained by police departments such as accident reports or 911 calls. It simply directs officers not to create or share intelligence files when the inquiry is unmoored from any suspicion of criminal activity.

Given their mandate to enforce the criminal law, this baseline requirement makes sense for state and local police departments. In fact, congressional research suggests that of all the counterterrorism roles that law enforcement agencies can play, "identifying terrorist precursor crimes is perhaps the most natural."[152] Irrespective of ideology, terrorist groups engage in a series of *illegal* activities to sustain themselves and plan attacks.[153] These crimes include "various fraud schemes, petty crime, identity and immigration crimes, the counterfeit of goods, narcotics trade, and illegal weapons procurement."[154] Local law enforcement agencies are in a good position to identify these precursor crimes, and the reasonable suspicion requirement is a fitting guide. Moreover, pursuing these offenses and sharing information about them will have the added benefit of reinforcing traditional law enforcement functions.

In short, the reasonable suspicion requirement serves an important function. Like a compass, it directs scarce resources away from conjectural or unsubstantiated threats. It separates the wheat from the chaff, preventing irrelevant or useless information from "clogging the system."[155] It is a standard to embrace, not an obstacle to overcome.[156]

* * *

Overall, although about half of the police departments in this survey use the reasonable suspicion standard quite successfully, there is no overall agreement among departments about what information to collect and share. This is deeply problematic given the overall trend toward intelligence-led policing and the national push to share information broadly. If the ultimate goal is to create a system in which law enforcement agencies at all levels of government share terrorism-related information, there must be clear rules that all participants can embrace. The reasonable suspicion standard is that well-established common denominator.

II. INFORMATION SHARING: FUSION CENTERS AND JOINT TERRORISM TASK FORCES

There are two primary institutions for sharing counterterrorism information among federal, state, and local law enforcement agencies: "fusion centers" funded by the Department of Justice and DHS, and Joint Terrorism Task Forces (JTTFs) led by the FBI. These entities work closely with one another, often located in the same building. They also have some overlapping responsibilities that can create competition for information, promote confusion about the rules, and lead to the proliferation of bad data without adequate oversight.

The mission of fusion centers, most of which did not exist until 2006, is not uniform or particularly well defined.[157] According to guidelines issued by the DOJ and DHS, a fusion center is a "collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity."[158] State or local agencies are responsible for establishing fusion centers, but they receive significant funding from the federal government and representatives from all levels of law enforcement participate in them (Wyoming is the lone holdout).[159] Since 2001, 49 states, 3 territories, and 26 major urban centers have created fusion centers.[160]

JTTFs are FBI-led partnerships among federal, state, and local agencies whose primary mission is to detect, prevent, and investigate acts of terrorism within their jurisdiction. JTTFs operate locally and serve as a conduit for the federal government to exchange information with state and local law enforcement.[161] There are now 103 JTTFs, including 71 established after 9/11.[162] Although a comprehensive assessment of JTTF operations is beyond the scope of this report, it is important to recognize the prominence of the FBI's "eGuardian" information sharing system, which competes with the national network of fusion center "Shared Spaces" and operates according to different rules.

From a state and local perspective, fusion centers and JTTFs serve as critical links to the federal intelligence community. However, the decentralized structure of these partnerships, combined with a distinct oversight deficit, poses significant concerns. Weak standards and inconsistent rules for collecting and sharing information produce inconsistent and poor-quality intelligence, much of which targets non-criminal activities. Untethered from the reasonable suspicion requirement, fusion centers may report "suspicious" activities to their local JTTF for investigation, including activities protected by the First Amendment, often on the basis of misguided notions about the role of race, ethnicity, religion, or political ideology as a terrorism indicator.

Fusion Centers

Although fusion centers were started with federal funding, they are not under federal government control. The state or local agency that establishes a fusion center determines its policies and purpose. The federal government takes the view that it cannot directly control fusion centers for the same reason it cannot directly control a local police department: the Constitution prohibits federal "commandeering" of state resources. [163] This doctrine may also preclude the federal government from directly setting rules for fusion centers – except, of course, through federal funding requirements. Notably, the federal government has not aggressively pursued the latter option. On the contrary, it seems to have deliberately

taken a back seat, failing to track how federal grants are allocated and spent, and leaving fusion centers to their own devices in ensuring compliance with federal privacy guidelines.[164] Federal funds for fusion centers simply flow to state legislatures, which allocate them as they see fit. This positions the federal government at arm's length from fusion centers. It has also generated great confusion when it comes to determining which rules apply and how.

Fusion Center Overview

The first National Criminal Intelligence Sharing Plan, issued in 2003, emphasized the new role of state and local law enforcement in domestic intelligence. This plan was the basis for the 2006 federal fusion center guidelines.[165] The guidelines called for the creation of "a collaborative environment for the sharing of intelligence and information among local, state, tribal, and federal law enforcement agencies, public safety agencies, and the private sector."[166] They also instructed fusion centers to "[l]everage the databases, systems, and networks available via participating entities," including "driver's license information, motor vehicle registration data, location information, law enforcement and criminal justice systems or networks, and correctional data."[167]

With the exception of large cities such as New York and Los Angeles, state police usually play the lead role in sub-federal homeland security initiatives.[168] As a result, fusion centers have been the primary vehicles for state contributions to counterterrorism intelligence. Although there is no uniformity, fusion centers usually include officers from state and local law enforcement agencies, the DHS Office of Intelligence and Analysis, the FBI Field Intelligence Group (FIG) and JTTF, and the National Guard, as well as civilian analysts, members of the military, and private companies. Beginning with a pilot program in Los Angeles, many local law enforcement agencies have also designated Terrorism Liaison Officers (TLOs) to serve as the primary point of contact for terrorism information sharing with fusion centers and to relay information, such as SARs, between the police, fusion center, and JTTF.[169]

Some city police departments have established their own fusion centers to cover their jurisdictions, such as Los Angeles, Chicago, Houston, and Miami-Dade. These "regional" fusion centers typically serve as "nodes" that are responsible for major urban areas and work closely with their state-run counterparts.[170] Figure 2 (opposite) lists the fusion centers associated with police departments in the Brennan Center survey.

Technically, each fusion center operates according to the laws of the state and municipality where it is located. Each fusion center is therefore unique, and each has developed its own rules for the collection, storage, and sharing of intelligence information. Some state or local laws are more protective of civil rights and civil liberties than the rules applied in other jurisdictions, or even federal rules. Some agencies require reasonable suspicion to collect intelligence on religious and political activities while others do not. Some utilize the SAR reporting process while others do not. Some share information automatically with FBI, while others seek to retain control of their data.[171]

Figure 2. Police Departments and Affiliated Fusion Centers

Police Departments	Regional (Recognized) Fusion Center	State (Primary) Fusion Center
New York City*	-	New York State Intelligence Center
Chicago	Crime Prevention and Information Center	Illinois Statewide Terrorism and Intelligence Center
Los Angeles County	Los Angeles Joint Regional Intelligence Center	California State Terrorism Threat Assessment Center
City of Los Angeles	Los Angeles Joint Regional Intelligence Center	California State Terrorism Threat Assessment Center
Philadelphia	Delaware Valley Intelligence Center	Pennsylvania Criminal Intelligence Center
Houston**	Houston Regional Intelligence Service Center	Texas Fusion Center
Washington, D.C.	Washington Regional Threat and Analysis Center	-
Miami-Dade County	Southeast Florida Fusion Center	Florida Fusion Center
Detroit	Detroit and Southeast Michigan Information and Intelligence Center	Michigan Intelligence Operations Center
San Francisco	Northern California Regional Intelligence Center	California State Threat Assessment Center
Seattle	-	Washington State Fusion Center
City of Miami	-	Florida Fusion Center
Portland	-	Oregon Terrorism Information Threat Assessment Network
Minneapolis	Strategic Information Center	Minnesota Joint Analysis Center
St. Paul	Strategic Information Center	Minnesota Joint Analysis Center
Dearborn	-	Michigan Intelligence Operations Center

* DHS will only recognize fusion centers that have been formally "designated" as such by their state governors. *See Fusion Centers and Contact Information*, U.S. Dep't of Homeland Sec., http://www.dhs.gov/fusion-center-locations-and-contact-information (last visited Mar. 7, 2013). Although the NYPD's Intelligence Division functions like a fusion center, it has not been designated by New York State as a fusion center. It is therefore not recognized by DHS as part of the nationwide fusion center structure. *See* Dan Verton, *Is It Time for the Federal Government to Rein in the NYPD?*, AOL Gov't (Oct. 13, 2011), http://gov.aol.com/2011/10/13/is-it-time-for-the-feds-to-rein-in-the-nypd/. As a consequence, the NYPD is not bound by federal privacy requirements that apply to "recognized" fusion centers receiving federal funding through the Homeland Security Grant Program. *See* Nat'l Criminal Intelligence Res. Ctr., DHS/DOJ Fusion Process Technical Assistance Program and Services 2 (n.d.), *available at* http://ise.gov/sites/default/files/Fact_Sheet_Enhancing_the_Privacy_for_State_and_Major_Urban_Area_FCs.pdf.

** Many of the regional fusion centers evolved out of local intelligence units. For example, the Homeland Security Bureau of the Miami-Dade Police Department *is* the Southeast Florida Fusion Center. Similarly, the Houston Regional Intelligence Service Fusion Center grew out of an intelligence unit in the Houston Police Department (HPD) that later became the HPD's Intelligence Division.

This uneven foundation has introduced a degree of disorder into the domestic intelligence structure built upon it. Because of different rules and practices about what information to collect, any effort to "fuse" this information will have variable results. A recent Senate investigation concluded that the quality of information produced by fusion centers has generally been shoddy.[172] Moreover, the investigation found that police have often needlessly intruded into Americans' privacy and impinged upon First Amendment-protected activity in the process.[173] Fusion centers are also increasingly under pressure as federal funds dry up and state legislatures seek to cut fat from their budgets. At least two fusion centers covered by this survey, Oregon and Texas, have been on the cusp of closing due to fiscal constraints and concerns about effectiveness.[174]

In reality, the overwhelming majority of fusion center staff does not even believe counterterrorism is their primary function. According to a 2012 survey of fusion center employees, only 28 percent said counterterrorism was their most important activity.[175] Instead, most fusion centers now have a broader purpose: to fight "all crimes" or coordinate and consolidate information and action on "all hazards," including, for example, disasters such as tornadoes or hurricanes.

This expansion is pragmatic. Simply put, there is not enough terrorism-related work for fusion centers. Sacramento police Lieutenant Milton Nenneman, who conducted a DHS-funded study of fusion centers at the Naval Postgraduate School, concluded that there is "insufficient purely 'terrorist' activity to support a multi-jurisdictional, multi-governmental level fusion center that exclusively processes terrorist activity." [176] In fact, with a counterterrorism-only diet, intelligence "analysts' skills would atrophy, as would their interest, from a lack of relevant work," Nenneman found. Since terrorism is relatively rare, an expanded mission increases possible funding sources and additional rationales for their continued operation.

From a national security perspective, however, broadening fusion centers' missions has the potential to dilute their potency as a counterterrorism tool. Information-sharing specific to terrorism may become less robust,[177] or lead to information overload, in which data is insufficiently scrutinized before is distributed. In fact, some say poor analysis is already a problem. A 2012 study by the Homeland Security Policy Institute concluded, "fusion centers excel at the dissemination of information, yet lack the analytical capabilities needed to fulfill their mandate to assess the local implications of threats."[178]

The Information Sharing Environment

In 2007, Congress passed the 9/11 Commission Act, which called for the creation of a new computer system to share information.[179] This network, the Information Sharing Environment (ISE), links fusion centers to the federal government and to each other. From the federal perspective, fusion centers help "connect the dots" by aggregating state and local counterterrorism information in searchable form on the ISE. The ISE links state and local law enforcement databases nationwide with various federal agencies and is intended to foster exchange of terrorism-related intelligence among all levels of government.

The ISE consists of "Shared Spaces" that are roughly analogous to personal folders on a shared computer server. Although accessible to other users, each individual is responsible for the contents of his or her own folder. Each fusion center has at least one Shared Space and can query other Shared Spaces, such as those operated by federal agencies and other fusion centers.[180] At the urging of the federal government,[181] 68 fusion centers have developed the ability to contribute and share SAR information through their Shared Spaces on the ISE.[182] This expands the reach of the National SAR Initiative to "over 14,000 law enforcement agencies in 46 states, including the District of Columbia."[183]

A "Functional Standard" developed at the national level dictates what information should be shared on the ISE. Under its provisions, SARs are included on ISE if they have a "potential nexus to terrorism." Fusion center officials determine whether their SARs meet this standard based on a list of 16 "suspicious activities" that include both criminal and non-criminal activities as well as some activities protected by the First Amendment.[184] A SAR that satisfies the Functional Standard is known as an "ISE-SAR."[185] SARs that do not satisfy the Functional Standard are not supposed to be shared on the ISE. However, what police departments do with the leftover information depends entirely on their local laws, policies, and procedures. Some departments will segregate the deficient reports on an internal database for further review. Some will not keep them at all. Others will bypass the Functional Standard and share the information directly with the FBI, which operates its own information sharing networks, "Guardian" and "eGuardian." As a result, there is still considerable variation in the types of SAR information collected and shared, subverting the purpose of a national standard and making quality control far more difficult.

A key feature of the ISE is that information stored on a Shared Space, *e.g.*, an ISE-SAR, is supposed to be under the control of the agency that produced it. In theory, this means the facts will remain accurate and up to date. If an ISE-SAR is no longer accurate or relevant, the agency has a responsibility to correct it or purge it from the ISE in order to ensure that bad data does not generate poor intelligence.[186] In practice, however, information updates may not happen for years.[187] Divergent rules and a lack of independent oversight also create wide variation in the quality and usefulness of the information shared.[188] Indeed, the ISE operates on the premise that fusion centers and law enforcement agencies will generate SARs based on their own laws and policies. The ISE is simply a platform to share and disseminate information that meets a minimum standard.[189]

The concern with such a decentralized system is that the participants are all playing by their own rules, or at least their own interpretation of them. A 2008 survey sponsored by DOJ and DHS concluded that among the Los Angeles, Chicago, Boston, and Miami-Dade police departments:

> Each agency employed different intake and preliminary review procedures to determine whether a report actually had a "potential" connection with terrorist activity subject to special treatment. In addition, … 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 [the reasonable suspicion requirement].[190]

This is still true today. In the absence of any significant federal, state, or local oversight, fusion centers continue to play by their own rules.[191]

Some police departments clearly collect intelligence information about constitutionally protected activities without a criminal predicate. Some have collected this information based on religion and ethnicity. And some fusion centers may share this information in the ISE. Intentionally or not, the federal government has facilitated this situation and has not fulfilled its obligation to prevent it from continuing to happen.

Joint Terrorism Task Forces

Unlike fusion centers, JTTFs conduct their own terrorism investigations and federal agents may collect their own intelligence according to federal guidelines. But police officers assigned to a JTTF must serve two masters. They remain bound by state and local laws while operating in a unit that follows FBI rules. In addition to the concern that state and local laws may conflict with the federal rules, the secrecy surrounding JTTF operations limits the ability of police officers to raise concerns with local supervisors, which undermines local oversight. Moreover, JTTFs duplicate some of the functions of fusion centers without heeding state and local privacy laws. Many JTTFs receive the same reports that fusion centers post on ISE Shared Spaces. But unlike information stored on a Shared Space, the FBI copies fusion center data, keeps it for longer than state or local laws might otherwise permit, and limits a fusion center's ability to update or correct bad information.[192]

JTTFs include more than 4,400 federal, state, and local officials from over 600 different agencies.[193] They also include analysts from Field Intelligence Groups (FIGs) at each of the FBI's 56 field offices who help direct JTTF efforts by assessing "raw" intelligence gleaned from FBI sources and case files.[194] According to a 2012 study by the Homeland Security Policy Institute, JTTFs were the second most important source for counterterrorism information for fusion center staffers, preceded only by local law enforcement. Some JTTFs are even "co-located" with fusion centers, meaning that they operate out of the same physical office or building.[195]

Guardian and eGuardian

The FBI has created its own information sharing networks, known as "Guardian" and "eGuardian,"[196] which operate in addition to (and often compete with) the ISE Shared Space system.[197] eGuardian is an unclassified network designed to receive SARs directly from fusion centers and convey them to the appropriate JTTF,[198] regardless of whether they meet the ISE Functional Standard requirements.[199]

Guardian is a classified version of the network that copies fusion center data from eGuardian.[200] Fusion centers have the option of sharing SAR information through an ISE Shared Space, eGuardian, or both.[201]

Paradoxically, eGuardian is both independent from and a part of the ISE. It exists as a stand-alone FBI database, accessible to fusion centers and JTTFs through its own web portal, Law Enforcement Online (LEO).[202] At the same time, the FBI has also configured eGuardian to operate on the ISE as if it were a Shared Space, allowing other fusion centers and JTTFs to search its records and upload ISE-SARs. However, unlike other ISE Shared Spaces, all of the reports submitted to eGuardian are copied to the classified Guardian database, thereby maintaining the data wholly within the Bureau's control. Even reports with no nexus to terrorism may be retained in eGuardian for 180 days, after which they are "deleted" and moved to the Guardian system, where they are kept for at least five years. [203] And after the record is "deleted" from Guardian, it is retained for another 30 years in the FBI's case management system.[204]

This data retention policy limits the ability of fusion centers to control information they share on the ISE, to update it, correct it, purge it, or limit access to it. It also raises serious concerns about the persistence of inaccurate or outdated information and presents a legal conflict for fusion centers, which are subject to state and local laws requiring police to maintain control of the intelligence information they share.[205]

It is important to recognize that the FBI uses its own criteria to determine whether to share information on the ISE through its eGuardian Shared Space. All other participants in the ISE must adhere to the Functional Standard, but eGuardian follows its own set of rules based on FBI investigative guidelines.[206] It defines "suspicious activity" as "behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal or other illicit intention."[207] Although the FBI contends that this rule is "generally consistent" with the Functional Standard,[208] it is in fact much broader. According to FBI officials, "certain terrorism-related activities – such as those related to terrorist financing, known terrorism subject location, and past terrorism event information – currently are not among the behavior-based criteria in the Functional Standard but would meet the FBI's guidelines."[209] Moreover, some JTTFs have explicitly told fusion centers to "provide all potentially terrorism-related information and not just ISE-SARs that [meet] the Functional Standard."[210] As a result, there is growing concern that Guardian and eGuardian networks provide an end-run around the Functional Standard, lowering the bar for sharing information on the ISE.

In sum, it is clear that eGuardian is competing with the ISE Shared Space system initially promoted by DHS.[211] A 2013 report from the Government Accountability Office found that the two systems offer "duplicative services," warning that information could inadvertently fall through the cracks.[212] Another concern is, of course, that duplicate systems with different rules sows confusion and results in a lack of transparency about how information is being shared among law enforcement agencies.

Quality Control and Civil Liberties

It is beyond question that there is a need to coordinate counterterrorism intelligence information. However, the standards for collecting and disseminating that information are so lax and variable that they not only endanger civil liberties, but risk hobbling the entire enterprise.[213] Harold "Skip" Vandover, the former DHS official in charge of reviewing fusion center reports, could not have been blunter when he told the Senate Homeland Security Committee "a bunch of crap is coming through."[214]

The Senate Homeland Security Committee published a bipartisan report in 2012 that supported Mr. Vandover's assessment, determining that many of the reports produced by fusion centers have been useless and potentially illegal.[215] This finding is reminiscent of the Church Committee report on intelligence abuses nearly 40 years ago. The Church Committee reached the conclusion that "the dissemination of large amounts of relatively useless or totally irrelevant information has reduced the efficiency of the intelligence process."[216] It also noted that "the dissemination practices of some local law enforcement agencies" resulted in federal agencies accumulating "inherently inaccurate and distortive data."[217]

Part of the problem today is the use of vague and poorly understood standards for placing information on the ISE. In order for a fusion center to share a report on the ISE, the Functional Standard requires that information have a "potential terrorism nexus."[218] Of course, virtually all information has a *potential* link to terrorism, including everyday activities such as taking photographs or dining out with a group of friends. More specifically, information posted to the ISE must be "*reasonably indicative* of criminal activity associated with terrorism, including evidence of pre-operational planning related to terrorism."[219]

While the Functional Standard appears to narrow the window for inclusion, in practice there is no requirement that the information be related to an actual or planned crime. According to the DOJ, information that flows through the ISE need "not be indicative of a potential crime," provided that it might help prevent a potential act of terrorism "when collated and analyzed with correlating pieces of data from other sources."[220] Consequently, there has been a regular problem with reporting and improperly characterizing First Amendment-protected activities without a nexus to violence or criminality.[221]

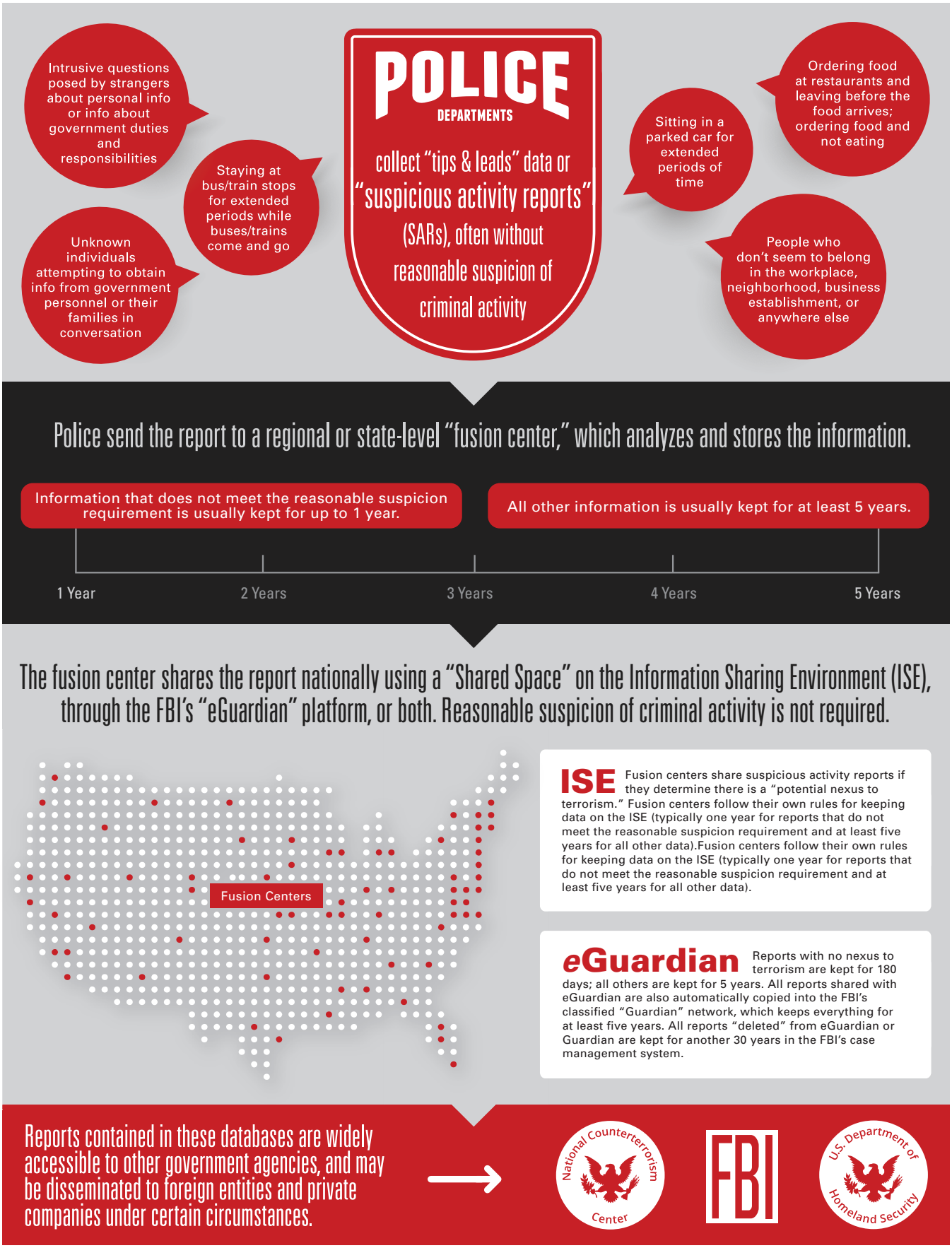
After a revision in 2009, the Functional Standard won some praise from civil liberties groups.[222] For one thing, it now includes a footnote recognizing that "[r]ace, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion."[223] It also acknowledges that First Amendment protected behaviors such as photography and asking questions require some articulable facts that support a connection to terrorism.[224] Nonetheless, it explicitly instructs state and local law enforcement that SARs shared on the ISE "may or may not meet the reasonable suspicion standard for criminal intelligence information."[225]

The difference between the "reasonably indicative" standard used in the Functional Standard and the "reasonable suspicion" standard used in typical criminal investigations is larger than it appears. Since the Supreme Court decided *Terry v. Ohio* in 1968, "reasonable suspicion" has become a fixture in police vocabulary.[226] By contrast, there is no common definition of the "reasonably indicative" standard. While there is little public information about individual SARs shared through the ISE or eGuardian, there is ample evidence that fusion centers continue to collect personal information without a criminal predicate.

For example, even with the revised Functional Standard in place, police officers throughout California have been encouraged to document and immediately report suspicious "surveillance activities." From the LAPD's *Characteristics of Terrorists Surveillance*,[227] police officers should report:

- Individuals who stay at bus or train stops for extended periods while buses and trains come and go;

Figure 3. State and Local Information Sharing Network



- Individuals who carry on long conversations on pay or cellular telephones;
- Individuals who order food at a restaurant and leave before the food arrives or who order without eating; and
- Joggers who stand and stretch for an inordinate amount of time.

Such activities may be "evidence of pre-operational planning related to terrorism"[228] or evidence of a sore hamstring, but in either case, they do not amount to reasonable suspicion of criminal activity.

In an interview with the Brennan Center, Mike Sena, director of the Northern California Regional Intelligence Center (NCRIC), confirmed that SARs shared on the ISE or eGuardian may not meet the reasonable suspicion requirement. Sena, who is also the president of the National Fusion Center Association, added that the NCRIC does not include personally identifiable information in such reports, but recognized that other fusion centers do include this information.[229] Indeed, the Functional Standard does not require fusion centers to omit personal information from SARs when there is insufficient evidence of a terrorism-related crime, leaving it up to each fusion center or police department to apply its own rules.[230]

Centers as careful about information sharing as the NCRIC appear to be the exception and not the rule. According to the 2012 Senate report, DHS employees shared information about reading suggestions by a Muslim community group, information about a motorcycle club leaflet advising what to do if pulled over by police, and information about a U.S. citizen lecturing at a mosque. [231] Also included was a report on a Muslim organization hosting a daylong seminar on marriage.[232]

Some officials have decried the reasonable suspicion requirement as an impediment to effective counterterrorism intelligence, citing the need to "connect the dots" or create a "mosaic" of all available threat information in order to unearth terrorist plots.[233] But the Senate report found that this approach has "yielded little, if any, benefit to federal counterterrorism efforts." Reviewing 13 months worth of fusion center reporting, the Senate determined that "DHS-assigned detailees to the centers forwarded 'intelligence' of uneven quality – oftentimes shoddy, rarely timely, sometimes endangering citizens' civil liberties and Privacy Act protections, occasionally taken from already-published public sources, and more often than not unrelated to terrorism."[234]

There is also no official data on the effectiveness of the FBI's eGuardian network, which employs a rule for sharing information that is even more permissive than the Functional Standard.[235] Two government surveys have found that eGuardian is the preferred platform among fusion centers,[236] but the Justice Department has not even attempted to track the role of SARs in deterring terrorist activities. In short, there are no means for establishing the efficacy of the eGuardian system.[237] The most detailed figures available indicate that of the thousands of suspicious activity reports generated by police departments and fusion centers, just 4.8 percent of ISE-SARs result in FBI investigations.[238] There is no data on whether these investigations led to arrests or convictions.[239] This modest figure suggests a proliferation of innocuous information, a profound lack of manpower, or some combination of the two.

The History of 28 CFR 23

More than 30 years ago, policymakers recognized the significance of the reasonable suspicion requirement, making it the touchstone for a set of guidelines on sharing criminal intelligence information among law enforcement agencies. A 1980 federal regulation, *Criminal Intelligence Systems Operating Policies,* prohibits collecting or retaining "criminal intelligence information" that does not meet the reasonable suspicion threshold.[240] Codified at 28 CFR 23, it specifically prohibits collecting or retaining First Amendment activities information "about 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 and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity."[241]

Even though the information they collect and retain is precisely the type of information that should be kept out of federal intelligence sharing networks, fusion centers and JTTFs have been able to sidestep the constraints of 28 CFR 23 in two ways. First, 28 CFR 23 only applies to networks that receive funding from the Omnibus Crime Control and Safe Streets Act of 1968, which the ISE and eGuardian do not.[242] Fusion centers receive federal funds through other grant programs, such as the State Homeland Security Program and the Urban Areas Security Initiative. Second, the government has essentially defined away the problem. Official guidance from the Department of Justice asserts that 28 CFR 23 applies only to "criminal intelligence" information, which supposedly does not include "tips and leads" data such as SARs.[243] A 2007 "Tips and Leads Issue Paper" published by the Justice Department, claims that "tips and leads" that do not rise to level of reasonable suspicion may be recorded and maintained "in a secure system similar to data that rises to the level of reasonable suspicion."[244]

Police officers have always collected "tips and leads." Dubbed "temporary" or "working" files, officers would conduct a quick follow-up to determine whether further investigation was warranted, and if not – if there was still no reasonable suspicion of criminal activity – they would discard the information.[245] Today, however, these records frequently find their way into the ISE and eGuardian despite fusion center privacy policies professing compliance with 28 CFR 23. In fact, the FBI has actively encouraged fusion centers to disseminate "tips and leads" information that does not meet the reasonable suspicion requirement. FBI documents distributed at the 2009 National Fusion Center Conference make the dubious claim that "[i] nformation that is deemed inconclusive will be maintained in eGuardian for a maximum of five years in accordance with [28 CFR 23]."[246] But 28 CFR 23 does not mention "tips and leads" and explicitly prohibits retaining records for any length of time that do not meet the reasonable suspicion standard.[247]

Consequently, fusion centers operate in a "gray area" of the law[248] – freed from compliance with the reasonable suspicion requirement of 28 CFR 23 while subject to state and local laws that vary considerably. To its credit, DHS has used grant-funding requirements to mandate that fusion centers establish privacy policies consistent with federal guidelines.[249] Indeed, almost all fusion centers have now established privacy policies stating they comply with 28 CFR 23 "as applicable." However, in light of the Justice Department's guidance, which states that 28 CFR 23 is inapplicable to "tips and leads," this statement is more form than substance.

Fusion centers have embraced the idea that "tips and leads" data (including SARs) is not criminal intelligence as defined by 28 CFR 23.[250] In Los Angeles, for example, the LAPD may report individuals for taking photographs of national landmarks, regardless of whether there is reasonable suspicion of criminal activity. The resulting SAR is shared with the Joint Regional Intelligence Center (JRIC), the regional fusion center for Los Angeles. In theory, the JRIC unequivocally adheres to 28 CFR 23.[251] But as is true of every fusion center in California, it also permits "temporary files" to be maintained for up to one year and shared as an ISE-SAR during that time.[252] Houston's fusion center, the Houston Regional Intelligence Service Center (HRISC), also professes to follow to 28 CFR 23.[253] But it too maintains intelligence information that does not meet the reasonable suspicion threshold for one year.[254] Moreover, if shared with the FBI's eGuardian network, the bureau can keep any of this information for at least five years.[255]

The Origins of 28 CFR 23

28 CFR 23 derives from a set of guidelines first developed in 1978 by the now-defunct Law Enforcement Assistance Administration (LEAA), an arm of the Department of Justice that administered the first federally funded criminal intelligence networks. The express purpose of the LEAA guidelines was to mitigate "the potential privacy violations surrounding the collection of criminal intelligence information."[256] Specifically, the guidelines sought to address such "basic concerns" by requiring intelligence information to "be relevant to criminal activity" and not "collected or stored in violation of First Amendment rights."[257]

In 1980, the LEAA guidelines were codified as 28 CFR 23.[258] According to the Justice Department's own position in 1993, "the potential for national dissemination of information in intelligence information systems, coupled with the lack of access by subjects to challenge the information, justifies the reasonable suspicion standard as well as other operating principle restrictions set forth in this regulation [28 CFR 23]." The Department also noted that "the quality and utility of 'hits' in an information system is enhanced by the reasonable suspicion requirement," adding that "[s]carce resources are not wasted by agencies in coordinating information on subjects for whom information is vague, incomplete and conjectural."[259]

As a practical matter, this approach to processing tips and leads data has considerable appeal. Police officers who receive a tip or lead must have an opportunity to conduct a limited inquiry to determine if further investigation is necessary. But extending this concept to a networked system of maintaining and sharing files, encouraging law enforcement agencies to maintain and disseminate such "temporary" files as if they were predicated criminal intelligence records, is antithetical to both the history and purpose of 28 CFR 23. It is also harmful to both national security and civil liberties. It is not a coincidence that the reports produced by fusion centers have been full of irrelevant information. Indeed, there is mounting evidence that the deluge of information may be overwhelming analysts rather than helping them "connect the dots."[260] The reasonable suspicion standard is as much a bulwark against abuse as it is a filter for bad information. All levels of government should embrace it and establish robust oversight mechanisms to enforce it.

III. LOCAL LAW ENFORCEMENT OVERSIGHT MECHANISMS

To have a full appreciation of the mechanics of police oversight, a little history is in order. Although the U.S. adopted some precepts of the British model of policing, a significant difference is that local law enforcement in America is highly decentralized and an extension of municipal politics. As policing expert Cynthia Brown has noted, "Initially, the police were an extension not of local government, but of the different political factions that made up municipal government. It was the local political leaders in a particular ward or precinct that recruited and selected police officers."[261] Not surprisingly, this patronage led to selective enforcement and corruption. From about 1920 to 1960, police departments underwent a wave of reform, replacing the political model with a "professional" and "legalistic" one. This transformation, which also ushered in the era of community policing, brought oversight along with it. Nonetheless, an absence of uniformity remains. Each jurisdiction sets its own policies. Generally, but not always, the intensity of oversight seems to be a function of past police department abuses.

None of the current oversight mechanisms, however, are especially well suited to monitoring state and local counterterrorism intelligence activities. Merrick Bobb, Special Counsel to the LASD Board of Supervisors and court-appointed monitor for the Seattle Police Department,[262] has explained that police oversight can be divided into three categories: (1) the review and appellate model; (2) the investigative and quality assurance model; and (3) the evaluative and performance-based model.[263] The table below uses these categories to show the oversight mechanisms of the departments in the Brennan Center survey. Some departments fall into more than one category.

Figure 4. Oversight Models by Police Department

Police Departments	Review and Appellate	Investigative and Quality Assurance	Evaluative and Performance-Based
New York City		✓	
Chicago	✓	✓	
Los Angeles County	✓	✓	✓
City of Los Angeles		✓	✓
Philadelphia		✓*	
Houston	✓		
Washington, D.C.		✓	
Miami-Dade County**			
Detroit		✓	
San Francisco		✓	
Seattle	✓	✓	✓
City of Miami		✓	
Portland	✓	✓	
Minneapolis		✓	
St. Paul	✓		
Dearborn***			

* Police Advisory Commission. Note that the Commission includes an Integrity and Accountability Office that shares some features with the evaluative and performance-based model. It is directed by an employee of the police department and has produced only seven reports since 1997, the last of which was published in 2004.

** The Miami-Dade Police Department used to have an Independent Review Panel that followed the Review & Appellate Model. However, it was eliminated in 2009 due to countywide budget cuts, leaving the police department without any form of external civilian oversight.

*** The Dearborn Police Department has no civilian oversight body, relying only on its Internal Affairs Unit to investigate civilian complaints.

Review and Appellate Model

Departments that use the review and appellate oversight model typically rely on boards to review internal investigations of individual complaints. These boards, often composed of civilians and police officers, generally lack the authority to receive complaints or conduct their own investigations. Subpoena power is also rare. The boards are usually limited to recommending whether to sustain, reverse, or remand for additional investigation an internal police probe.[264]

The Houston Independent Police Oversight Board is typical of this approach. This 20-member civilian board, appointed by the mayor, reviews all major internal investigations to "determine if the investigation was sufficient and the conclusions were correct."[265] It can make nonbinding disciplinary recommendations or request additional investigation by the police, and if necessary, by the city's Inspector General.[266] The board is new, created in 2011 after the disclosure of video showing four Houston police officers beating a 15-year old burglary suspect. Although intended to operate independently from the police, its lack of subpoena power and investigative authority has raised concerns about its effectiveness.[267] The board also has no authority to sit in on questioning during an Internal Affairs investigation.

Other examples of the review and appellate models include: the Los Angeles County Ombudsman;[268] the St. Paul Police-Civilian Internal Affairs Review Commission;[269] the Portland Citizen Review Committee;[270] and the Seattle Office of Professional Accountability Auditor.[271] Like Houston's Independent Police Oversight Board, many of these bodies were corrective measures taken in the wake of high-profile episodes of police violence and criticism that the police could not adequately discipline its personnel.[272]

The review and appellate oversight model has had a mixed record of success, due in large part to the focus on individual incidents instead of systemic problems.[273] It is not, however, a good option for intelligence oversight. Whatever the merits of a particular review board, the potential complainant must at least be aware that they have encountered law enforcement. Unlike a traffic stop, for example, virtually all counterterrorism intelligence gathering is covert; subjects are unlikely to be in a position to identify and report misconduct. Even if evidence of abuse came to light, police reluctance to cooperate with investigators could cripple any review.

Additionally, review bodies do not have the power to evaluate underlying policies or procedures that may be indicative of a systemic problem. They "do not, as a rule, look at the department as a whole or search for patterns and practices of police misconduct."[274] While some panels may have limited authority to issue policy recommendations, their focus on discrete instances of misconduct ensures that they do not exercise this power with any frequency.[275]

Lack of access to adequate staff and resources often plagues review boards.[276] While this problem can affect every model of oversight, the process of reviewing individual cases is particularly resource-intensive. At minimum, inadequate funds result in a large backlog of unresolved cases.[277] At worst, fiscal constraints can cause elimination of the board altogether, as was the case in Miami-Dade when budget cuts in 2009 abolished the Independent Review Panel, the department's only form of external civilian oversight.[278]

Investigative and Quality Assurance Models

Departments using the investigative and quality assurance model seek to supplement the internal police disciplinary process, usually called Internal Affairs, by giving investigative authority to an outside entity, such as a civilian board, a group of lawyers/investigators, or an individual.[279] Unlike the appellate and review models, this body can investigate police misconduct on its own and is not limited to reviewing an Internal Affairs investigation.[280] In theory, subpoena power and independent investigative authority provide "teeth" to civilian review of Internal Affairs investigations.[281] This arrangement is often a second stage in the quest for effective oversight, deployed by jurisdictions dissatisfied with a review board.[282]

For counterterrorism intelligence, however, this model has many of the same limitations as the appellate and review model: the boards are generally restricted to oversight of specific cases where there is known misconduct. While some may have the power to address policy issues, they rarely do; and insufficient resources and departmental resistance can hamper their work.[283]

New York City's Civilian Complaint Review Board (CCRB) is a prominent example of the limitations of this brand of oversight. The CCRB devotes almost all of its resources to investigating specific complaints against individual officers and making disciplinary recommendations to the Police Commissioner, who frequently ignores them.[284] It has the power to subpoena documents and witnesses,[285] and the City Charter requires the NYPD to cooperate with CCRB investigations.[286] In practice, however, the CCRB does not issue subpoenas to the NYPD. It relies instead on the cooperation of the NYPD through an officer assigned to assist the board.[287] Consequently, the CCRB has had difficulty obtaining information from the NYPD about particularly sensitive incidents. One striking example is the CCRB inquiry into allegations of police misconduct surrounding the arrest of 247 demonstrators during the 2004 Republican National Convention. The NYPD refused to cooperate with the investigation and high-ranking officers simply ignored requests to appear before the CCRB.[288] According to one former CCRB supervisor, the board has "broadcast its irrelevance" through its "near total absence" from controversial issues such as "stop and frisk, invasive surveillance of Muslim communities, and deliberate heavy-handedness in the policing of public demonstrations."[289]

It is also rare for the CCRB to make policy recommendations. Over the past 20 years, the CCRB has issued just a handful of recommendations to the NYPD, most of which concerned the use of force and relied on expert testimony rather than an examination of police records.[290] According to a 12-year survey by the New York Civil Liberties Union, "The CCRB has failed to discover, or has ignored, patterns of police misconduct; and the NYPD has therefore failed to adopt reforms – in police training, tactics, policies and practices – that could prevent foreseeable risks of harm."[291]

Investigative and quality assurance models are the most common form of oversight found in the Brennan Center survey, utilized by 12 out of 16 police departments.[292] Unfortunately, the problems that have beset New York City's CCRB are true elsewhere as well. For example, a 2012 editorial in *The Philadelphia Inquirer* lamented that the Police Advisory Commission is "underfunded and lacks authority," and called for an independent office that would "identify trends in policing, and made recommendations for strengthening the department."[293] One bright spot is the San Francisco Office of

Citizen Complaints, which conducts annual First Amendment compliance audits of police intelligence files, but this function is more frequently associated with evaluative and performance-based oversight mechanisms, as described below.[294]

Evaluative and Performance-Based Model

This model places discipline for misconduct entirely in the hands of a department's Internal Affairs unit, and focuses instead on accountability throughout the chain of command.[295] According to Merrick Bobb, the evaluative component considers "a police department in its entirety" with the goal of publicly assessing "how well it minimizes the risk of police misconduct, identifies and corrects patterns and practices of unconstitutional and illegal behavior, and finds solutions to systemic failures."[296] The performance-based component "examines how individual officers perform, how supervisors and executives respond, and how the institution as a whole manages the risk that its employees engage in unconstitutional or illegal behavior."[297]

Three police departments in the Brennan Center survey use this approach: the Los Angeles Police Department (Office of the Inspector General); the Los Angeles Sheriff's Department (Special Counsel); and the Seattle Police Department (Office of Professional Accountability Review Board). These entities are empowered to address big picture issues and foster systemic change. Although such oversight may be rare at the state or local level, it is the norm in the federal government. All major intelligence agencies – including the FBI and CIA – operate with inspectors general.[298] As an earlier Brennan Center report explained, this system of oversight has increased transparency and the permitted independent review of controversial policies while allowing intelligence professionals to do their jobs and making their agencies more effective.[299]

The impetus to follow this model came from blue ribbon panels formed in the wake of highly publicized incidents of police misconduct that revealed the insufficiency of existing oversight mechanisms. In Los Angeles, for example, the 1991 beating of Rodney King led to the Christopher Commission, which in turn recommended the creation of an Inspector General to oversee the LAPD.[300] In Los Angeles County, four controversial police shootings prompted the LASD Board of Supervisors to hire a "special counsel" to investigate and make recommendations for reform.[301] The position was later made permanent,[302] and the county is now in the process of hiring a full-time inspector general following the recommendation of a blue ribbon commission on jail violence.[303] In Seattle, the mayor convened a panel in 1999 to evaluate mechanisms for investigating police misconduct after eight officers failed to report allegations that a veteran homicide detective stole $10,000 from a crime scene. [304] The panel recommended a "hybrid" approach that employs all three models of oversight. [305]

The common denominator among the LAPD Inspector General, the LASD Special Counsel, and Seattle's Review Board is that they have a mandate to look beyond the four corners of a complaint. They are empowered to determine whether the police's own machinery of oversight is operating effectively. Moreover, because their work is not case-dependent, they tend to assume a more flexible and policy-oriented role. According to University of Nebraska Emeritus Prof. Samuel Walker, an expert on police accountability, this approach may succeed where others fail because it is "focused on organizational

change" and because it has the authority to "probe deeply into departmental policies and procedures with an eye toward correcting them and reducing future misconduct." [306] These bodies also have the "capacity for sustained follow-up" to determine whether their recommendations have been followed.[307] The Seattle Review Board, for example, assesses departmental policies and practices and reports its recommendations to the City Council. Instead of investigating individual complaints of police misconduct,[308] it reviews audits about how the police handle complaints and community outreach, and researches national trends and best practices in police oversight and accountability.[309] Seattle also has a civilian Police Intelligence Auditor (distinct from the Office of Professional Accountability Auditor) dedicated to ensuring the department does not run afoul of its longstanding "Intelligence Ordinance," which prohibits the police from collecting information about a person's political or religious associations, activities, beliefs, or opinions without reasonable suspicion of criminal activity.[310] If the Auditor has a reasonable belief that the police have violated the Ordinance, he or she must notify the person who is the subject of the breach.[311] The Ordinance also permits the subject of a violation to sue the city for redress.[312]

The evaluative and performance-based approach may be the most conducive to monitoring a department's intelligence activities. For example, the LAPD Inspector General has published three audits since the department established the Anti-Terrorism Intelligence Section (ATIS) in 2003.[313] The audits evaluate the Section's compliance with guidelines governing intelligence investigations, including a reasonable suspicion requirement for maintaining intelligence files. In a 2012 report, the Inspector General found that ATIS was in "substantial compliance" with the guidelines, but that it did not adequately document the necessary reasonable suspicion before starting an investigation. As a result, ATIS personnel received training to ensure that intelligence reports demonstrate reasonable suspicion.[314] In 2013, the Inspector General completed an audit of the LAPD's SAR program for the first time.[315] While the audit report found the department in compliance with its own SAR policy, it unfortunately did not scrutinize the policy itself or express an opinion on the broad categories of "suspicious activities."[316] Nonetheless, the report serves a valuable transparency function and represents one of the few available data points on the operation of police SAR programs.

Such intelligence oversight is extremely uncommon at the state and local level. Only 5 of the 22 police oversight bodies examined by the Brennan Center have conducted intelligence audits: San Francisco, Los Angeles, Washington, D.C., Seattle, and Chicago.[317] Moreover, many of these inquiries have been cursory or incomplete. In Washington, D.C., for example, the District Council passed a 2004 law requiring annual audits of investigations and inquiries involving First Amendment activity. However, there has been just one audit in the past nine years. Worse still, it failed to report any information about the most sensitive issue: the use of "preliminary inquiries," which do not require reasonable suspicion of criminal activity.[318] In Seattle, the Police Intelligence Auditor conducts frequent audits, as required by local ordinance,[319] but the reports offer little detail beyond conclusory statements that all information has been appropriately collected, distributed, and/or maintained.[320] In Chicago, a 1982 consent decree mandated independent audits every five years, but the department has not established audit procedures following dissolution of the decree in 2009.[321]

In sum, the evaluative and performance-based model appears best positioned to conduct meaningful oversight of police intelligence operations, but it is important to recognize its limitations. It is susceptible

to funding cuts as well as the willingness of police departments to embrace oversight and participate in the process. Still, this model has worked relatively well for federal oversight of the FBI and CIA, which depends on reports from independent inspectors general to inform congressional supervision.[322] For cities with large police departments and significant intelligence operations, it may be the best hope for effective local oversight.

IV. FUSION CENTER OVERSIGHT

Despite modest encouragement from DHS, many fusion centers operate with minimal oversight, or no oversight whatsoever. Moreover, the oversight that does exist can hardly be described as independent. Designated privacy officers are usually fusion center employees while representatives from the participating agencies populate the governing boards. Of the 19 centers in the Brennan Center survey, only five mandate independent audits of the information they retain, and it is often unclear when or whether such audits have actually been conducted. Indeed, the ISE's 2013 Annual Report to Congress recognizes that there is no "effective ISE-wide performance measurement for internal agency compliance, oversight, and accountability mechanisms to ensure consistent application of [privacy, civil rights, and civil liberties] protections."[323]

Figure 5. Independent Oversight of Regional and State Fusion Centers [324]

Police Departments	Regional (Recognized) Fusion Center	Independent Oversight?	State (Primary) Fusion Center	Independent Oversight?
New York City	—	—	New York State Intelligence Center	No
Chicago	Crime Prevention and Information Center	No	Illinois Statewide Terrorism & Intelligence Center	No
Los Angeles County	Los Angeles Joint Regional Intelligence Center	No	California State Terrorism Threat Assessment Center	No
City of Los Angeles	Los Angeles Joint Regional Intelligence Center	No	California State Terrorism Threat Assessment Center	No
Philadelphia	Delaware Valley Intelligence Center	No	Pennsylvania Criminal Intelligence Center	No
Houston	Houston Regional Intelligence Service Center	No	Texas Fusion Center	No
Washington, D.C.	Washington Regional Threat and Analysis Center	Yes	—	—
Miami-Dade County	Southeast Florida Fusion Center	No	Florida Fusion Center	Yes
Detroit	Detroit and Southeast Michigan Information and Intelligence Center	Yes	Michigan Intelligence Operations Center	Yes
San Francisco	Northern California Regional Intelligence Center	No	California State Threat Assessment Center	No
Seattle	—	—	Washington State Fusion Center	No
City of Miami	—	—	Florida Fusion Center	Yes
Portland	—	—	Oregon Terrorism Information Threat Assessment Network	No
Minneapolis	—	—	Minnesota Joint Analysis Center	Yes
St. Paul	—	—	Minnesota Joint Analysis Center	Yes
Dearborn	—	—	Michigan Intelligence Operations Center	No

As early as 1977, experts in the government recognized that regional intelligence sharing networks focused on organized crime and drug trafficking could slip through the cracks of federalism and operate without adequate oversight. A study from the time warned that regional systems "operate across political boundaries and are therefore not subject to continued review, funding and control by a State legislature," adding that they "could operate outside the scope of normal channels of legislative control and oversight."[325] Fusion centers magnify these concerns; they not only operate outside normal channels of oversight but can also share exponentially more information than the regional networks of the 1970s. Efforts by the federal government to address this oversight gap have been half-hearted and ineffective. State and local governments have not stepped into the breach.

As a condition of continued funding, DHS has required each fusion center to craft a privacy policy and encouraged each of them to designate a "privacy officer" to ensure compliance.[326] DHS has also provided model language setting out the duties of privacy officers, which include resolving complaints and reviewing reports of alleged privacy policy violations.[327] The Chicago, Detroit, Houston, Los Angeles, Miami-Dade, and San Francisco fusion centers have all incorporated these provisions into their privacy policies. But in each instance, the privacy officer is a fusion center employee.[328]

Annual audits of intelligence files are required in nearly 90 percent of the centers surveyed.[329] But with staff or supervisors conducting the audits at 13 of the 17 fusion centers, they are hardly independent.[330] One of the few centers that uses an outside auditor (and equally important, publicly discloses its findings) is the Minnesota Joint Analysis Center.[331] The Florida Fusion Center also provides for regular independent audits by the Florida Office of the Inspector General.[332] Privacy policies require independent audits for the Michigan state fusion center as well as the Detroit and Washington, D.C., regional centers, but our research has found no public record of these audits, including when they happened, who conducted them, what they found, or whether the fusion center has taken action to correct any problems.[333]

Regular independent audits are especially important for fusion centers because the information they disseminate has such a wide audience – more than 14,000 law enforcement agencies in 49 states as well as the District of Columbia, Puerto Rico, and the Virgin Islands.[334] Sharing biased, inaccurate, or irrelevant information through the ISE magnifies the harm to civil liberties as well as national security. According to the former director of DHS's Collection and Requirements Division, the agency has been "flooded" with inappropriate reporting from state and local fusion center officials.[335]

If the tried and true framework of 28 CFR 23 were applied, the federal government would be responsible for conducting regular compliance audits to ensure that the data shared by fusion centers through the ISE meets the reasonable suspicion standard and other federal requirements.[336] But because federal agencies maintain that 28 CFR 23 is not applicable to the ISE or eGuardian, there is no federal audit process in place for fusion centers.[337] As a result, there are often significant differences in the quality of information shared by state and local law enforcement agencies on the ISE.

Without federal audits at the fusion center level, the quality of state and local intelligence information shared through the ISE will continue to depend on the inner workings of each fusion center. In order to ensure that the information collected and shared by fusion centers is both actionable and respectful of civil liberties, fusion centers should embrace the reasonable suspicion requirement and encourage independent audits of their files.

V. JOINT TERRORISM TASK FORCE OVERSIGHT

The most significant oversight problem with assigning police officers to JTTFs is that there is no mechanism geared towards ensuring compliance with state and local laws. This problem is exacerbated by the fact that rules relating to how police officers should act in the event of a conflict between their federal and state/local obligations are sometimes unknown and almost always unclear. Several municipalities and government reports have expressed concern that local officers assigned to JTTFs may be asked to engage in activities not permitted under state and local rules.

A 2005 report by the DOJ Inspector General found that the FBI did not have signed memoranda of understanding (MOUs) addressing these matters with many of the agencies participating in JTTFs.[338] While 88 percent of the police departments in the Brennan Center survey now have MOUs, the language of these documents is ambiguous and provides little concrete guidance.*

For example, the Houston MOU cites the FBI guidelines as a "controlling document" with only a caveat that any conflict with state or local law "will be jointly resolved."[339] This hedging provides Houston officers with little practical instruction as to what to do in case of conflicts. In Detroit's case, the police department signed an MOU with the JTTF but, disturbingly, it does not appear to have retained a copy.[340]

There is also an ongoing concern that the JTTF structure undermines state and local supervision of personnel and information. The FBI Special Agent in Charge of a JTTF supervises assigned police personnel.[341] These officers, deputized as United States Marshals, must obtain high-level security clearances.[342] But because JTTF operations are often classified, police commanders and city officials who commonly do not hold federal security clearances are unable to supervise and oversee the work of their own officers who are detailed to the JTTF.

The experiences of the Portland and San Francisco police departments demonstrate the problems police personnel can encounter when working on JTTFs. Oregon state law is stricter than the federal guidelines, and requires a criminal predicate before collecting information about political, religious, or social views.[343] Recognizing this discrepancy, MOUs between the Portland Police Bureau and the FBI were (uncharacteristically) clear that should a conflict between the federal and local directives arise, Portland officers must comply with Oregon law.[344] But the MOUs did not provide for any mechanism to review the work of Portland police assigned to JTTFs.[345] Moreover, officers uncertain about their authority were not

---

* The NYPD and Dearborn Police Department are the only two local law enforcement agencies surveyed that claim not to have an MOU with the JTTF. *See* Letter from Richard Mantellino, Records Access Officer, N.Y.C. Police Dep't, to Faiza Patel, Co-Director, Liberty & Nat'l Sec. Program, Brennan Ctr. for Justice (Mar. 2, 2012) (on file with the Brennan Center) ("A thorough and diligent search was conducted for Memorandums of Understanding between the NYPD and the FBI concerning the Joint Terrorist Task Force. However, no responsive records were located pursuant to our search."); Letter from Office of the Corporate Counsel, City of Dearborn Mich., to Michael Price, Counsel, Brennan Ctr. for Justice (Mar. 21, 2012) (on file with the Brennan Center) ("There is no current MOU presently in force and copies of a past MOU are not available."). *But see* Memorandum from Michael Jacobson, Assistant Gen. Counsel, Fed. Bureau of Investigation 4 (Sep. 5, 2003), *available at* http://www.scribd.com/doc/61419208/FBI-NYPD-Joint-Terrorism-Task-Force-Dysfunction ("There is a new updated MOU on D'Amuro's desk which is very different from the previous MOUs. The previous MOUs were 3 pages, and this is a booklet, with a far different tone.").

permitted to consult with the City Attorney to obtain legal advice about compliance with Oregon law.[346] The FBI refused to allow the City Attorney to apply for the necessary security clearance or to assure the mayor and police chief that they would have access to the same information as their officers serving on the JTTF.[347] Consequently, Portland withdrew from the JTTF in 2005, agreeing instead to work with the FBI on a case-by-case basis, if and when there was sufficient criminal predicate.[348]

The Portland Police Bureau rejoined the JTTF in 2010. The following year, the City Council passed a resolution clearly delineating the circumstances under which an officer could be detailed to a JTTF and providing for stronger oversight.[349] The police chief can now assign officers to a JTTF on an as-needed basis but only for investigations "of suspected terrorism that have a criminal nexus."[350] In other words, the investigation must meet the reasonable suspicion requirement. Both the police chief and the Commissioner-in-Charge are to receive security clearances and the City Attorney is supposed to have access to classified information when necessary.[351] This would leave the FBI in control of JTTF investigations but permit supervisors to understand the context of their officers' actions. Any officer asked to do something in violation of Oregon law must report the incident immediately to the police chief. [352] Finally, the police chief must provide an annual public report about Portland officers' work for JTTFs.[353]

San Francisco confronted many of the same issues following a lengthy February 2011 report by the San Francisco Human Rights Commission. The study questioned whether San Francisco's association with the JTTF compromised compliance with police policy,[354] which requires reasonable suspicion of criminal activity before monitoring First Amendment-protected activity.[355] Indeed, without informing the Police Commission or the public, the police department signed a revised MOU in 2007 that eliminated all provisions ensuring the full application of local rules to San Francisco officers participating in the JTTF.[356] The MOU did not become public until 2011. The San Francisco Board of Supervisors responded by adopting an ordinance that requires local participation in the JTTF to be consistent with state and local privacy laws as well as department policies, procedures, and orders.[357] The ordinance also mandates that any MOU with the JTTF be open to public notice and comment and that the police chief provide annual public reports on the police department's work with the JTTF.[358]

Portland and San Francisco are national leaders in a "legislative approach" to defining local law enforcement participation in JTTFs. Other agencies surveyed still rely on MOUs that are not publicly debated and might perpetuate uncertainty about the law and create barriers to effective supervision and oversight of local officers.[359] Five police departments have agreements like the 2007 San Francisco MOU that eliminate restrictions based on local laws.[360]

By passing local legislation, Portland and San Francisco provided clear, practical guidance to ensure that officers dispatched to JTTFs comply with state and local laws. These lawmakers set out procedures for annual audits and public reports. Local legislators, especially in jurisdictions with strong state privacy laws or local rules that require a criminal predicate before conducting intelligence activities, may do well to follow the examples of these two West Coast cities.

VI. CONCLUSION AND RECOMMENDATIONS

The need to adapt to new threats with speed and agility has fueled the transformation of state and local law enforcement since 9/11. But in the race to improve intelligence sharing across all levels of government, oversight and accountability have not kept pace. The entire homeland security enterprise runs on disparate and ambiguous rules about what intelligence information can or should be collected, maintained, and shared. The result has been a great deal of confusion, serious infringements on civil rights and civil liberties, and a pile of useless information.

We must recognize that giving local police broad new powers requires, at the very least, consistent rules and robust oversight. We would not set up a federal intelligence agency today without such safeguards, and it is dangerous to do so at the state and local level. Concrete steps to alleviate these concerns – at the federal, state, and local levels – are set out below.

Substantive Recommendations

When engaged in intelligence operations, law enforcement agencies should create, maintain, or share records of personal information only if there is reasonable suspicion of criminal activity and the information is relevant and material to that criminal activity.

- There must be a consistent, transparent standard for state and local intelligence activities. The Brennan Center believes that the reasonable suspicion standard is both consistent with our nation's core constitutional values and flexible enough to allow law enforcement to identify and investigate potential threats. State and local governments should require their police forces to adopt the reasonable suspicion standard for creating, maintaining, or sharing any intelligence records containing personal information. When the information contained in a record concerns First Amendment-protected activities, it must also directly relate to the suspected criminal activity.

- State and local governments should expressly prohibit the collection, maintenance, or dissemination of information that relies on race, ethnicity, national origin, or religious affiliation as a factor in establishing reasonable suspicion (except as part of a specific suspect description).

Fusion centers should not disseminate information that does not meet the reasonable suspicion requirement on any federally funded intelligence network.

- The Program Manager for the ISE should amend the Functional Standard to require reasonable suspicion of criminal activity, consistent with 28 CFR 23.

- The FBI should amend its eGuardian guidelines to require reasonable suspicion of criminal activity, consistent with 28 CFR 23.

- The DOJ should revise its guidance to clarify that sharing "temporary files," "tips and leads" information, or SARs without reasonable suspicion of criminal activity is not permissible under 28 CFR 23.

Oversight Recommendations

Strengthen oversight of state and local intelligence activities with independent police monitors tasked with reviewing intelligence files and local supervision of officers working with federal agencies.

- Although the extent of oversight needed will depend on the size of the police department and the scope of its activities, the inspector general model has worked well for federal intelligence agencies and is most likely to produce the best oversight of state and local intelligence activities. Complaint-driven models – such as civilian complaint boards – are likely to prove ineffective due to the secretive nature of intelligence work.

- If a police department participates in a JTTF, the state or local legislature should require a publicly available, written MOU that preserves local supervision and includes clear rules for resolving any legal conflicts.

Require regular independent audits for fusion centers to ensure compliance with applicable laws and policies.

- As a condition of continued grant funding, DHS should require all fusion centers to fully implement their privacy policies and demonstrate compliance through regular independent audits available to the public.

- State and local governments that have created fusion centers should empower an independent auditor to review the center's files for compliance and publish a report of the findings.

The United States has a long and sordid history of spying on people with unpopular beliefs – a tragically predictable cycle of fear, excess, reprimand, and relapse that has threatened our liberty and our security time and again. We can do better. We must praise the good, but we must learn from our mistakes. We must strive to make the state and local role in national security more effective, rational, efficient, and fair. We must get smart on surveillance.

ENDNOTES

1 Josiah Stamp, Some Economic Factors in Modern Life 258-59 (1929).

2 The White House, National Strategy for Counterterrorism 11 (2011), *available at* http://www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf; *see also* Michael P. Downing, Commanding Officer, Counter-Terrorism/Criminal Intelligence Bureau, L.A. Police Dep't, Remarks at the Washington Institute: Counterterrorism and Crime Fighting in Los Angeles 6 (Oct. 22, 2009), *available at* http://www.washingtoninstitute.org/html/pdf/LAPD-Stein.pdf.

3 U.S. Gov't Accountability Office, GAO-13-233, Information Sharing: Additional Actions Could Help Ensure That Efforts to Share Terrorism-Related Suspicious Activity Reports Are Effective 32 (2013) [hereinafter "GAO-13-233"], *available at* http://www.gao.gov/assets/660/652995.pdf.

4 *See Law Enforcement and the Intelligence Community: Hearing Before the Nat'l Comm'n on Terrorist Attacks Upon the U.S.* (2004) (statement of John Brennan, Director, Terrorist Threat Integration Center), *available at* https://www.cia.gov/news-information/speeches-testimony/2004/brennan_testimony_04142004.html.

5 Sir Robert Peel famously proclaimed that the basic mission for which police exist is to "prevent crime and disorder as an alternative to the repression of crime and disorder by military force and severity of legal punishment." *See* Charles Reith, A Short History of the British Police 64 (1948).

6 *See generally* Paul G. Chevigny, *Politics and Law in the Control of Local Surveillance*, 69 Cornell L. Rev. 735, 768-775 (1984). For a detailed discussion of the history and substance of intelligence rules governing the police departments in this survey, see *infra*, notes 105-122, 128.

7 The FBI also loosened its investigative rules through repeated modifications to the Attorney General Guidelines. *Compare* Richard Thornburgh, U.S. Dep't of Justice, the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations § III (1989), *available at* http://www.justice.gov/ag/readingroom/generalcrimea.htm, *with* John Ashcroft, U.S. Dept' of Justice, The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations § III.A.2.a (2002), *available at* http://www.fas.org/irp/agency/doj/fbi/generalcrimes2.pdf. For concerns raised by these new powers, see Emily Berman, Brennan Ctr. for Justice, Domestic Intelligence: New Powers, New Risks 26-37 (2011), *available at* http://www.brennancenter.org/publication/domestic-intelligence-new-powers-new-risks.

8 Permanent Subcomm. On Investigations of the S. Comm. On Homeland Sec. and Governmental Affairs, 112th Cong., Federal Support for and Involvement in State and Local Fusion Centers 2 (2012) [hereinafter 2012 Senate HSGAC Fusion Center Report], *available at* http://www.hsgac.senate.gov/download/?id=49139e81-1dd7-4788-a3bb-d6e7d97dde04.

9 *Id.*; GAO-13-233, *supra* note 3, at 33-38.

10 *See, e.g.*, Matt Apuzzo and Adam Goldman, Enemies Within 89 (2013) (Chronicling how "[a]fter years of raking, the NYPD knew where New York's Muslims were … [but] [t]hey still didn't know where the terrorists were. And they didn't know a thing about [Najibuallah] Zazi," an al-Qaeda-trained U.S. citizen convicted of plotting to bomb the New York subway system. The NYPD had files on the restaurants in Zazi's neighborhood, on his mosque, and on the travel agency where he bought his plane tickets to Pakistan - none of which offered any early warning of the plot or proved useful in locating Zazi.).

11 Michael B. Ward, the special agent in charge of the FBI's Newark office, explained: "People are concerned that they are being followed, … that they can't trust law enforcement, and it's having a negative impact." Al Baker, *F.B.I. Official Faults Police Tactics on Muslims*, N.Y. Times, Mar. 7, 2012, *available at* http://www.nytimes.com/2012/03/08/nyregion/chief-of-fbi-newark-bureau-decries-police-monitoring-of-muslims.html; Jason Grant, *Recent NYPD Spying Uproar Shakes FBI's Foundations in N.J. Terror Intelligence*, N.J. Star-Ledger, Mar. 7, 2012, *available at* http://www.nj.com/news/index.ssf/2012/03/recent_nypd_spying_uproar_shak.html.

12 *Joint Terrorism Task Force*, U.S. Dep't of Justice, http://www.justice.gov/jttf/ (last visited Feb. 28, 2012).

13 *State and Major Urban Area Fusion Centers*, U.S. Dep't of Homeland Security, http://www.dhs.gov/state-and-major-urban-area-fusion-centers (last visited July 12, 2013).

14 *See, e.g.*, Constitution Project, Recommendations for Fusion Centers: Preserving Privacy & Civil Liberties while Protecting Against Crime & Terrorism (2012) [hereinafter Recommendations for Fusion Centers], *available at* http://www.constitutionproject.org/pdf/fusioncenterreport.pdf; Milton Nenneman, An Examination of State and Local Fusion Centers and Data Collection Methods 78-86 (Mar. 2008) (unpublished thesis, Naval Postgraduate School), *available at* https://www.fas.org/irp/eprint/fusion.pdf; David Thacher, *The Local Role in Homeland Security*, 39 Law & Soc'y Rev. 635 (2005); John G. Comiskey, Effective State, Local, and Tribal Police Intelligence: The New York City Police Department's Intelligence Enterprise – A Smart Practice 13-19 (Mar. 2010) (unpublished thesis, Naval Postgraduate School), *available at* http://edocs.nps.edu/npspubs/scholarly/theses/2010/Mar/10Mar_Comiskey.pdf.

15 *Crime in the United States: Full-time Civilian law Enforcement Employees by Population Group*, *Percent of Total, 2011*, Fed. Bureau of Investigation, http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2011/crime-in-the-u.s.-2011/tables/table_75_full-time_civilian_law_enforcement_employees_by_population_group_percent_of_total_2011.xls (last visited Mar. 1, 2013).

16 GAO-13-233, *supra* note 3, at 10.

17 Info. Sharing Env't, Annual Report to the Congress 7 (2013) [hereinafter ISE Annual Report], *available at* www.ise.gov/sites/default/files/2013_ISE_Annual_Report_Final.pdf.

18 Press Release, Fed. Bureau of Investigation, 2011 Request for Information on Tamerlan Tsarnaev from Foreign Government (Apr. 19, 2013), *available at* http://www.fbi.gov/news/pressrel/press-releases/2011-request-for-information-on-tamerlan-tsarnaev-from-foreign-government.

19 *See* Michael Rezendes, *Bombing Case Casts Shadow Over Waltham Triple Murder*, Boston Globe (Jun. 8, 2013), *available at* http://www.bostonglobe.com/metro/2013/06/07/waltham-triple-homicide-raises-troubling-question-about-marathon-bombing/mJ2MwjWEZNZqYPRDixQX4I/story.html; Margaret Hartmann, *Police Let Tsarnaev Get Away With 2011 Murder, or Had No Evidence*, N.Y. Magazine (Jul. 11, 2013), *available at* http://nymag.com/daily/intelligencer/2013/07/did-officials-fail-to-nab-tsarnaev-for-murder.html; Michael Daly, *How Local Police Missed a Chance to Stop Tamerlan Tsarnaev in 2011*, Daily Beast (Jul. 12, 2013), *available at* http://www.thedailybeast.com/articles/2013/07/12/how-local-police-missed-a-chance-to-stop-tamerlan-tsarnaev-in-2011.html.

20 *See* Paul Lewis, *Boston Police Urge FBI to Share Intelligence as Tsarnaev Is in Court*, Guardian, Jul. 10, 2013, *available at* http://www.theguardian.com/world/2013/jul/10/boston-police-fbi-tsarnaev-court.

21 *See* Michael Isikoff, *Unaware of Tsarnaev Warnings, Boston Counterterror Unit Tracked Protesters*, NBC News (May 10, 2013), *available at* http://investigations.nbcnews.com/_news/2013/05/10/18152849-unaware-of-tsarnaev-warnings-boston-counterterror-unit-tracked-protesters.

22 *See* Lois M. Davis et al., Rand Corp., Long-Term Effects of Law Enforcement's Post-9/11 Focus on Counterterrorism and Homeland Security 107-11 (2010) [hereinafter 2010 RAND Report], *available at* http://www.rand.org/content/dam/rand/pubs/monographs/2010/RAND_MG1031.pdf.

23 2012 Senate HSGAC Fusion Center Report, *supra* note 8, at 3 ("The Subcommittee investigation also found that DHS failed to adequately police how states and municipalities used the money intended for fusion centers. The investigation found that DHS did not know with any accuracy how much grant money it has spent on specific fusion centers, nor could it say how most of those grant funds were spent, nor has it examined the effectiveness of those grant dollars.").

24 GAO-13-233, *supra* note 3, at 35.

25 *See e.g.*, Recommendations for Fusion Centers, *supra* note 14, at 9-11; Am. Civil Liberties Union, Spying on First Amendment Activity – State-by-State (2011), *available at* http://www.aclu.org/files/assets/policingfreespeech_20111103.pdf; Adam Goldman & Matt Apuzzo, *With CIA Help, NYPD Moves Covertly in Muslim Areas*, Associated Press (Aug. 23, 2011), *available at* http://ap.org/Content/AP-In-The-News/2011/With-CIA-help-NYPD-moves-covertly-in-Muslim-areas.

26 2012 Senate HSGAC Fusion Center Report, *supra* note 8, at 2.

27 Matthew C. Waxman, *Police and National Security: American Local Law Enforcement and Counterterrorism After 9/11*, 3 J. Nat'l Security L. & Pol'y 377, 380-81 (2009).

28 Nat'l Comm'n on Terrorist Attacks Upon the U.S., 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States 427 (2004) [hereinafter 9/11 Report], *available at* http://www.9-11commission.gov/report/911Report.pdf.

29 Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (establishing the Department of Homeland Security). Congress tasked DHS with commissioning an independent study on the feasibility of creating a domestic intelligence agency. The RAND Corporation conducted the study and published its findings in 2009, assessing the merits of various configurations, but Congress ultimately took no action. *See* RAND Corp., Considering the Creation of a Domestic Intelligence Agency in the United States: Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom (Brian A. Jackson, ed. 2009), *available at* http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG805.pdf; *see also* 9/11 Report, *supra* note 28, at 423-424.

30 *See* U.S. Census Bureau, Statistical Abstract of the United States: 2012, Federal Civilian Employment by Branch and Agency: 1990 to 2010 (2012), *available at* http://www.census.gov/compendia/statab/2012/tables/12s0499.pdf.

31 Robert Mueller, Dir., Fed. Bureau of Investigation, Address at Stanford Law School: Terrorism in a Post-9/11 World (Oct. 19, 2002), *available at* http://www.fbi.gov/news/speeches/terrorism-in-a-post-9-11-world ("Of course, we will continue to investigate criminal cases and are proud of our work in such areas as violent crime, organized crime, financial fraud, civil rights, and public corruption. But in the wake of September 11th, our first and abiding priority, plain and simple, is counterterrorism. That priority is to stop another attack like we saw on September 11th. To do that, we have to enter into an age of preventive investigation. At the heart of our attack on counterterrorism is this massive redeployment of Agents from other programs."). *See also* Fed. Bureau of Investigation, U.S. Dep't of Justice, Report to National Commission on Terrorist Attacks Upon the United States: The FBI's Counterterrorism Program Since September 2001 12 (2004), *available at* http://www.fbi.gov/stats-services/publications/fbi_ct_911com_0404.pdf.

32 Berman, *supra* note 7, at 17.

33 Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1021(3)(d), 118 Stat. 3638, 3673.

34 *Id.*

35 Office of Justice Programs, U.S. Dep't of Justice, The National Criminal Intelligence Sharing Plan 43-46 (2003) [hereinafter NCISP 2003], *available at* http://www.fas.org/irp/agency/doj/ncisp.pdf ("Recommendation 22: Interoperability with existing systems at the local, state, tribal, regional, and federal levels with the RISS/LEO communications capability should proceed immediately, in order to leverage information sharing systems and expand intelligence sharing."); Deborah J. Daniels, *From the Assistant Attorney General: Increasing Information Sharing to Help Reduce Crime and Respond to Emergencies*, 71 The Police Chief, no. 10, Oct., 2004, *available at* http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1402&issue_id=102004.

36 David L. Carter, Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies 344 (Office of Cmty. Oriented Policing Servs., U.S. Dep't of Justice, 2nd ed. 2009), *available at* www.it.ojp.gov/docdownloader.aspx?ddid=1133.

37 Christopher Dickey, Securing the City: Inside America's best Counterterror Force—The NYPD 99-216 (Simon & Schuster 2009) [hereinafter Securing the City]; Leonard Levitt, NYPD Confidential: Power and Corruption in the Country's Greatest Police Force 232-83 (Thomas Dunne Books 2009); *Preliminary Budget Hearing for Fiscal Year 2013 and the Fiscal Year 2012 Mayor's Management Report: Hearing Before the N.Y.C. Council Pub. Safety Comm.* 21-25 (2012) (testimony of Raymond Kelly, Chief, New York City Police Department), *available at* http://legistar.council.nyc.gov/View.ashx?M=F&ID=1828553&GUID=FD7A13D2-9BF4-4898-8309-8BADF961BB38; George L. Kelling & William J. Bratton, *Policing Terrorism*, Civic Bulletin, Sept. 2006, at 5-6, *available at* http://www.manhattan-institute.org/pdf/cb_43.pdf.

38 Carter, *supra* note 36, at 80.

39 Marilyn Peterson, Int'l Ass'n of Chiefs of Police, Intelligence-Led Policing: The New Intelligence Architecture 3-4 (2005), *available at* https://www.ncjrs.gov/pdffiles1/bja/210681.pdf.

40 The NYPD, for example, asserts that it has thwarted or helped thwart at least 14 terrorist plots against New York City. But a widely-cited investigation by ProPublica found that the figure "overstates both the number of serious, developed terrorist plots against New York and exaggerates the NYPD's role in stopping attacks." Justin

Elliott, *Fact-Check: How the NYPD Overstated Its Counterterrorism Record*, ProPublica (July 10, 2012, 9:33 AM), http://www.propublica.org/article/fact-check-how-the-nypd-overstated-its-counterterrorism-record. *See also All Things Considered: Counterterrorism and the NYPD*, Nat'l Pub. Radio (Jul. 15, 2012), *available at* http://www.npr.org/2012/07/15/156815759/counterterrorism-and-the-nypd; Leonard Levitt, *Lone Wolves or Sheep?*, NYPD Confidential (Mar. 19, 2012), http://nypdconfidential.com/columns/2012/120319.html; Ctr. for Human Rights and Global Justice, Targeted and Entrapped: Manufacturing the "Homegrown Threat" in the United States 38 (2011), *available at* http://chrgj.org/wp-content/uploads/2012/07/targetedandentrapped.pdf. The Senate Homeland Security Committee and the Government Accountability Office have also raised serious concerns about the quality of intelligence generated by fusion centers and Suspicious Activity Reporting programs. *See* 2012 Senate HSGAC Fusion Center Report, *supra* note 8, at 2; GAO-13-233, *supra* note 3, at 33-38.

41 Declaration of Deputy Commissioner David Cohen at ¶ 52, Handschu v. Special Servs. Div., 273 F. Supp. 2d 327 (S.D.N.Y. 2003) (No. 71 Civ. 2203).

42 *See generally* Faiza Patel, Brennan Ctr. For Justice, Rethinking Radicalization (2011), *available at* http://www.brennancenter.org/publication/rethinking-radicalization.

43 Colin Moynihan, *Wall Street Protesters Complain of Police Surveillance*, N.Y. Times, Mar. 11, 2012, *available at* http://www.nytimes.com/2012/03/12/nyregion/occupy-wall-street-protesters-complain-of-police-monitoring.html.

44 Kevin Strom, et al., Inst. for Homeland Sec. Solutions, Building on Clues: Examining Successes and Failures in Detecting U.S. Terrorist Plots, 1999-2009 12 (2010), *available at* http://sites.duke.edu/ihss/files/2011/12/Building_on_Clues_Strom.pdf. Only federal law enforcement sources (30 percent) rival the importance of public tips (29 percent) in foiling terrorist plots. *Id.* Moreover, the vast majority of initial clues – 78 percent – did *not* come from local law enforcement. *Id.*

45 Statement of Interest of the United States at 10, Floyd v. City of New York, 2013 WL 4046209 (S.D.N.Y. 2013) (No. 08 Civ. 1034).

46 Stephen J. Schulhofer, Tom R. Tyler & Aziz Z. Huq, *American Policing at a Crossroads: Unsustainable Policies and the Procedural Justice Alternative*, 101 J. of Crim. L. & Criminology 335, 369 (2011); *see also* Muslim Am. Civil Liberties Coal. et al., Mapping Muslims: NYPD Spying and its Impact on American Muslims 32-28 (2013) [hereinafter Mapping Muslims], *available at* http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf.

47 *See, e.g.,* Final Report of the William H. Webster Commission on the Federal Bureau of Investigation, Counterterrorism Intelligence, and the Events at Ft. Hood, Texas, on November 5, 2009, 88 (2012) (finding that the "exponential growth in the amount of electronically stored information" posed a critical challenge to the FBI in its assessment of Nidal Hasan, creating "relentless" demands on a limited number of personnel), *available at* http://www.fbi.gov/news/pressrel/press-releases/final-report-of-the-william-h.-webster-commission.

48 Frank J. Cilluffo et al., The Geo. Wash. Univ. Homeland Sec. Policy Inst., Counterterrorism Intelligence: Fusion Center Perspectives 31 (2012), *available at* http://www.gwumc.edu/hspi/policy/HSPI%20Counterterrorism%20Intelligence%20-%20Fusion%20Center%20Perspectives%206-26-12.pdf [hereinafter 2012 HSPI Report].

49 *See generally* Peterson, *supra* note 40.

50 *See, e.g.*, NCISP 2003, *supra* note 35, at viv ("the primary purpose of intelligence-led policing is to provide public safety decision makers the information they need to protect the lives of our citizens."); Jerry H. Ratcliffe, *Intelligence-Led Policing*, *in* Environmental Criminology and Crime Analysis 263, 268 (Richard Wortley & Lorraine Mazerolle eds., 2008) ("Intelligence-led policing is a business model and managerial philosophy where data analysis and crime intelligence are pivotal to an objective, decision-making framework that facilitates crime and problem reduction, disruption and prevention through both strategic management and effective enforcement strategies that target prolific and serious offenders."); Global Justice Info. Sharing Initiative, U.S. Dep't of Justice, Navigating Your Agency's Path to Intelligence-Led Policing 3 (2009), *available at* http://www.it.ojp.gov/docdownloader.aspx?ddid=1082 ("Intelligence-led policing (ILP) is a business process for systematically collecting, organizing, analyzing, and utilizing intelligence to guide law enforcement operational and tactical decisions.").

51 2010 RAND Report, *supra* note 22, at 4.

52 The Brennan Center characterized the police departments in this report based in large part on self-identifying statements in annual reports and internal strategy documents. A handful of departments do not describe their overall approach as "intelligence-led" but explicitly use elements of the philosophy in officer training or specific programs. The Los Angeles and Minneapolis Police Departments ascribe to "predictive policing," which is a variant of intelligence-led policing.

53 Securing the City, *supra* note 37, at 171-72.

54 *Hearing Before the Nat'l Comm'n on Terrorist Attacks Upon the U.S.* 2-3 (2004) (testimony of Raymond Kelly, Chief, New York Police Department) [hereinafter *Kelly May 18, 2004 Testimony*], *available at* http://www.globalsecurity.org/security/library/congress/9-11_commission/040518-kelly.pdf; *see also* Charlie Savage, *C.I.A. Report Finds Concerns With Ties to New York Police*, N.Y. Times, Jun. 26, 2013, *available at* http://www.nytimes.com/2013/06/27/nyregion/cia-sees-concerns-on-ties-to-new-york-police.html.

55 *International Liaison Program*, New York City Police Found., https://www.nycpolicefoundation.org/netcommunity//Page.aspx?pid=639 (last visited April 21, 2013).

56 *See generally Highlights of AP's Pulitzer Prize-Winning Probe Into NYPD Intelligence Operations*, Associated Press, http://www.ap.org/media-center/nypd/investigation (last visited Feb. 28, 2012); *AP's Probe Into NYPD Intelligence Operations*, Associated Press, http://www.ap.org/Index/AP-In-The-News/NYPD#tpHdr (last visited Feb. 28, 2012).

57 N.Y. Police Dep't, Intelligence Division 18-26 (n.d.) [hereinafter NYPD demographics Unit Document], *available at* http://enemieswithinbook.com/documents/Analytical%20Units%20PowerPoint.pdf.

58 Confidential informants and undercover officers were sent to monitor so-called "hot spots" by eavesdropping and noting "extremist" literature or rhetoric. *Id.* at 2. The NYPD formed teams to collect this information, using one detective "handler" to supervise undercover officers called "rakers." *Id.* at 7. The "rakers" would visit communities "consistent with their ethnicity and or language" and report information on a daily basis. *Id.*; *see also* Apuzzo & Goldman, *supra* note 25. At businesses, officers were instructed to "determine the ethnicity of the owner," "gauge sentiment" by "interacting, observing and conversing with owners and patrons," "[p]urchase extremist literature or paraphernalia" and determine if the business is "facilitating criminal acts which may be enablers of terrorism" such as untaxed cigarettes, narcotics, or sales of fraudulent identity documents. NYPD demographics Unit Document, at 23. The Intelligence Division also deploys informants known as "mosque crawlers" to monitor sermons and conversations among congregants. Apuzzo & Goldman, *supra* note 25. It has created an intelligence file for every mosque within 100 miles of New York City, *id.*, and prepared analytical reports on the reaction to news events such as a Danish newspaper's publication of 12 cartoons depicting the Prophet Mohammed or the shooting death of Sean Bell, an African American man who died in a hail of police bullets outside a Queens nightclub. N.Y. Police Dep't, NYPD Intelligence Note: NYC Mosque Statements on Danish Cartoon Controversy (2006), *available at* http://hosted.ap.org/specials/interactives/documents/nypd/nypd_cartoons.pdf; Intelligence Division, N.Y. Police Dep't, Deputy Commissioner's Briefing (2008) [hereinafter April 25, 2008 Briefing], *available at* http://hosted.ap.org/specials/interactives/documents/nypd/dci-briefing-04252008.pdf.

59 N.Y. Police Dep't, Weekly MSA Report 3 (2006), *available at* http://hosted.ap.org/specials/interactives/documents/nypd-msa-report.pdf. In one highly publicized incident, the NYPD infiltrated a student whitewater-rafting trip using an informant who reported on how often the students prayed and the religious content of their conversations. April 25, 2008 Briefing, *supra* note 58, at 3-4.

60 *See* Declaration of Paul Chevigny at ¶ 4, Handschu v. Special Servs. Div., No. 71 Civ. 2203 (S.D.N.Y. Feb. 4, 2013) (on file with the Brennan Center); First Amended Complaint at 21-22, Hassan v. New York, No. 12-03401 (D.N.J. Oct. 3, 2012), *available at* http://www.ccrjustice.org/files/10_First%20Amended%20Complaint.10.3.2012.pdf; Complaint at 1, Raza v. New York, No. 13 Civ. 03448 (E.D.N.Y., Jun. 18, 2013), *available at* http://www.aclu.org/files/assets/nypd_surveillance_complaint_-_final_06182013_0.pdf.

61 *See* David A. Harris, *Law Enforcement and Intelligence Gathering in Muslim and Immigrant Communities After 9/11*, 34 N.Y.U. Rev. L. & Soc. Change 123, 161-168 (2010); David H. Bayley & David Weisburd, *Cops and Spooks: The Role of the Police in Counterterrorism*, *in* To Protect and To Serve: Policing in an Age of Terrorism 94-95 (David Weisburd et al. eds., 2009), *available at* http://www.scribd.com/doc/97752927/Policing-in-Age-of-Terrorism ("The problem is that a single episode of thoughtlessness or overreaching may undermine public trust. Perception is everything. The loss of public confidence is especially costly for the success of counterterrorism itself if it increases the alienation of minority and immigrant communities.").

62 Letter from Imam al-Hajj Talib 'Abdur-Rashid, Imam, The Mosque of Islamic Brotherhood, et al., to Michael Bloomberg, Mayor of the City of New York (Dec. 29, 2011), *available at* http://interfaithletter.wordpress.com/; *Some Local Muslims Boycott NYPD's Annual Pre-Ramadan Conference*, NY1 (Jul. 11, 2012), http://manhattan.ny1.com/content/top_stories/164630/some-local-muslims-boycott-nypd-s-annual-pre-ramadan-conference; *Muslims to Boycott NY Mayor's Interfaith Breakfast*, MSNBC.com (Dec. 29, 2011, 5:29 PM), http://www.msnbc.msn.com/id/45814786/ns/us_news-life/t/muslims-boycott-ny-mayors-interfaith-breakfast/; Mapping Muslims, *supra* note 46, at 37.

63 Chris Hawley, *Muslim Groups Hold Rally After NYPD Intel Report*, WABC-TV N.Y.C. (Feb. 3, 2012), http://abclocal.go.com/wabc/story?section=news/local/new_york&id=8530224; Samantha Gross & Tom Hays, *Muslims Call for NYPD Chief to Resign Over Movie*, Wall St. J., Jan. 26, 2012, *available at* http://online.wsj.com/article/APbe6d40631fdb4cc89bc868e32ba0aace.html; *New York Muslims to rally against NYPD*, Press TV (Feb. 1, 2012), http://presstv.com/detail/224295.html; Christie Thompson, *Momentum Builds in the Fight Against Stop-and-Frisk*, The Nation, Oct. 31, 2012, *available at* http://www.thenation.com/article/170944/momentum-builds-fight-against-stop-and-frisk.

64 Richard Winton & Teresa Watanabe, *LAPD's Muslim mapping plan killed*, L.A. Times, Nov. 15, 2007, *available at* http://articles.latimes.com/2007/nov/15/local/me-muslim15; *The Role of Local Law Enforcement in Countering Violent Islamic Extremism: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 110th Cong. 7 (2007) (statement of Michael P. Downing, Commanding Officer, Counter-Terrorism/Criminal Intelligence Bureau, Los Angeles Police Department), *available at* http://www.lapdonline.org/assets/pdf/Michael%20DowningTestimonyfortheU.S.Senate-Final.PDF; Letter from Ranjana Natarajan, Staff Attorney, Am. Civil Liberties Union of S. Cal., to Michael P. Downing, Commanding Officer, Counter-Terrorism/Criminal Intelligence Bureau, L.A. Police Dep't (Nov. 8, 2007) (on file with the Brennan Center) ("In addition to constitutional concerns that such a practice would violate equal protection and burden the free exercise of religion, religious profiling engenders fear and distrust in the community that hampers law enforcement efforts. A mapping project that aims only to gather intelligence and identify 'risk factors' unfairly targets members of the Muslim community based on their religion and ethnicity, and also increases the inaccurate perception among the larger community that Muslims are doing something suspicious that merits investigation.").

65 Hugh Dellios, *Garry McCarthy, Chicago Police Chief, Pledges No NYPD-esque Spying on Muslims*, Huffington Post (Mar. 4, 2012, 4:04 PM), http://www.huffingtonpost.com/2012/03/04/chicago-police-chief-pled_0_n_1319515.html.

66 Chi. Police Dep't, General Order G02-04: Prohibition Regarding Racial Profiling and Other Bias-Based Policing I(B) (2012), *available at* http://directives.chicagopolice.org/directives/data/a7a57be2-1287e496-14312-87ee-0dae86849cf9f737.html.

67 Emergency Operations Bureau, L.A. Cnty. Sheriff's Dep't, Unit Order No. 5: Intelligence Guidelines 2 (n.d.) (on file with the Brennan Center).

68 *The Extent of Radicalization in the American Muslim Community and the Community's Response: Hearing Before the H. Comm. On Homeland Sec.*, 112th Cong. 2 (2011) [hereinafter Baca Testimony 2011] (statement of Leroy Baca, Sheriff, L.A. Sheriff's Dep't), *available at* http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Baca_0.pdf.

69 *Id.*

70 The Brennan Center conducted interviews with over a dozen Arab and South Asian community leaders and advocates in Los Angeles for this report. Two of them were willing to go on the record. Personal Interview with Personal Interview with Zoheb Munshi, Founding Member, Young Muslim American Leaders Advisory Council (Sept. 20, 2013); Personal Interview with Ameena Qazi, Deputy Executive Director and Staff Attorney, Council on American Islamic Relations (CAIR) of Los Angeles, Feb. 22, 2013. In the wake of the July 7, 2005 London bombings, the LASD partnered with members of the Muslim American community to establish a "Muslim American Homeland Security Congress" (MAHSC) that includes the Council on American Islamic Relations (CAIR), the Islamic Shura Council of Southern California, the Muslim Public Affairs Council, and the Muslim American Society. *Muslim American Homeland Security Congress (MAHSC)*, Facebook, http://www.facebook.com/pages/Muslim-American-Homeland-Security-Congress-MAHSC/199844210096880?id=199844210096880&sk=info (last visited Mar. 4, 2013); The group facilitates dialogue and partnership between law enforcement and the Muslim community through town hall meetings, trainings, seminars and presentations. Hussam Ayloush, the

executive director of CAIR-Los Angeles, called the relationship "an example for the rest of the nation to emulate." CAIR-LA, *Calif. Muslims Hold Law Enforcement Training Conference*, Facebook, http://www.facebook.com/notes/cair/cair-la-calif-muslims-hold-law-enforcement-training-conference/10150936570909442 (last visited Mar. 4, 2013). *See also* Laurie Goodstein, *Police in Los Angeles Step Up Efforts to Gain Muslims' Trust*, N.Y. Times, Mar. 9, 2011, *available at* http://www.nytimes.com/2011/03/10/us/10muslims.html.

71 Dave Zirin, *Not a Game: How the NYPD Uses Sports for Surveillance*, The Nation, Sept. 10, 2013, *available at* http://www.thenation.com/blog/176082/not-game-how-nypd-uses-sports-surveillance#; *see also* N.Y. Police Dep't, Sports Venue Report 2 (n.d.), *available at* http://s3.documentcloud.org/documents/779743/demographics-sports-venues.pdf.

72 Personal Interview with Debbie Almontaser, President, Muslim Consultative Network (Mar. 29, 2013). Furthermore, according to a former member of the NYPD's Muslim Advisory Council, established in 2012, the NYPD's willingness to receive and engage feedback from Muslim leaders has been lackluster at best. Personal Correspondence with Asim Rehman, President, Muslim Bar Association of New York (Jun. 27, 2013). Following revelations that the NYPD is using "terrorism enterprise investigations" to put entire mosques and Muslim non-profit organizations under intensive surveillance, Dr. Ahmad Jaber, another member of the NYPD's Advisory Council, resigned in protest. Documents indicated that the NYPD had attempted to place an informant on the board of the Arab American Association of New York, a Brooklyn-based social services organization; Dr. Jaber is the organization's president. Mary Murphy, *Muslim Doctor Resigns from NYPD Advisory Board after Alleged Secret Investigations*, PIX 11, Aug. 29, 2013, *available at* http://pix11.com/2013/08/29/muslim-doctor-resigns-from-nypd-advisory-board-as-backlash-grows/; Kerry Burke and Tina Moore, 'New NYPD Low': Muslims Outraged by 'Terror Enterprise' Mosque Probes, N.Y. Daily News, Aug. 28, 2013, *available at* http://www.nydailynews.com/new-york/new-nypd-muslims-outraged-terror-enterprise-mosque-probes-article-1.1439951.

73 *See* Patrick A. Burke, Collecting and Connecting the Dots: Leveraging Technology to Enhance the Collection of Information and the Dissemination of Intelligence 29-30 (Sept. 2009) (unpublished thesis, Naval Postgraduate School), *available at* https://www.hsdl.org/?view&did=33358. To the extent that a shift towards intelligence-led policing also entails the redistribution of personnel and resources, it may disrupt more traditional police functions. According to a 2010 study by the RAND Corporation, a 1% reduction in sworn personnel devoted to routine crime fighting would result in at least $4.7 million in crime costs and an additional two homicides per year. 2010 RAND Report, *supra* note 22, at 99. While this cost might be reasonable compared to the cost of another successful terrorist attack, it is not at all clear that "community mapping" or eavesdropping at cafes are effective means of preventing a terrorist incident. Indeed, NYPD Assistant Chief Thomas Galati testified in 2012 that the Demographics Unit has produced no actionable intelligence in at least the past six years, and perhaps longer. Transcript of Examination Before Trial at 124, Handschu v. Special Servs. Div., 273 F.Supp.2d 327 (S.D.N.Y. June 28, 2012) (No. 71 Civ. 2203) (testimony of Thomas Galati, Assistant Chief, NYPD), *available at* http://www.nyclu.org/files/releases/Galati_EBT_6.28.12.pdf.

74 Officers tasked with guarding transportation infrastructure, such as ports or airport terminals, may well have counterterrorism responsibilities even if they are not described as counterterrorism personnel. In Seattle, for example, one assistant chief is responsible for overseeing "the day to day operations of the Traffic Section, Parking Enforcement, Homeland Security, the Intelligence Section and the Metropolitan Section (SWAT, Canine, Mounted, Crisis Intervention, and Harbor Patrol)." *Seattle Police Chief Diaz Reorganizes Command Structure*, W. Seattle Herald, Sept. 15, 2010, http://www.westseattleherald.com/2010/09/15/news/seattle-police-chief-diaz-reorganizes-command-str.

75 *See* Greg Krikorian, *Terrorism Early Warning Group Works to Keep L.A.'s Guard Up*, L.A. Times, Nov. 7, 2004, *available at* http://articles.latimes.com/2004/nov/07/local/me-terror7. The LAPD had an "Anti-Terrorist Division" pre-9/11, "formed prior to 1984 Summer Olympics in the aftermath of the 1983 dismantling of the department's scandal-ridden Public Disorder Intelligence Division." William Overend, *Schlei Bids a Tearful Farewell to LAPD*, L.A. Times, Sept. 21, 1988, *available at* http://articles.latimes.com/1988-09-21/local/me-2305_1_tearful-farewell; *see generally* L.A. Terrorism Early Warning Grp., Terrorism Early Warning: 10 Years of Achievement in Fighting Terrorism and Crime (John P. Sullivan & Alain Bauer eds., 2008), *available at* http://file.lacounty.gov/lasd/cms1_144939.pdf.

76 This is consistent with the national trend, identified by the DOJ in a 2007 report, which determined that more than 90% of local police departments serving a population of 500,000 or more have such personnel. Brian A.

Reaves, Bureau of Justice Statistics, U.S. Dep't of Justice, Local Police Departments, 2007, at 32 (2010), *available at* http://www.bjs.gov/content/pub/pdf/lpd07.pdf. It is also consistent with recommendations from the International Association of Chiefs of Police and the National Criminal Intelligence Sharing Plan. *See* Int'l Ass'n of Chiefs of Police & Office of Cmty. Oriented Policing, National Plan for Intelligence-Led Policing at the Local, State and Federal Levels vii, 9-10 (2002), *available at* http://www.ncirc.gov/documents/public/supplementaries/intel_sharing_report.pdf; NCISP 2003, *supra* note 35, at 21-22.

77 The DPD appears to have devoted little of its own resources to counterterrorism intelligence work. Instead, the city and state stepped in to fill this role. The City of Detroit formed an Office of Homeland Security, which is responsible for counterterrorism planning and operations, emergency management, and the protection of critical infrastructure and resources. According to the city's 2012-2013 budget, the Office of Homeland Security will be consolidated under the control of the DPD. However, it is comprised of just two employees (a director and an emergency management specialist) whose counterterrorism intelligence duties remain unclear. *See* Budget Dep't, City of Detroit, *Detroit Office of Homeland Security, in* Executive Budget 46-1, 46-5 (2012), *available at* http://www.detroitmi.gov/Portals/0/docs/budgetdept/2012-13%20Budget/Executive%20Budget/46%20EB%2012-13%20Detroit%20Office%20of%20Homeland%20Security_stamped.pdf; Budget Dep't, City of Detroit, Executive Budget Summary A8, B43 (2012), *available at* http://www.detroitmi.gov/Portals/0/docs/budgetdept/2012-13%20Budget/Executive%20Summary/Budget_2012-13%20OVERVIEW.pdf; *see also* Budget Department, City of Detroit, *Departmental Budget Information: Detroit Office of Homeland Security, in* Executive Budget 46-1, 46-2 (2007), *available at* http://www.detroitmi.gov/Portals/0/docs/budgetdept/2007-08_Budget/Summary/EBS_46_HOMELAND%20SECURITY_07-08.pdf. The Office has worked closely with the state to establish a regional fusion center called the "Detroit and Southeast Michigan Information and Intelligence Center" (DSEMIIC), which adopts an "all crimes, all hazards" approach that includes terrorism. *See* Detroit & Se. Mich. Info. Ctr., Privacy Policy 4 (n.d.) (discussion draft), *available at* http://www.nfcausa.org/files/DDF/DetroitPrivacyPolicy.pdf; IJIS Inst., TA Report Abstract: Detroit and Southeastern Michigan Information and Intelligence Center (DSEMIIC) Review and Assessment 1 (2007), *available at* http://www.kms.ijis.org/db/share/public/Library/TA%20Abstracts/ijis_ta_abstract_detroit_fusion_20080902.pdf.

78 Daniel Fisher, *Detroit Tops The 2012 List Of America's Most Dangerous Cities*, Forbes, Oct. 18, 2012, *available at* http://www.forbes.com/sites/danielfisher/2012/10/18/detroit-tops-the-2012-list-of-americas-most-dangerous-cities/.

79 Dearborn has not created a special unit to handle counterterrorism-related work. When it announced in 2002 that it would establish a "Homeland Security" unit to spearhead counterterrorism efforts, there was widespread community suspicion over fears of government surveillance. Thacher, *supra* note 14, at 662-63. As a result, the city quickly renamed the unit the "Office of Community Preparedness" in an effort to demonstrate that the police would be focused on community protection and not new surveillance efforts. David Thacher recounts one city official's view of the episode: "We got hung for that one. The federal government can call it homeland security, the state can call it homeland security. Dearborn says, "OK, we've got a homeland security [office]." "Why? Have you got terrorists in your town?" No, that's not what we said! ... It was [just] a nice name because it was consistent with the federal government and the state. And of course we quickly changed that name to community preparedness coordinator just so there wouldn't be any more [criticism]. To quiet the ... perception that we had a terrorist problem in Dearborn. Because that's what everyone said, "You're doing this because you must have this problem." *Id.* Indeed, re-naming the office appears to have been more than a symbolic act. While at least one member of the Office is assigned to the local Joint Terrorism Task Force, its activities continue to be centered on increasing coordination with regional and state emergency management. In 2010, it was primarily responsible for administering federal grants related to emergency response programs. City of Dearborn, *Dearborn Police Department Annual Report, in* Administrative Report 2009/2010, at 531, 607-608 (2010), *available at* http://www.cityofdearborn.org/documents/doc_view/721-annual-administrative-report-fy10. It also operates a "Buffer Zone Protection Program" and a public-private partnership called the "Critical Incident Protocol" program. *Id.*

80 The Portland Police Bureau has a Criminal Intelligence Unit (CIU) that recently reestablished ties to the local JTTF and assigns personnel to JTTF activities at the case-by-case discretion of the Chief. As of February 2012, only two officers had been detailed. *See* Memorandum from Mike Reese, Chief, Portland Police Bureau, to Portland City Council 2 (Feb. 28, 2012), *available at* www.portlandonline.com/shared/cfm/image.cfm?id=386900. The CIU collects its own criminal intelligence, but Portland's policy is that "it is the responsibility of the Federal Bureau of Investigation (FBI) to prevent, investigate, and respond to terrorism in the United States." *See* Portland Police Bureau, Criminal Intelligence Unit Standard Operating Procedure #23, at 1 (2011) (on file with the Brennan Center). Consequently, Portland does not have a dedicated counterterrorism intelligence unit.

81 *Hearing Before the Comm'n on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism*, (2008) (statement of Michael R. Bloomberg, Mayor, N.Y.C) [hereinafter Bloomberg Sept. 10, 2008 Testimony], *available at* http://www.nyc.gov/portal/site/nycgov/menuitem.c0935b9a57bb4ef3daf2f1c701c789a0/index.jsp?pageID=mayor_press_release&catID=1194&doc_name=http%3A%2F%2Fwww.nyc.gov%2Fhtml%2Fom%2Fhtml%2F2008b%2Fpr351-08.html&cc=unused1978&rc=1194&ndi=1; *see also Homeland Security: The Next Five Years: Hearing Before the S. Comm. On Homeland Sec. & Governmental Affairs*, 109th Cong. 3-4 (2006) (statement of Richard A. Falkenrath, Deputy Comm'r for Counterterrorism, N.Y. Police Dep't), *available at* http://www.investigativeproject.org/documents/testimony/259.pdf (testifying that in 2006 the NYPD budget for counterterrorism and intelligence was some $200 million).

82 Fin. Div., N.Y.C Council, Hearing on the Mayor's Fiscal 2013 Preliminary Budget & the Fiscal 2012 Preliminary Mayor's Management Report : Police Department 7 (2012), *available at* http://council.nyc.gov/downloads/pdf/budget/2013/056%20Police%20Department.pdf.

83 Raymond W. Kelly, *9/11: 10 Years Later*, The Police Chief, Sept. 2011, at 20, *available at* http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=2473&issue_id=92011; *International Liaison Program*, *supra* note 55. The NYPD has also signed international cooperation agreements, which are historically (and constitutionally) the province of the President of the United States. *See* Jaime Sinapit, *PNP Links up with NYPD to Combat Terrorism, International Crime*, InterAksyon (Nov. 3, 2012), http://www.interaksyon.com/article/47111/pnp-links-up-with-nypd-to-combat-terrorism-transnational-crimes (agreement between the NYPD and the Philippines National Police); *see also* U.S. Const. art. II, § 2, cl. 2 (Treaty Clause).

84 Leonard Levitt, *The NYPD's "Privately" Funded War on Terrorism*, NYPD Confidential (Nov. 7, 2011), http://nypdconfidential.com/columns/2011/111107.html.

85 L.A. Police Dep't Bd. of Police Comm'rs, Intelligence Guidelines for Major Crimes Division: Anti-Terrorism Intelligence Section 2 (2012) [hereinafter LAPD Intelligence Guidelines 2012], *available at* http://www.lapdonline.org/assets/pdf/INTELLIGENCE%20GUIDELINES%20FOR%20MAJOR%20CRIMES%20DIV.pdf. The Board of Police Commissioners recently approved sweeping new guidelines for the Anti-Terrorism Intelligence Section, whose objective is the "detection, collection, analysis and dissemination of information for the purpose of developing a strategy for crime prevention." *Id.* at 2. The unit produces "link charts, timelines, financial analysis, etc." to reveal terrorist trends, networks, and tactics. Counter-Terrorism and Criminal Intelligence Bureau, L.A. Police Dep't, Counter-Terrorism and Crime-Fighting in Los Angeles 4, *available at* http://lapdblog.typepad.com/files/ctcib-approach-and-summary.pdf; LAPD Intelligence Guidelines 2012, at 12. ATIS personnel may open counterterrorism investigations on the basis of tips and leads, including "suspicious activity reports," without reasonable suspicion of criminal activity. *Id.* at 14. Such initial lead investigations may involve photo or video monitoring, the use of informants, or other clandestine surveillance methods. *Id.* at 15-16. But unlike the NYPD, the primary intent of such activities must be to "corroborate information," not to "map" neighborhoods or "bait" community members in an effort to gin up new leads. *Id.* at 16.

86 Email from Michael Downing, Commanding Officer, Counter-Terrorism and Special Operations Bureau to the Brennan Ctr. (Nov. 27, 2012) (Note: The Bureau's $77 million budget covers salaries only and does not include operating expenses or any additional grant funding.).

87 *See* Frank Stoltze, *LAPD Key Player in Preventing Attacks, Chief Says*, S. Cal. Pub. Radio (Sept. 11, 2011), http://www.scpr.org/news/2011/09/11/28770/lapd-key-player-in-preventing-terrorist-attacks-ch/; Judith Miller, *On the Front Line in the War on Terrorism*, City Journal, Summer 2007, *available at* http://www.city-journal.org/html/17_3_preventing_terrorism.html.

88 2 Dist. of Columbia, *Agency Budget Chapters—Part I, in* FY 2013 Proposed Budget and Financial Plan A1, C-6, C-8 (2012), *available at* http://cfo.dc.gov/sites/default/files/dc/sites/ocfo/publication/attachments/ocfo_fy2013_volume_2_chapters_part_1.pdf; Yolanda Branch, Office of the D.C. Auditor, Audit of the Metropolitan Police Department's Investigations and Preliminary Inquiries Involving First Amendment Activities 11 (2012), *available at* http://dcauditor.org/sites/default/files/DCA232012.pdf (Of the 63 intelligence officers, 36 work for the Criminal Intelligence Branch, which includes two undercover officers assigned to conduct First Amendment investigation and three staff members to monitor websites, manage investigations, and write annual reports on First Amendment investigation activities).

89 David Lepeska, *Preparing for 2012, Police Create Counterterrorism Unit*, N.Y. Times, Sept. 8, 2011, *available at* http://www.nytimes.com/2011/09/09/us/09cncpolice.html.

90 The "Counterterrorism and Intelligence Division," now defunct, consisted of six sections: the Airport Law Enforcement; the Bomb and Arson Section; the Deployment Operations Center; the Intelligence Section; the Predictive Analytics Group; and the Public Transportation Section. *See* Office of Budget Mgmt., City of Chi., 2012 Budget Recommendations 218-219 (2011), *available at* http://www.cityofchicago.org/dam/city/depts/obm/supp_info/2012%20Budget/2012MayorsRecommendation.pdf; Chi. Police Dep't, General Order G01-02: Department Organization for Command, attachment 2.5 (2009), *available at* http://directives.chicagopolice.org/attachments/G01-02_Att1.pdf; *see also* Research and Dev. Div., Chi. Police Dep't, Annual Report 2010: A year in Review 52 (2011), *available at* https://portal.chicagopolice.org/portal/page/portal/ClearPath/News/Statistical%20Reports/Annual%20Reports/10AR.pdf.

91 Office of Budget Mgmt., City of Chi., 2013 Budget Recommendations 155 (2012), *available at* http://www.cityofchicago.org/content/dam/city/depts/obm/supp_info/2013%20Budget/2013BUDGETRECFINAL.pdf (listing the Deployment Operations Section under the aegis of the new Office of Crime Control Strategies); Chi. Police Dep't, Department Notice D12-01: Organizational Changes, attachment 2 (2012), *available at* https://portal.chicagopolice.org/portal/page/portal/ClearPath/About%20CPD/CPD%20Organization/DeptOrgChartMar12.pdf.

92 Jeremy Gorner & Robert McCoppin, *Police: Chicago Ends 2012 with 506 Homicides*, Chicago Tribune, Jan. 2, 2013, *available at* http://articles.chicagotribune.com/2013-01-02/news/ct-met-chicago-homicides-2012-20130102_1_homicide-surge-homicide-toll-chicago-homicide-victims.

93 *See* Whet Moser, *Garry MCarthy's New Chicago Crime Strategy: Social Networks, 'Hot People'*, ChiagoMag.com (Oct. 1, 2012), http://www.chicagomag.com/Chicago-Magazine/The-312/October-2012/Garry-McCarthys-New-Chicago-Crime-Strategy-Social-Networks-Hot-People/; *Chicago Shootings: Garry McCarthy Defends Police Strategies as Weekend Gun Violence Continues*, Huffington Post (Aug. 26, 2012, 11:05 AM), http://www.huffingtonpost.com/2012/08/26/chicago-shootings-garry-m_n_1831254.html. As the Chicago Police Department determined in 2004, "Concern about terrorism is real, although what this city can do about it is not clear. Recent attention to violent crime has taken its share of energy that could be directed at responding to some of the program's weak spots." Chi. Cmty. Policing Evaluation Consortium, Community Policing in Chicago, CAPS at Ten ix (2004), *available at* https://portal.chicagopolice.org/i/cpd/clearpath/Caps10.pdf.

94 L.A. Cnty. Sheriffs Dep't, Manual of Policies and Procedures § 2-05/090.00 (2009) (on file with the Brennan Center). The Emergency Operations Bureau is also responsible for collecting "criminal intelligence in support of the overall mission of the department to protect the public health through suppression of criminal activity." Emergency Operations Bureau, *supra* note 67.

95 *Intelligence and Terrorism*, Miami Police Dep't (n.d.), http://www.miami-police.org/intelligence_terrorism.html. According to the department's 2010 annual report, "[o]ne of the most significant investigations involved a multi-million dollar Ponzi scheme which resulted in the prosecution of individuals who defrauded over $35 million from investors and pocketed about $7 million in fraudulent business loans." Miami Police Dep't, Miami Police Dep't Annual Report 10-11 (2010), *available at* http://www.miami-police.org/docs/PD_Annual_Report_10.pdf.

96 Christopher J. Brown, Countering Radicalization: Refocusing Responses to Violent Extremism within the United States 44 (Dec. 2011) (unpublished thesis, Naval Postgraduate School), *available at* www.hsdl.org/?view&did=699530 ("A drawback to this approach is that police departments must carry out normal duties while working to prevent terrorism and meeting the intelligence and agenda requirements of higher agencies."); *see also* Renee Graphia Joyal, State Fusion Centers: Their Effectiveness in Information Sharing & Intelligence Analysis 19-20 (2012) (discussing organizational obstacles to allocating resources for counterterrorism units).

97 Waxman, *supra* note 27, at 383-84; Bayley & Weisburd, *supra* note 61, at 87 ("Besides collecting intelligence and undertaking preventive actions, counterterrorism involves limiting the damage from terrorism and investigating, arresting, and prosecuting those who have done it. It is important to remember that all terrorist attacks are local. This means that although some counterterrorism functions can be the responsibility of dedicated units deployed and centralized levels of organization, police on the ground will necessarily become involved wherever terrorism strikes or is likely to strike.").

98 2010 RAND Report, *supra* note 22, at 82, 97.

99 *Id.* at 97.

100 *See generally* Janet Napolitano, *Homeland Security Begins with Hometown Security*, U.S. Dep't of Homeland Sec. (Aug. 3, 2010, 6:35 PM), http://www.dhs.gov/blog/2010/08/03/homeland-security-begins-hometown-security;

Thacher, *supra* note 14, at 635.

101 Thacher, *supra* note 14, at 637-38; Douglas Page, *Community Policing or Homeland Security: Sophie's Choice For Police?*, Officer.com (Sept. 12, 2011), http://www.officer.com/article/10325312/community-policing-or-homeland-security-sophies-choice-for-police.

102 Thacher, *supra* note 14, at 637-38.

103 *See, e.g.*, *The Role of Local Enforcement in Countering Violent Islamic Extremism: Hearing Before the S. Comm. on Homeland Sec. and Gov'tal Affairs*, 110th Cong. (2007) (statement of Lawrence H. Sanchez, Assistant Comm'r, N.Y.C. Police Dep't) ("The key to it was . . . to start appreciating what most people would say would be non-criminal would be innocuous looking behaviors that could easily be argued in a Western Democracy especially in the United States to be protected by First and Fourth Amendment rights but not to look at them in the vacuum but to look across to them as potential precursors to terrorism"), *available at* http://votesmart.org/public-statement/301624/hearing-of-the-senate-committee-on-homeland-security-role-of-local-law-enforcement-in-countering-violent-islamist-extremism-panel-1.

104 *See* Declaration of Paul Chevigny at ¶ 46, Handschu v. Special Servs. Div., No. 71 Civ. 2203 (S.D.N.Y. Feb. 4, 2013) (on file with the Brennan Center).

105 Carter, Law Enforcement Intelligence, *supra* note 36, at 134 ("It must be emphasized that law enforcement authority to perform any kind of intelligence activity is based solely in the statutory authority to enforce the criminal law, hence the obligation to follow the law of criminal procedure. As such, collecting and retaining information about citizens without an articulable criminal nexus is improper.").

106 In *Laird v. Tatum*, 408 U.S. 1, 5-6 (1972), the Supreme Court suggested that police departments may use informants and undercover officers to attend public events and gather intelligence concerning First Amendment activities in order to detect or prevent crime. However, it also recognized that "constitutional violations may arise from the deterrent, or 'chilling,' effect" of such political surveillance. *Id* at 11. The same can be said about the role of the Equal Protection Clause and constitutional violations that may arise out of discriminatory intelligence gathering. *See, e.g.*, Complaint at 21-22, Hassan v. New York, No. 12-03401 (D.N.J. Oct. 3, 2012), *available at* http://www.ccrjustice.org/files/10_First%20Amended%20Complaint.10.3.2012.pdf. Consequently, many courts have required police to demonstrate – at minimum – that they have a "legitimate law enforcement purpose" that outweighs the potential harm to constitutional interests. *See*, *e.g.,* United States v. Mayer, 503 F.3d 740, 753 (9th Cir. 2007); United States v. Aguilar, 883 F.2d 662, 703 (9th Cir. 1989); *Anderson* v. Davila, 125 F.3d 148, 161 (3d Cir. 1997) ("[W]here the First Amendment is concerned, the motives of government officials are indeed relevant, if not dispositive, when an individual's exercise of speech precedes government action affecting that individual."). Following this logic, courts in New York, Los Angeles, and Chicago have found it reasonable to require police departments to demonstrate "reasonable suspicion" of criminal conduct in order to collect intelligence on otherwise lawful political activities. *See infra*, note 112.

107 *See* Terry v. Ohio 392 U.S. 1, 30 (1968).

108 United States v. Mason, 628 F.3d 123, 128 (4th Cir. 2010) (quoting United States v. Branch, 537 F.3d 328, 336 (4th Cir. 2008)).

109 Handschu v. Special Servs. Div., 349 F.Supp. 766, 768-70 (S.D.N.Y. 1972); *Civil Rights Implications of Post-September 11 Law Enforcement Practices in New York: Hearing Before N.Y. Advisory Comm. to the U.S. Comm. on Civil Rights* (March 2004) (statement of Arthur N. Eisenberg, New York Civil Liberties Union), *available at* http://www.nyclu.org/content/testimony-police-surveillance-of-political-activity-history-and-current-state-of-handschu-de ("[T]he renewed political energy and activity of the 1960's served as a catalyst for the renewed activity of the police intelligence unit in New York City. Accordingly, '[d]uring the sixties, the unit launched a yearly average of one thousand intensive political investigations of dissident groups and individuals and about six hundred lesser probes.' The targets of such police investigations included the NAACP, the ACLU, CORE, the Fifth Avenue Peace Parade Committee, and the Lower East Side Mobilization for Peace Action."); *see also* Chris Hawley, *Barbara Handschu Likens NYPD Spying on Muslims to Spying on Free Speech Advocates*, Huffington Post (Nov. 17, 2011, 7:53 AM), http://www.huffingtonpost.com/2011/11/17/in-nypd-spying-a-yippie-l_n_1099479.html.

110 *Alliance to End Repression v. City of Chicago*, 742 F.2d 1007, 1009 (7th Cir. 1984).

111 Jim Newton, *LAPD Pushing to Relax Limits on Undercover Probes*, L.A. Times, Oct. 11, 1996, *available at* http://articles.latimes.com/1996-10-11/news/mn-52716_1_police-department.

112 *See* Stipulated Consent Decree and Judgment at § IV.A, Coalition Against Police Abuse v. Bd. of Police Comm'rs, No. 243-458 (L.A. Cnty. Ct. Feb. 22, 1984) (permitting preliminary investigations based "upon reasonable and articulated suspicion …"); Alliance to End Repression v. City of Chicago, 561 F.Supp. 537, 564 (N.D. Ill. 1982) (§ 3.2 requires "reasonable suspicion" that evidence of criminal conduct will be obtained); Handschu v. Special Servs. Division, 605 F.Supp. 1384, 1421 (S.D.N.Y. 1985) (requiring "specific information" that the person or group was linked to criminal conduct.). *See also* 69 Cornell L. Rev. at 768-775.

113 Handschu v. Special Servs. Div. 273 F.Supp.2d 327, 329 (S.D.N.Y. 2003); *see also* Christopher Dunn, *Balancing the Right to Protest in the Aftermath of September 11*, 40 Harv. C.R.-C.L. L. Rev. 327, 339 (2005).

114 Handschu, 605 F.Supp. at 1421.

115 Handschu, 273 F.Supp.2d at 333-35, 349. The Los Angeles and Chicago consent decrees were eventually both dissolved. The Los Angeles decree expired in 1996 and the LAPD won changes to the rules that relaxed the threshold for engaging in investigative activities. *See* Newton, *supra* note 111. No longer bound by the decree, the LAPD eliminated the reasonable suspicion requirement and increased its authority to conduct undercover probes in the name of counterterrorism. *Id.* The Chicago decree remained in force as originally written until 2001, when the CPD successfully moved a federal court to eliminate the need to demonstrate indicia of past, present, or imminent future criminal conduct – i.e., the reasonable suspicion requirement. Alliance to End Repression, 237 F.3d 799, 802 (7th Cir. 2001). Judge Posner, writing for the Seventh Circuit, noted that the nature of the issue had changed, with the targets of police investigation being terrorist groups rather than political dissidents. *Id.* The decree was entirely dissolved in 2009 and has not been replaced, although portions of it survive as a part of the department's own rules. *See* Alliance to End Repression, 328 Fed.Appx. 339, 340 (7th Cir. 2009).

116 Under the terms of the revised 2003 Handschu Guidelines, the NYPD may use undercover officers and confidential informants during a "preliminary inquiry," which does not require any "reasonable indication" of criminal activity. Handschu v. Special Servs. Div., 288 F.Supp.2d 411, 423 (S.D.N.Y. 2003) (Appendix A, § V(B)(5)); *see also* Raymond Kelly, Commissioner, N.Y. Police Dep't, Remarks to Fordham Law School Alumni (Mar. 3, 2012), *available at* http://www.nyc.gov/html/nypd/html/pr/pr_2012_03_03_remarks_to_fordham_law_school_alumni.shtml ("This is what Handschu says about the broadest form of intelligence gathering: 'The NYPD is authorized to visit any place and attend any event that is open to the public' and 'to conduct online search activity and to access online sites and forums on the same terms… as members of the public.' The department is further authorized to, 'prepare general reports and assessments… for purposes of strategic or operational planning.' Anyone who intimates that it is unlawful for the Police Department to search online, visit public places, or map neighborhoods has either not read, misunderstood, or intentionally obfuscated the meaning of the Handschu Guidelines.").

117 N.Y. Police Dep't, NYPD Patrol Guide, 2011-A Edition § 212-72 (2011); Handschu v. Special Servs. Div., 288 F.Supp.2d 411, 430-31 (S.D.N.Y. 2003) (Appendix A, § IX).

118 Transcript of Examination Before Trial, *supra* note 73, at 124.

119 *Id.*

120 *See* Handschu, 288 F.Supp. 2d 411, 430-31 (Appendix A, § IX). Moreover, the Demographics Unit's ongoing investigation and infiltration of Muslim organizations in the absence of indications of unlawful terrorist activity also appears to violate sections V(B), (C) and (D) of the *Handschu* Guidelines, which still require some criminal predicate. Declaration of Paul Chevigny, *supra* note 104, at ¶ 4.

121 Declaration of Paul Chevigny, *supra* note 104, at ¶ 8.

122 *Id.*

123 See generally *supra* note 64.

124 L.A. Police Dep't, Special Order No. 11 (2008) [hereinafter LAPD Special Order 11], *reprinted in* Suspicious Activity Report (SAR) Support and Implementation Project, Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project app. B, at 36 (2008), *available at* http://online.wsj.com/public/resources/documents/mccarecommendation-06132008.pdf.

125 *See generally The Nationwide SAR Initiative (NSI)*, Nationwide SAR Initiative, http://nsi.ncirc.gov/(last visited Mar. 5, 2013).

126 *See generally NYPD Shield*, N.Y.C. Police Dep't, http://www.nypdshield.org/public/about.aspx (last visited Mar. 6, 2013).

127 As of 2011, the Nationwide SAR Initiative (NSI) was under various stages of implementation at 33 sites, covering two thirds of the US population. *See Understanding the Homeland Threat Landscape—Considerations for the 112th Congress: Hearing Before the H. Comm. On Homeland Security*, 112th Cong. 13 (2011), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg72212/pdf/CHRG-112hhrg72212.pdf. Chicago, LAPD, Houston, DC, Miami-Dade, and Seattle began participating in the NSI as part of a 2009 pilot program. *See* U.S. Dep't of Justice Et Al., Final Report: Information Sharing Environment (ISE) - Suspicious Activity Reporting (SAR) Evaluation Environment 2 (2010) [hereinafter Evaluation Environment 2010], *available at* http://nsi.ncirc.gov/documents/NSI_EE.pdf; Nationwide SAR Initiative, U.S. Dep't of Justice, Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) 4 (2009), *available at* www.it.ojp.gov/docdownloader.aspx?ddid=1229. A 2012 map of participating sites includes Philadelphia. *Implementation Map*, Nationwide SAR Initiative (Oct. 4, 2012), http://nsi.ncirc.gov/implementation_map.aspx. *See also* Phila. Police Dep't, Directive 126, Collection and Dissemination of Protected Information Policy V (on file with the Brennan Center) (delineating the process for reporting and sharing homeland security information, including SARs). Also note that the NYPD does not participate in the NSI, although the New York State Police have been participants since 2009. Evaluation Environment 2010, at 2.

128 **NYPD:** The NYPD is bound by a federal consent decree, which was modified in 2003 to remove the criminal predicate requirement for various types of investigative activity targeting First Amendment activities. *See supra* notes 113-117.

Chicago: According to a 2012 order issued by Superintendent Garry McCarthy, Chicago police may conduct an investigation implicating First Amendment rights for any "reasonable law enforcement purpose," including "public safety issues, whether they amount to criminal conduct or not." Chi. Police Dep't, General Order G02-02-01, Investigations Directed at First Amendment-Related Information A(2)(b) (2012), *available at* http://directives.chicagopolice.org/directives/data/a7a57be2-12936eaa-d1812-9373-a45df889893a9f52.html.

LA Sheriff: A set of intelligence guidelines prohibits LASD officers from retaining intelligence files unless they contain reasonable suspicion that an individual or group is suspected of being or having been involved in criminal activity. Emergency Operations Bureau, *supra* note 67, at 3. It also prohibits sorting intelligence about "political, religious, or social views, associations, or activities" unless it is "related directly to the criminal predicate which is the basis for focusing on the individual group." *Id.* at 2.

LAPD: *See infra*, notes 131-137; L.A. Police Dep't, Special Order No. 1, at 2-3 (2012) [hereinafter LAPD Special Order 1], *available at* http://stoplapdspying.org/wp-content/uploads/2012/04/SO-1.pdf. In April 2012, the LAPD reportedly agreed to collect SARs only where there is reasonable suspicion of criminal activity, but according to Deputy Chief Michael Downing, who commands the LAPD's Counterterrorism and Special Operations Bureau, "All we did was put the ODNI [Office of the Director of National Intelligence] definition of SAR in the order and separated the 9 non-criminal behaviors from the 6 criminal behaviors and included an indented note about Terry vs Ohio. … There is no real substantive change." Matthew Harwood, *LAPD Agrees to Suspicious Activity Reporting Reforms*, Security Management (Apr. 18, 2012), http://www.securitymanagement.com/news/lapd-agrees-suspicious-activity-reporting-reforms-009873?page=0%2C0; *see also* Press Release, Stop LAPD Spying Coalition, Stop LAPD Spying Coalition Continues to Demand Answers from LAPD About Suspicious Activity Reporting Program (May 22, 2012), *available at* http://stoplapdspying.org/2012/05/beware-of-misleading-stories/. Moreover, the Board of Police Commissioners approved sweeping new guidelines for the Anti-Terrorism Intelligence Section in late 2012, permitting officers to use informants and engage in surveillance for up to 180 days without reasonable suspicion of criminal activity. *See* LAPD Intelligence Guidelines 2012, *supra* note 85, at 5, 15-16 ("The Initial Lead Investigation threshold need not rise to the reasonable suspicion standard …").

Philadelphia: *See* Phila. Police Dep't, *supra* note 127, at 3 (requiring reasonable suspicion of criminal activity in order to collect information about First Amendment conduct and other personal information); *see also* Phila. Police Dep't, Directive 122, Race, Ethnicity, and Policing 1 (2011) (requiring reasonable suspicion to engage in a temporary investigatory detention of an individual and prohibiting the use of race/ethnicity in determining whether there is reasonable suspicion) (on file with the Brennan Center). Pennsylvania state law also requires reasonable suspicion to collect or maintain "protected information," which includes "concerning the habits, practices, characteristics, possessions, associations or financial status of any individual compiled in an effort to anticipate, prevent, monitor, investigate or prosecute criminal activity." *See* 18 Pa. Cons. Stat. § 9106 (Westlaw through 2012 legislation); Linda L. Kelly et al., Office of the Attorney Gen., Commonwealth of Pa., Criminal History Record Information Handbook 3 (6th ed. 2012), *available at* http://www.attorneygeneral.

gov/uploadedfiles/crime/chria.pdf. However, both the regional and state-run fusion centers have privacy policies that appear to conflict with this rule, explicitly permitting the centers to "retain protected information that is based on a level of suspicion that is less than 'reasonable suspicion,' such as tips and leads or suspicious activity report (SAR) information, subject to the policies and procedures specified in this policy."). Pa. Criminal Intelligence Ctr., Pa. State Police, Privacy Policy 4 (n.d.), *available at* http://www.nfcausa.org/files/DDF/PennsylvaniaPaCICApprovedPrivacyPolicy02-11_3.pdf; Del. Valley Intelligence Ctr., Privacy Policy 6 (2011) (on file with the Brennan Center).

Houston: *See* Hous. Police Dep't, General Order 800-07: Criteria for Submitting Incident Reports 2-3 (2007) (on file with the Brennan Center) (requiring officers to report "suspicious persons, vehicles, or activities involved in videotaping, photographing, sketching, drawing … or asking detailed questions regarding buildings"; "a person or event associated with suspicious possession of ... suspicious posters, fliers, or other publications"; "any protest or demonstration associated with terrorism, acts of war, attacks, [or] unusual suspicious activity …"; and "any suspicious person or event not listed in the above categories but determined as suspicious or worthy of reporting by an officer or supervisor.").

Washington, D.C.: *See* DC Code § 5-333.06(a) (permitting "preliminary inquiries" involving First Amendment activities where the police have "information or an allegation the responsible handling of which requires further scrutiny," but "does not justify opening a full investigation because it does not establish reasonable suspicion that persons are planning or engaged in criminal activity."). When conducting a preliminary inquiry, DC police may examine government records and open sources, conduct surveillance, and utilize informants as well as undercover officers. DC Code § 5-333.07(c)-(d). DC models its SAR criteria on an old version of the LAPD's list. *Compare* Metro. Police Dep't, GO-HSC-802.06, § III.A.7 (2011), *available at* https://go.mpdconline.com/GO/GOHSC80206.pdf, *with* L.A. Police Dep't, Special Order 11, *supra* note 124. The fusion center serving the D.C. region, known as the Washington Regional Threat & Analysis Center, also explicitly permits officers to "retain protected information that is based on a level of suspicion that is less than 'reasonable suspicion,' such as tips and leads or suspicious activity report (SAR) information." Wash. Regional Threat and Analysis Ctr., Privacy Policy 3 (2010) (on file with the Brennan Center).

Miami-Dade: Miami-Dade's Homeland Security Bureau (HSB) doubles as a regional fusion center, known as the Southeast Florida Fusion Center (SEFFC). The HSB Standard Operating Procedure recognizes that some databases are subject to the reasonable suspicion requirement in 28 C.F.R. § 23. *See* Homeland Sec. Bureau, Miami-Dade Police Dep't, Standard Operating Procedure 67-69. But the rules do not specify whether it applies this requirement to sharing SARs as part of the NSI. On the contrary, the SEFFC privacy policy states that officers will seek and retain information if it is "based on (a) a criminal predicate *or* (b) a possible threat to public safety, including potential terrorism-related conduct." Se. Fla. Fusion Ctr., SEFFC ISE-SAR EE Privacy Policy: ISE-SAR Evaluation Environment Initiative Privacy, Civil Rights and Civil Liberties Protection Policy 3 (n.d.) (emphasis added), *available at* http://iwatchmiamidade.com/Documents/SEFFC_ISE_SAR_EE_PrivacyPolicy0811.pdf. This policy is consistent with other SAR programs examined by the Brennan Center, including the state-run Florida Fusion Center, which has established a privacy policy that is binding on all participating state and local agencies. Fla. Fusion Ctr., Privacy Policy Version 3.0 3 (2010), *available at* http://www.fdle.state.fl.us/Content/Florida-Fusion-Center/Menu/Privacy-Policy.aspx. Like the SEFFC, the Florida Fusion Center does not have a firm reasonable suspicion requirement, instead permitting officers to seek and retain information that constitutes "a potential threat to public safety," is "relevant" to an ongoing investigation, or is "reasonably believed to be reliable." *Id.* at 6.

Detroit: The Detroit Police Department has a blanket policy forbidding the "collection, indexing, maintenance, or dissemination of information dealing with beliefs, opinions, associations, or expressions of any individual, group, or organization" unless connected to valid law enforcement activities. Detroit Police Dep't, Directive 203.6-2(1) (2008) (on file with the Brennan Center). Any surveillance which has the purpose of gathering the "beliefs, opinions, attitudes, statements, associations and activities of persons, groups or organizations" is prohibited unless the target is violating the law or under reasonable suspicion of violating or conspiring to violate the law. *Id.* at 203.6-2(2). The Chief of Police is responsible for ensuring adherence to the policy and must provide the Board a quarterly report on compliance. *Id.* at 203.6-3.

San Francisco: *See* S.F. Police Dep't, Department General Order 8.10: Guidelines for First Amendment Activities 1 (2008) [hereinafter SFPD DGO 8.10"], *available at* http://www.sf-police.org/modules/

ShowDocument.aspx?documentid=24722 ("The Department may conduct a criminal investigation that involves the First Amendment activities of persons, groups or organizations where there is an articulable and reasonable suspicion to believe that: 1) They are planning or are engaged in criminal activity … and 2) The First Amendment activities are relevant to the criminal investigation.").

Seattle: *See* Seattle Mun. Code § 14.12.150(C) (requiring reasonable suspicion of criminal activity in order to collect information about a person's political or religious associations, activities, beliefs, or opinions); *see also* Seattle Police Dep't, Procedures and Tactics Publication: 024 (2007) [hereinafter Procedures and Tactics Publication] (implementing Seattle Mun. Code § 14.12.150(C)) (on file with the Brennan Center); Seattle Police Dep't, Policies & Procedures: 5.140 – Unbiased Policing at § I(C)(2) (2011) (requiring reasonable suspicion to engage in investigative stops and prohibiting the use of race or ethnicity as a motivating factor in establishing reasonable suspicion) (on file with the Brennan Center); Seattle Police Dep't, Seattle Police Manual § 1.110 IV(B)(1) (2009) (requiring reasonable suspicion of criminal activity for the collection and analysis of information on individuals and groups by the department's Special Investigations Squad and Organized Crime Intelligence Squad).

Miami: Standard operating procedures for Miami's Intelligence and Terrorism Unit (ITU) expressly permit officers to conduct "preliminary inquiries" where "there is not yet a 'reasonable indication' of criminal activities." Intelligence & Terrorism Unit, Miami Police Dep't, *General Principles of Investigations*, *in* Standard Operating Procedure 2 (2012) (on file with the Brennan Center). The ITU may use a preliminary inquiry to investigate a "sensitive criminal matter" such as "the activities of a religious organization or a primarily political organization, or the related activities of any individual prominent in such organizations." *Id*. at 2-3. Such an inquiry may include database queries, the use of previously established informants and confidential sources, interviews, and physical or photographic surveillance. *Id*. at 5. The ITU maintains information generated during these inquiries, including those that have been closed. *Id*. The procedures are silent on when information obtained during an inquiry may be shared or disseminated. Information obtained pursuant to a full investigation based on reasonable suspicion may be disseminated if it "may assist in preventing a crime or the use of violence or any other conduct dangerous to life." *Id*. at 15.

Portland: *See* Or. Admin. Rules § 137-090-0060 (2013) (defining a criminal intelligence file as stored information about the activities and associations of individuals or groups that is based upon reasonable suspicion of criminal activity); Or. Admin. Rules § 137-090-0070 (2013) ("No information will be collected or maintained about the political, religious, racial, or social views, sexual orientation, associations or activities of any individual, group, association organization, corporation, business or partnership unless information directly relates to an investigation of criminal activities, and there are reasonable grounds to suspect the subject of information is, or may be, involved in criminal conduct.").

Minneapolis: *See* Strategic Info. Ctr., Policy & Procedure, Minneapolis Police Dep't at § 2(2)(B) & (E) (n.d.) ("Information gathering for intelligence purpose[s] shall be premised on circumstances that provide a reasonable suspicion … that specific individuals or organizations may be planning or engaging in criminal activity.") ("Criminal intelligence information shall not be collected or maintained about the political, religious, social views, associations or activities of any individual or any group, association, … or other organization, unless there is reasonable suspicion that the subject or information is or may be involved in criminal conduct or activity.") (on file with the Brennan Center).

St. Paul: St. Paul's policies and procedures on collecting information for intelligence purposes are ambiguous at best, if not outright contradictory. The department manual states that only information "related to" criminal activities may be retained, but there is a large gap between "reasonable suspicion of criminal activity" and "related to" criminal activity. St. Paul Police Dep't, St. Paul Police Department Manual 154 (n.d.) (on file with the Brennan Center). Unfortunately, the department has heavily redacted portions of the manual, including entire sections on the use of informants and intelligence information, making it difficult to tell how officers are to implement this rule. *Id.* at 257-60, 263.The manual adds that information will not be gathered about groups or organizations unless they are "known or reasonably suspected of involvement in criminal activities," but there is no similar requirement for personal information. *Id.* at 153. A set of guidelines for the Special Investigation Unit, while unredacted, is equally vexing. With respect to First Amendment activities, the guidelines state that investigations or information gathering operations must be based on "an existing criminal predicate or the reasonable suspicion that unlawful

acts have occurred or may occur." St. Paul Police Dep't, SIU Policy and Guidelines for Investigations and Information Gathering Operations Involving First Amendment Activity 1 (2008) (on file with the Brennan Center). But at the same time, they explicitly permit the use of undercover officers and existing informants at the "preliminary inquiry" stage of investigation, where there "is not yet reasonable suspicion of unlawful activity." *Id.* at 4-5. Using language similar to the modified *Handschu* guidelines that govern the NYPD, reasonable suspicion is required only for "full investigations." *Id.* at 5. Moreover, the guidelines permit officers to seek and maintain information about individuals or organizations based *solely* on the individual's or group's race, ethnicity, and First Amendment-protected activities, provided it is "relevant" to whether an individual or organization is engaged in criminal activity. *Id.* at 2. Corresponding policy in the department manual is redacted.

Dearborn: The City of Dearborn denied the Brennan Center's request for the Dearborn Police Department's policies and procedures for investigations and information collection related to First Amendment activities. However, in a personal interview with the Brennan Center, Chief Ronald Haddad confirmed that Dearborn police officers must have reasonable suspicion of criminal activity in order to collect information about lawful First Amendment activities. Telephone Interview with Dearborn Police Department Chief Ronald Haddad, Dep't Chief, Dearborn Police Dep't (Feb. 26, 2013). It remains unclear, however, whether the reasonable suspicion requirement applies to the collection of intelligence information about activities that are not specifically protected by the First Amendment.

129 *See infra*, notes 244-251.

130 In Houston, officers are required to report: "suspicious persons, vehicles, or activities involved in videotaping, photographing, sketching, drawing … or asking detailed questions regarding buildings"; "a person or event associated with suspicious possession of ... suspicious posters, fliers, or other publications"; "any protest or demonstration associated with terrorism, acts of war, attacks, [or] unusual suspicious activity …"; and "any suspicious person or event not listed in the above categories but determined as suspicious or worthy of reporting by an officer or supervisor." Hous. Police Dep't, *supra* note 128, at 2-4.

131 LAPD Special Order 1, *supra* note 128, at 1 (revising and renaming LAPD Special Order 11, *supra* note 124, which established the LAPD SAR program in 2008).

132 *Id.* at 1-3.

133 *Id.*

134 Yaman Salahi, *Beware of Photographers, Note-Takers and Protesters*, Huffington Post (Sept. 4, 2012, 10:37 AM), http://www.huffingtonpost.com/yaman-salahi/lapd-counter-terrorism_b_1847961.html.

135 L.A. Police Dep't, Departmental Manuel: Volume IV § 271.46 (2012), *available at* http://www.lapdpolicecom.lacity.org/082812/BPC_12-0358.pdf.

136 Recommendations for Fusion Centers, *supra* note 14, at 12-13; Thomas Cincotta, Political Research Assocs., Platform for Prejudice: How the Nationwide Suspicious Activity Reporting Initiative Invites Racial Profiling, Erodes Civil Liberties, and Undermines Security 19 (2010), *available at* http://www.publiceye.org/liberty/matrix/reports/sar_initiative/sar-full-report.pdf; *see also* Stop LAPD Spying Coalition, To Observe And To Suspect: A People's Audit of the Los Angeles Police Department's Special Order 1, at 4 (2013), *available at* http://stoplapdspying.org/wp-content/uploads/2013/03/PEOPLES-AUDIT-FINAL.pdf.

137 Alexander A. Bustamante, Office of the Inspector General, L.A. Police Comm'n, Suspicious Activity Reporting System Audit 2 n. 4 (2013) [hereinafter LAPD SAR Audit], *available at* http://www.lapdpolicecom.lacity.org/031913/BPC_13-0097.pdf.

138 *See, e.g., Selected Suspicious Activity Reports from the Central California Intelligence Center and Joint Regional Intelligence Center*, Am. Civil Liberties Union (Sept. 19, 2013), https://www.aclunc.org/sites/default/files/asset_upload_file470_12586.pdf.

139 Mark Lowenthal, President, Intelligence & Security Acad., Remarks at the Ctr. for Strategic and Int'l Studies Panel: Homeland Security Intelligence Analytic Tradecraft 8 (Sept. 7, 2011), *available at* http://csis.org/files/attachments/110907_hs_intelligence_analytic_tradecraft_transcript.pdf.

140 Patel, *supra* note 42, at 10-11.

141 Letter from Peter Bibring et al., Senior Staff Attorney, Am. Civil Liberties Union of S. Cal., to Charlie Beck, Chief,

L.A. Police Dep't, and Michael Downing, Deputy Chief, L.A. Police Dep't 3 (Mar. 2, 2012), *available at* http://www.chirla.org/sites/default/files/20120312SARSACLUCHIRLA.pdf.

142 *Id.*

143 *Id.* at 4.

144 Complaint at 22, Hassan v. New York, No. 2:12-cv-03401 (D.N.J. Oct. 3, 2012), *available at* http://www.ccrjustice.org/files/10_First%20Amended%20Complaint.10.3.2012.pdf.

145 Defendant's Brief in Opposition to Class Counsel's Motion for Injunctive Relief and Appointment of a Monitor 6, No. 71 Civ. 2201 (S.D.N.Y. May 17, 2013) (on file with the Brennan Center).

146 Floyd v. City of New York, No. 08 Civ. 1034, 2013 WL 4046209, at *6, 22-23 (S.D.N.Y. Aug. 12, 2013).

147 *Id.* at *6.

148 *Id.* at *10. According to Sheriff Leroy Baca of the LASD, the reasonable suspicion requirement keeps law enforcement agencies from "shotgunning societies or groups of people as a general strategy," a strategy that is ineffective to say the least. Leroy Baca, Sheriff, L.A. Sheriff's Dep't, Remarks on Panel 1 at Brennan Center for Justice Symposium: Intelligence Collection and Law Enforcement: New Roles, New Challenges, YouTube.com (Mar. 20, 2011), http://www.youtube.com/watch?v=Op1TgEGVuso.

149 Leroy Baca, *supra* note 144, at 8.

150 Emergency Operations Bureau, *supra* note 67.

151 *See* Bureau of Justice Assistance, U.S. Dep't of Justice, 1998 Policy Clarification 20 (1993), *available at* http://www.it.ojp.gov/documents/28cfr_part_23.pdf ("Information that is relevant to the identification of a criminal suspect or to the criminal activity in which the suspect is engaged may be placed in a criminal intelligence database, provided that (1) appropriate disclaimers accompany the information noting that is strictly identifying information, carrying no criminal connotations; (2) identifying information may not be used as an independent basis to meet the requirement of reasonable suspicion of involvement in criminal activity necessary to create a record or file in a criminal intelligence system; and (3) the individual who is the criminal suspect identified by this information otherwise meets all requirements of 28 CFR Part 23.").

152 Siobhan O'Neil, Cong. Research Serv., RL340114, Terrorist Precursor Crimes: Issues and Options for Congress 25 (2007).

153 *Id.* at 1.

154 *Id.*

155 2012 Senate HSGAC Fusion Center Report, *supra* note 8, at 27.

156 *Cf.* Info. Sharing Env't, A Legal and Policy Approach for Responsible Information Sharing: The Role of the Information Sharing Environment (ISE) 3 (2012), *available at* http://ise.gov/sites/default/files/Legal_and_Policy_Approach_White_Paper.pdf (encouraging state and local agencies to overcome "legal problems" that limit data sharing and change "overly restrictive" interpretations of laws designed to protect privacy and civil liberties).

157 *See* Beth Sheridan & Spencer S. Hsu, *Localities Operate Intelligence Centers To Pool Terror Data*, Wash. Post, Dec. 31, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/12/30/AR2006123000238.html (reporting 37 fusion centers in existence at the end of 2006).

158 Global Justice Info. Sharing Initiative, U.S. Dep't of Justice, et al., Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era 2 (2006) [hereinafter Fusion Center Guidelines], *available at* http://www.it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf.

159 Janet Napolitano, Dep't of Homeland Sec., Address at the National Fusion Center Conference (Mar. 11, 2009), *available at* http://www.dhs.gov/ynews/speeches/sp_1236975404263.shtm.

160 *The National Preparedness Report: Assessing the State of Preparedness: Hearing Before the Subcomm. on Emergency Preparedness, Response, and Commc'ns of the H. Comm. on Homeland Sec.*, 112th Cong. 2 (2012) (statement of Mike Sena, President, National Fusion Center Association), *available at* http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Sena.pdf (counting 77 fusion centers in 2012); GAO-13-233, *supra* note 3, at 10 (counting 78 fusion centers). In addition to the presence of fusion centers in the two U.S. territories listed by Mike Sena in his 2012 testimony, the GAO told the Brennan Center that fusion centers are now present in a total of three

U.S. territories, with the newest center having been established in the U.S. territory of Guam. Telephone Interview with Eileen R. Lawrence, Director, Homeland Sec. and Justice, U.S. Gov't Accountability Office (May 21, 2013).

161 Jerome P. Bjelopera, Cong. Research Serv., R4178, The Federal Bureau of Investigation and Terrorism Investigations 13 (2013), *available at* http://www.fas.org/sgp/crs/terror/R41780.pdf.

162 *Id.*

163 *See generally* Printz v. United States, 521 U.S. 898, 919-22 (1997); New York v. United States, 505 U.S. 144, 176 (1992).

164 2012 Senate HSGAC Fusion Center Report, *supra* note 8, at 27, 35-36, 61.

165 Global Info. Sharing Initiative, U.S. Dep't of Justice, The National Criminal Intelligence Sharing Plan (2003), *available at* http://www.au.af.mil/au/awc/awcgate/doj/nat_crim_intel_share_plan2003.pdf.

166 Fusion Center Guidelines, *supra* note 158, at 29.

167 *Id.* at 33.

168 Council of State Gov'ts & E. Ky. Univ., The Impact of Terrorism on State Law Enforcement: Adjusting to New Roles and Changing Conditions 7 (June 2006) (unpublished report), *available at* https://www.ncjrs.gov/pdffiles1/nij/grants/216642.pdf (estimating that approximately three-quarters of state law enforcement agencies serve as their "state's leader for gathering, analyzing and sharing terrorism-related intelligence."). The study also found that 92% of state law enforcement agencies allocated substantial resources for intelligence gathering, analysis, and sharing since 9/11. *Id.* at 24.

169 *See* Nenneman, *supra* note 14, at 78-86; *see also* Chi. Police Dep't, Special Order 05-08-03: Terrorism Liaison Officer (TLO) Program (2009) (on file with the Brennan Center).

170 U.S. Gov't Accountability Office, GAO-11-223, Information Sharing: DHS Could Better Define How it Plans to Meet its State and Local Mission and Improve performance Accountability 19 n.33 (2010), *available at* http://www.gao.gov/new.items/d11223.pdf ("Of the 72 designated fusion centers, 50 (one in each state) are considered the primary designated state fusion centers. The remaining 22 centers are "secondary designated" fusion centers. Secondary fusion centers are located in cities that receive Urban Area Security Initiative funding—grants administered by the Federal Emergency Management Agency to state, local, tribal jurisdictions, and urban areas to build and sustain national preparedness capabilities—and agree to work in conjunction with the primary fusion center."); Info. Sharing Env't, ISE-G-112, Information Sharing Environment Guidance (ISE-G): Federal Resource Allocation Criteria (RAC) 3 (2011), *available at* http://www.ise.gov/sites/default/files/RAC_final.pdf.

171 GAO-13-233, *supra* note 3, at 24-25.

172 2012 Senate HSGAC Fusion Center Report, *supra* note 8, at 27.

173 *Id.* at 36-38, 57-59; *see also* Michael Price, *Senate to DHS: No Tanks, Thanks*, The Hill (Dec. 6, 2012, 4:00 PM), http://thehill.com/blogs/congress-blog/economy-a-budget/271511-senate-to-dhs-no-tanks-thanks.

174 Due to anticipated reductions in federal grant funding, the Oregon Terrorism Information Threat Assessment Network reported in December 2012 that Oregon may become the "first state in the nation to close the doors on its fusion center." Queenie Wong, *Budget Cuts May Close Salem Terrorism Center*, Statesman Journal, Dec. 4, 2012. The Texas state legislature has also taken steps to close the state-level Texas Fusion Center due to concerns that it has been expensive and ineffective. Brenda Bell, *Budget Conferees Vote Not to Fund DPS Fusion Center*, Austin American-Statesman, May 14, 2003, *available at* http://www.mystatesman.com/news/news/budget-conferees-vote-not-to-fund-dps-fusion-cente/nXrPx/. *See also* Jonathan Tamari, *Federal Report Cites Unfinished Philadelphia Counterterrorism Center as Flawed*, Phila. Inquirer, Oct. 5, 2012, *available at* http://articles.philly.com/2012-10-05/news/34261225_1_regional-intelligence-center-federal-money-fusion-centers (cataloguing the sluggish and expensive operation underway in Philadelphia to house its regional fusion center in a new facility).

175 2012 HSPI Report, *supra* note 48, at 27.

176 Nenneman, *supra* note 14, at 2-3.

177 2010 RAND Report, *supra* note 22, at 52.

178 2012 HSPI Report, *supra* note 48, at 1.

179 *See* Intelligence Reform and Terrorism Prevention Act, Pub. L. No. 108-458 § 1016, 118 Stat. 3638, 3664 (as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007, §§ 501-504); *see also* 9/11 Report, *supra* note 28, at 427 ("The FBI is just a small fraction of the national law enforcement community in the United States, a community comprised mainly of state and local agencies. The network designed for sharing information, and the work of the FBI through local Joint Terrorism Task Forces, should build a reciprocal relationship, in which state and local agents understand what information they are looking for, and, in return, receive some of the information being developed about what is happening, or may happen, in their communities. In this relationship, the Department of Homeland Security will also play an important part.").

180 Office of the Program Manager for the Info. Sharing Env't et al., Suspicious Activity Reporting Functional Standard and Evaluation Environment: Initial Privacy and Civil Liberties Analysis 6 (2008) [hereinafter Initial Privacy and Civil Liberties Analysis], *available at* http://www.ise.gov/sites/default/files/ISE_SAR_Initial_Privacy_and_Civil_Liberties_Analysis.pdf.

181 Global Justice Info. Sharing Initiative, U.S. Dep't of Justice, Baseline Capabilities for State and Major Urban Area Fusion Centers: A Supplement to the *Fusion Center Guidelines* 15 (2008), *available at* www.it.ojp.gov/documents/baselinecapabilitiesa.pdf.

182 Nationwide SAR Initiative, U.S. Dep't of Justice, Annual Report 2011 3 (2012), *available at* http://nsi.ncirc.gov/documents/NSI_Annual_Report_2011.pdf.

183 *Id.*

184 Info. Sharing Env't, ISE-FS-200, Information Sharing Environment (ISE) Functional Standard (FS): Suspicious Activity Reporting (SAR) 9, 29-30 (2009) [hereinafter ISE-SAR Functional Standard], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-dhswide-sar-ise-appendix.pdf.

185 *Id.* at 2.

186 *Id.* at 26 (recognizing that purge policies vary from jurisdiction to jurisdiction).

187 *See infra*, notes 252-257.

188 2012 Senate HSGAC Fusion Center Report, *supra* note 8, at 27.

189 Initial Privacy and Civil Liberties Analysis, *supra* note 180, at 15.

190 Suspicious Activity Report (SAR) Support and Implementation Project, Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project 30 (2008), *available at* http://online.wsj.com/public/resources/documents/mccarecommendation-06132008.pdf.

191 *Are We Safer?: Interview of Michael German*, PBS (Nov. 18, 2010), http://www.pbs.org/wgbh/pages/frontline/are-we-safer/interviews/michael-german.html#2.

192 GAO-13-233, *supra* note 3, at 22-25.

193 Jerome B. Bjelopera, Cong. Research Serv., R41780, The Federal Bureau of Investigation and Terrorism Investigations 13 (2011), *available at* http://www.fas.org/sgp/crs/terror/R41780.pdf.

194 *Id.* at 15.

195 Three of the 19 fusion centers surveyed in this report are known to be co-located with their local JTTF: the Los Angeles Joint Regional Intelligence Center, the Northern California Regional Intelligence Center, and the Washington State Fusion Center.

196 In addition to the eGuardian and Guardian networks, the FBI also operates the Law Enforcement Regional Data Exchange (R-DEx) and National Data Exchange (N-DEx), both of which provide access to criminal justice data. Moreover, the Department of Justice funds six interstate Regional Information Sharing Systems (RISS) that pre-date 9/11 and are strictly limited to criminal intelligence that has met the reasonable suspicion threshold.

197 Recall that the FBI has encouraged fusion center participation by advertising that the eGuardian system would maintain "inconclusive" files for up to five years, during which time they would be viewable by other law enforcement agencies. *Protecting National Security and Civil Liberties: Strategies for Terrorism Information Sharing: Hearing Before the Subcomm. On Terrorism & Homeland Sec. of the S. Comm. On the Judiciary*, 111th Cong. 11 (2009) (statement of Caroline Fredrickson, Dir., Am. Civil Liberties Union Wash. Legis. Office) [hereinafter *Statement of Caroline Fredrickson*], *available at* http://www.fas.org/irp/congress/2009_hr/042109fredrickson.pdf; *Privacy Impact*

Assessment for the eGuardian Threat Tracking System, Fed. Bureau of Investigation [hereinafter *eGuardian Privacy Impact Assessment*], http://www.fbi.gov/foia/privacy-impact-assessments/eguardian-threat (last visited Mar. 10, 2013) ("…[I]f a nexus to terrorism can neither be substantiated nor discounted, the Referred report is determined to be inconclusive, marked as such, and then referred to Guardian for further assessment by the JTTF. Again, at this point, the Referred report will be viewable to other law enforcement agencies with eGuardian accounts. The report will continue to remain in the eGuardian system for tracking and further analytic review. The information in these reports – where a nexus to terrorism is inconclusive or a nexus to terrorism has been substantiated – will be maintained for five years.").

198 Fed. Bureau of Investigation, U.S. Dep't of Justice, eGuardian Brief: IACP 2009 4 (2009), *available at* http://www.aclu.org/files/assets/aclueg000072.pdf; *eGuardian Privacy Impact Assessment*, *supra* note 197 ("If a clear determination is made of "a nexus to terrorism," the information will be passed along to the eGuardian SDR for further dissemination and then on to Guardian for analysis. If no determination can be made regarding "a nexus to terrorism," but neither can the nexus be discounted, the information will be added to the eGuardian SDR for pattern and trend analysis."); *see also* Program Manager, Info. Sharing Env't, Nationwide Suspicious Activity Reporting Initiative: Concept of Operations 14 (2008), *available at* http://nsi.ncirc.gov/documents/NSI_CONOPS_Version_1_FINAL_2008-12-11_r4.pdf.

199 GAO-13-233, *supra* note 3, at 8.

200 *Id.* at 53.

201 *Id.* at 18; U.S. Dep't of Homeland Security, 2011 National Network of Fusion Centers: Final Report 20-21 (2012), *available at* http://www.dhs.gov/sites/default/files/publications/2011-national-network-fusion-centers-final-report.pdf.

202 Fed. Bureau of Investigation, U.S. Dep't of Justice, eGuardian 1 (2008), *available at* http://www.aclu.org/files/assets/aclueg000014.pdf; Fed. Bureau of Investigation, U.S. Dep't of Justice, eGuardian Quick Study Instructional 3 (n.d.), *available at* http://www.aclu.org/files/assets/aclueg000040.pdf.

203 GAO-13-233, *supra* note 3, at 53.

204 *Id.*

205 GAO-13-233, *supra* note 3, at 19-20.

206 *Id.* at 7 n. "a".

207 *eGuardian Privacy Impact Assessment*, *supra* note 197, at 6.

208 GAO-13-233, *supra* note 3, at 7 n. "a".

209 *Id.* at 15.

210 *Id.* at 16.

211 *Id*. at 2.

212 *Id*. at 17.

213 Dr. Bridget Nolan, a sociologist at the University of Pennsylvania and a former intelligence analyst at the National Counterterrorism Center (NCTC), interviewed 20 of her NCTC colleagues about their work and found that it is "best described as chaotic and overwhelming," due in large part to the "perils of too much information." Bridget Rose Nolan, Information Sharing and Collaboration in the United States Intelligence Community: An Ethnographic Study of the National Counterterrorism Center 22-23 (2013) (unpublished Ph.D. dissertation, University of Pennsylvania), *available at* http://media.philly.com/documents/Nolan_Dissertation.PDF. According to one analyst, "people will send everything to everybody" for fear of missing something, "but when everybody does that, it creates its own noise. And people drown in it. And as a consequence of too much information sharing, key pieces of information … may be ignored." *Id.* "More information is not necessarily better," the analysts concludes. "Better information is better." *Id.* at 29. Consequently, Nolan recognizes that "many analysts balk when reporters or politicians use the phrase 'connecting the dots' … [as if it were] as simple as completing the activities on a child's paper placemat. … 'The page is black with dots.'" *Id.* at 33.

214 2012 Senate HSGAC Fusion Center Report, *supra* note 8, at 27.

215 *Id.* at 36-38, 57-59.

216 Select Comm. to Study Governmental Operations with respect to Intelligence Activities, Intelligence Activities and the Rights of Americans: Book II, S. Rep. No. 94-755, at 259 (1976), *available at* http://www.intelligence.senate.gov/pdfs94th/94755_II.pdf.

217 *Id.* at 260 (internal footnotes omitted).

218 ISE-SAR Functional Standard, *supra* note 184, at 2.

219 *Id.* at 29 n. 11.

220 Global Justice Info. Sharing Initiative, U.S. Dep't of Justice, Tips and leads Issue Paper 3 (2007) [hereinafter Tips and Leads Issue Paper] (on file with the Brennan Center).

221 2012 Senate HSGAC Fusion Center Report, *supra* note 8, at 36.

222 *See, e.g.*, *More About Suspicious Activity Reporting*, Am. Civil Liberties Union (Jan. 18, 2013), http://www.aclu.org/spy-files/more-about-suspicious-activity-reporting.

223 ISE-SAR Functional Standard, *supra* note 184, at 29 n.11.

224 *Id.*

225 *Id.* at 33.

226 Terry v. Ohio, 392 U.S. 1, 27 (1968) (describing reasonable suspicion as something more than an "inchoate and unparticularized suspicion or 'hunch,'" and based on "specific reasonable inferences" drawn from the facts and an officer's experience).

227 *See Characteristics of Terrorist's Surveillance*, L.A. Police Dep't, http://www.lapdonline.org/home/content_basic_view/27436 (last visited Mar. 11, 2013); N. Cal. Regional Intelligence Ctr., Anti-Terrorism (2012) (on file with the Brennan Center).

228 ISE-SAR Functional Standard, *supra* note 184, at 29 n.11.

229 The 2009 revised Functional Standard *allows* fusion centers to omit "privacy fields" containing personally identifiable information from an ISE-SAR when the report lacks a nexus to terrorism-related crime. *Id.* at 12. But the Functional Standard does not *require* fusion centers to omit personal information. *Id.* ("Each ISE participant can exclude additional data elements from the Summary ISE-SAR Information format in accordance with its own legal and policy requirements.).

230 *Id.*

231 2012 Senate HSGAC Fusion Center Report, *supra* note 8, at 36-38. To their credit, DHS privacy officials eventually cancelled federal intelligence reports that sought to use this information, noting that the activities were constitutionally protected and that there was nothing illegal, nefarious, or objectionable about them. *Id.* According to the Senate investigation, had federal employees disseminated such reports themselves, they would have violated provisions of the Privacy Act of 1974. *Id.* at 35. The Privacy Act prohibits federal officials from collecting or maintaining information about people in United States for the purpose of monitoring their exercise of First Amendment freedoms. 5 U.S.C § 522a (e)(7) (2013). Fusion centers are almost always owned and operated by state and local authorities, exempting them from the Act. 5 U.S.C. § 552a(e)(7); 2012 Senate HSGAC Fusion Center Report, *supra* note 8, at 35.

232 2012 Senate HSGAC Fusion Center Report, *supra* note 8, at 38.

233 *See, e.g.*, Declaration of Deputy Commissioner David Cohen, *supra* note 41, at ¶ 52; Philip Mudd, Former Deputy Director, Fed. Bureau of Investigation, Nat'l Sec. Branch, Remarks on Panel 3 at Brennan Center for Justice Symposium: Intelligence Collection and Law Enforcement: New Roles, New Challenges (March 18, 2011) (transcript on file with the Brennan Center). ("[The Intelligence Reform and Terrorism Prevention Act of 2004 dictated] that the [FBI] must have a preventive counter terrorism posture. That means stop things before they happen. That means by definition, you cannot always tether investigations to proof of criminal activity. It's not a choice by the Department of Justice, by the executive branch, and by people like me."); *see also* Office of the Inspector General, U.S. Dep't of Justice, Audit Report 04-10, The Federal Bureau of Investigation's Efforts to Improve the Sharing of Intelligence and Other Information 18 (2003), *available at* http://www.justice.gov/oig/reports/FBI/a0410/final.pdf (noting that after 9/11, the FBI "lacked the ability to 'connect the dots' or create a mosaic of information.").

234 2012 Senate HSGAC Fusion Center Report, *supra* note 8, at 27.

235 *See supra* notes 206-210.

236 A 2011 DHS survey found that 66.2 percent of fusion centers use eGuardian, while 38.2 percent use an ISE Shared Space. *Id.* And the Government Accountability Office found that as of November 2012, all fusion centers have adopted eGuardian while only 73 percent use ISE Shared Spaces. U.S. Gov't Accountability Office, *supra* note 3, at 18.

237 *Id.* at 33-38.

238 *Id*. at 33-34 (between January 2010 and October 2012, there were 24,599 ISE-SARs added to the ISE, approximately 1,200 of which resulted in an FBI investigation).

239 *Id*. at 35.

240 28 C.F.R. § 23.20(a).

241 *Id*. at § 23.20(b).

242 Tips and Leads Issue Paper, *supra* note 220, at 1.

243 Tautologically, the DOJ distinguishes the two categories by defining "criminal intelligence" as information that meets the reasonable suspicion requirement whereas "tips and leads" or SARs do not. *Id.* This is consistent with the ISE-SAR Functional Standard, which states that fusion centers may share "fact information" without a criminal predicate "in accordance with 28 CFR Part 23." ISE-SAR Functional Standard, *supra* note 184, at 33.

244 Tips and Leads Issue Paper, *supra* note 220, at 2. Because revisions to the Functional Standard in 2009 did not include reasonable suspicion requirement, fusion centers are still relying on DOJ's guidance in this paper.

245 *Id.* at 2-3. The concept of a "temporary" or "working" file is not new. As early as the 1970s, a private organization called the Law Enforcement Intelligence Unit (LEIU) developed guidance "interpreting" 28 CFR 23 and creating a model policy for law enforcement agencies known as the *LEIU File Guidelines*. One of the most prominent differences between 28 CFR 23 and the *Guidelines* is the way in which the *Guidelines* treat information lacking a criminal predicate. They propose the concept of a "temporary file" in which to store such information for a period of time before being moved to a "permanent file" – if a criminal predicate is established – or being purged from the system. Law Enforcement Intelligence Unit, Criminal Intelligence Guidelines § IV(B) (2002), *available at* http://www.it.ojp.gov/documents/LEIU_Crim_Intell_File_Guidelines.pdf. To be clear, 28 CFR 23 does not even hint at the notion of a "temporary file." David Carter, however, argues that the *Guidelines* are designed to fill a perceived "operational gap" in the law. Carter, Law Enforcement Intelligence, *supra* note 36, at 149. According to Carter: "Often, intelligence personnel will receive a tip from the public or perhaps a Suspicious Activity Report (SAR) which suggests a crime but has insufficient information to establish a criminal predicate. … Since the 28 C.F.R. Part 23 guidelines do not address this circumstance, a practical interpretation of the regulation … was created in the *LEIU File Guidelines*." *Id.* at 153-54.

246 *Statement of Caroline Fredrickson*, *supra* note 197, at 11; *see also eGuardian Privacy Impact Assessment*, *supra* note 197 ("In keeping with the retention period currently in effect for state criminal intelligence systems under 28 C.F.R. Part 23, suspicious activity reports in this third category (reports for which a determination cannot be made whether or not a nexus to terrorism exists) will be retained for a period of five years and will be used for analytical purposes and/or to demonstrate trends.").

247 *See* 28 C.F.R. § 23.20(a). The FBI's statement appears to ignore this rule and misstate the purpose of 28 C.F.R. § 23.20(h), which authorizes the retention of information that satisfies the reasonable suspicion requirement for up to five years.

248 Tips and Leads Issue Paper, *supra* note 220, at 1.

249 *See, e.g.*, U.S. Dep't of Homeland Sec., Homeland Security Grant Program: Guidance and Application Kit 4 (2009), *available at* http://www.fema.gov/pdf/government/grant/2010/fy10_hsgp_kit.pdf (requiring privacy policies "at least as comprehensive as the ISE Privacy Guidelines"); *see also* Info. Sharing Env't, Guidelines to Ensure That the Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment 5-6 (n.d.), *available at* http://www.ise.gov/sites/default/files/PrivacyGuidelines20061204.pdf; Initial Privacy and Civil Liberties Analysis, *supra* note 180, at 17.

250 Tips and Leads Issue Paper, *supra* note 220, at 1.

251 Cal. State Terrorism Threat Assessment Sys., Information Privacy Policy 1 (n.d.) [hereinafter Cal. STTAS Privacy Policy], *available at* http://www.nfcausa.org/files/DDF/CaliforniaSTTASPrivacyPolicy3.pdf; *see also*

Major Crimes Div., L.A. Police Dep't, Divisional Order No. 15: Privacy Guidelines for Information Sharing Environment, Suspicious Activity Report (ISE-SAR) Evaluation Environment Initiative 1 (2009) (emphasis added), *available at* http://documents.law.yale.edu/sites/default/files/LAPD_Div_Order15_Aug09-ocr.pdf ("Application of 28 CFR Part 23: All ISE-SAR information posted to LAPD's shared space under the Initiative shall meet *applicable* provisions of 28 CFR Part 23. This is to include applying the operating policies set forth in 28 CFR § 23.20 to all individual and organizational criminal subjects …").

252 Cal. STTAS Privacy Policy, *supra* note 251, at 4; Major Crimes Div., L.A. Police Dep't, Divisional Order No. 16: Privacy Guidelines for Evaluation Environment Initiative 3 (2009) (on file with the Brennan Center) ("Retention and Destruction: … Information submitted and determined to qualify as an ISE-SAR, but which does not reach the reasonable suspicion standard of 28 CFR Part 23, will be retained as a temporary file for up to one-year to permit the information to be validated or refuted and its credibility and value to be assessed. … Temporary files that are evaluated during their retention period and determined to meet applicable 28 CFR Part 23 and ISE-SAR criteria, shall be submitted to the shared space. 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, as appropriate.").

253 According to the Houston privacy policy, "[a]ll information and intelligence will be obtained lawfully and products produced will be handled in accordance with 28 CFR Part 23, and applicable State of Texas laws." Hous. Reg'l Intelligence Serv. Ctr. (HRISC), Houston Regional Intelligence Service Center (Fusion Center) Privacy Policy: Privacy, Civil Rights, and Civil Liberties Policy 4 (2009), *available at* http://www.nfcausa.org/files/DDF/Privacy%20Policy%20HRISC%20September%2009%20SSNP%20.pdf.

254 *Id.* at 6 ("All SAR data, Inquiries, including tips and leads that are in the SAR database will be kept in that database for a period of one year, unless there is reasonable suspicion of criminal activity, in which [case] they can be retained for up to five years.").

255 *eGuardian Privacy Impact Assessment*, *supra* note 197.

256 U.S. Gen. Accounting Office, Office of the Comptroller General, GGD-81-36, The Multi-State Regional Intelligence Projects – Who Will Oversee These Federally Funded Networks? 9 (1980), *available at* http://www.gao.gov/assets/140/132128.pdf.

257 *Id.* at 11. As initially conceived, the LEAA guidelines did not specify the level of suspicion necessary to collect and maintain intelligence information. But in response to privacy concerns raised during a notice and comment period, the Justice Department revised the guidelines to explicitly require reasonable suspicion of criminal activity. Criminal Intelligence Systems Operating Policies, 43 Fed. Reg. 28,572 (June 30, 1978). The LEAA touted the result as "some pretty tough, tight guidelines on insuring [sic] that grants for intelligence activities were not used in violation of privacy and political rights of individuals." *Law Enforcement Assistance Reform: Hearing on S. 241 Before the S. Committee on the Judiciary*, 96th Cong. 78 (1979) (statement of Henry S. Dogin, Acting Administrator of the LEAA) (According to the LEAA Administrator, the guidelines "are an indication of how much we are concerned with the privacy and security of these intelligence systems.").

258 In 1979, Congress passed the Justice System Improvement Act, which restructured the Department of Justice and replaced the LEAA with the Office of Justice Assistance, Research, and Statistics (OJARS). Pub. L. No. 96-157 § 801, 93 Stat. 1167, 1201 (1979). An amendment to the Act introduced by Rep. William Edwards of California required OJARS to prescribe a set of guidelines that would govern all federally funded criminal intelligence systems. And members of Congress already knew exactly what to expect out of OJARS – the LEAA guidelines. Responding to a question on the House floor about what standard the guidelines would employ, Rep. Edwards invoked the LEAA policy: "Mr. Chairman, does the gentleman say there must be criminal activity involved or potential suspected criminal activity? There is a big difference. The guidelines that are in existence at the moment are instructions from LEAA to say that criminal intelligence information shall be maintained only if it is reasonably suspected that the individual is involved in criminal activity." 125 Cong. Rec. 27,699 (Oct. 10, 1979) (statement of Rep. William Donlon Edwards). Indeed, the standard promulgated by OJARS in 1980 and codified in 28 CFR 23 is identical to the 1978 LEAA guidelines: "Criminal intelligence information concerning an individual shall be collected and maintained only if it is reasonably suspected that the individual is involved in criminal activity and that the information is relevant to that criminal activity." *Compare* Criminal Intelligence Systems Operating Policies, 43 Fed. Reg. 28,572 § I(A) (June 30, 1978*) with* 28 C.F.R. § 23.20(a).

259 Office of Justice Programs, U.S. Dep't of Justice, 1993 Revision and Commentary: Final Revision to the

Office of Justice Programs, Criminal Intelligence Systems Operating Policy 11 (1993), *available at* http://www.it.ojp.gov/documents/28cfr_part_23.pdf.

260 Am. Civil Liberties Union, Unleashed and Unaccountable: The FBI's Unchecked Abuse of Authority 23-27 (2013), *available at* https://www.aclu.org/sites/default/files/assets/unleashed-and-unaccountable-fbi-report.pdf.

261 Cynthia A. Brown, *Divided Loyalties: Ethical Challenges for America's Law Enforcement in Post 9/11 America*, 43 Case W. Res. J. Int'l L. 651, 667 (2011).

262 *See* Kim Murphy, *L.A. Sheriff Watchdog Merrick Bobb Hired as Seattle Police Monitor*, L.A. Times, Oct. 30, 2012, *available at* http://www.latimes.com/news/nation/nationnow/la-na-nn-merrick-bobb-seattle-police-20121030,0,6073936.story.

263 Police Assessment Res. Ctr., Review of National Police Oversight Models for the Eugene Police Commission 2 (2005), *available at* http://www.parc.info/client_files/Eugene/Review%20of%20National%20Police%20Oversight%20Models%20%28Feb.%202005%29.pdf; *see also* Merrick Bobb, Police Assessment Res. Ctr Internal and External Police Oversight in the United States 9-19 (2005), *available at* http://www.parc.info/client_files/Altus/10-19%20altus%20conf%20paper.pdf.

264 Police Assessment Res. Ctr., *supra* note 263, at 11.

265 City of Houston, Executive Order No. 1-5 Revised § 6.1 (2011) (Independent Police Oversight Board), *available at* http://www.houstontx.gov/execorders/1-5.pdf.

266 The Inspector General for the City of Houston serves as an "ombudsmen" to assist citizens in filing complaints. City of Houston, Executive Order No. 1-39 Revised § 5.1.5 (2011) (Establishment of Office of Inspector General for Investigation of Employee Misconduct), *available at* http://www.houstontx.gov/legal/1-39.pdf. The IG may also conduct its own investigation if it agrees with the Independent Police Oversight Board that additional investigation is necessary and the Chief of Police has refused to do so. City of Houston, Executive Order No. 1-5, *supra* note 265, at § 7.1.6; City of Houston, *Press Conference: Police Oversight Initiatives*, YouTube.com (Feb. 23, 2011), http://www.youtube.com/watch?v=Sk9wuAY5G7k. The Houston Independent Police Oversight Board also has authority to make policy recommendations on a limited range of issues: hiring new police officers, training on the proper treatment of citizens, and community concerns. City of Houston, Executive Order No. 1-5, *supra* note 265, at § 5.2.

267 Cindy George, *Some Doubt City's Efforts to Rebuild Trust in HPD*, Houston Chron. (Feb. 18, 2011), http://www.chron.com/news/houston-texas/article/Some-doubt-city-s-efforts-to-rebuild-trust-in-HPD-1690326.php; *see also Who's Policing the Police?*, MyFox Houston (Feb. 11, 2011), http://www.myfoxhouston.com/story/18179645/whos-policing-the-police; James Pinkerton, *Punishments for HPD Officers Often Unravel*, Houston Chron. (Feb. 20, 2011), http://www.chron.com/news/houston-texas/article/Punishments-for-HPD-officers-often-unravel-1687733.php.

268 *See generally What We Do*, Office of Ombudsman of L.A. Cnty., http://ombudsman.lacounty.info/what-we-do.aspx (last visited Mar. 18, 2013). The Ombudsman "only reviews completed service reviews or investigations which have been appealed to the Ombudsman by dissatisfied complainants. The Ombudsman does not have investigative authority and is not empowered to initiate or conduct an administrative investigation, nor will he involve himself in criminal investigations of misconduct." *Transparency, Openness, Public Trust, and the Los Angeles County Sheriff's Department*, L.A. Cnty. Sheriff's Dep't, http://1.usa.gov/XIE24H (last visited Mar. 18, 2013).

269 The St. Paul Police-Civilian Internal Affairs Review Commission is a seven-member commission that includes two St. Paul police officers; all members are appointed by the mayor with approval by the city council. Police-Civilian Internal Affairs Review Comm'n, City of Saint Paul, Annual Report: 2009 6 (2010), *available at* http://www.stpaul.gov/DocumentCenter/Home/View/13234. The police department's internal affairs unit investigates all civilian complaints. *Id.* The Review Commission has subpoena power and can review completed investigations, but the final word on disposition and discipline belongs to the police chief. *Id.* at 12, 14.

270 The Portland Citizen Review Committee is a six-member body appointed by the City Council and includes at least two community members as well as the director of the Independent Police Review Division, which is part of the Office of the City Auditor. Office of the City Auditor, City of Portland, PSF-5.06, Citizen Review Committee (CRC) – Independent Police Review Division (IPR) – Process for Appointment and Reappointment to the CRC ¶ 2 (2007), *available at* http://www.portlandonline.com/auditor/index.cfm?&a=9035&c=27455. The Review Committee does not process civilian complaints; it hears appeals and is limited to agreeing or disagreeing

with the police department's investigation. Office of the City Auditor, City of Portland, PSF-5.03, Citizen Review Committee (CRC) – Independent Police Review Division (IPR) – Appeals Procedures (2012), *available at* http://www.portlandonline.com/auditor/index.cfm?&a=9030&c=27455. The Review Committee does not have subpoena power.

271 The Seattle Office of Professional Accountability Auditor is an independent civilian contractor appointed by the mayor and confirmed by the city council. Seattle, Wash., Code § 3.28.850 (2002), *available at* http://clerk.seattle.gov/~scripts/nph-brs.exe?d=CODE&s1=3.28.850.snum.&Sect5=CODE&Sect6=HITOFF&l=20&p=1&u=/~public/code1.htm&r=1&f=G. Although the name of the office has been the source of some confusion, the Auditor functions like an appellate review board, responsible for "auditing" all investigations conducted by the Office of Professional Accountability. *Id.* at § 3.28.855; Office of Prof'l Accountability Review Bd., City of Seattle, Policy Report: Revised Names, Roles, and Powers of the Office of Processional Accountability Review Board 5-6 (2012) [hereinafter Review Board Policy Report], *available at* http://clerk.seattle.gov/~CFS/CF_312426.pdf. The Auditor does not have subpoena power, but he or she can request additional investigation. *Id.* The Auditor prepares biannual reports on these investigations and can make policy recommendations but is not allowed to make any disciplinary recommendations. *Id.*; *see, e.g.*, Anne Levinson, Office of Prof'l Accountability, Semi-Annual Report of the Civilian Auditor (2012), *available at* http://www.seattle.gov/police/OPA/Docs/Auditor/Auditor_Report_Dec_11_May_12.pdf; *see also* Review Board Policy Report, *supra,* at 8-9.

272 N.Y. Civil Liberties Union Found., Civilian Review of Policing: A Case Study Report 3 (1993), *available at,* http://www.nyclu.org/files/publications/NYCLU.CivilianReviewPolicing.CaseStudyRep.1993.pdf.

273 Samuel Walker, The New World of Police Accountability 20 (2005); *see generally* Patrick O'Hara, Why Law Enforcement Organizations Fail: Mapping the Fault Lines in Policing (2005). And as Matthew Waxman notes, "the counter-terrorism agenda may influence or disrupt systems and patterns of political accountability of local police agencies." *See* Waxman, *supra* note 27, at 378.

274 Police Assessment Res. Ctr., *supra* note 263, at 13.

275 Bobb, *supra* note 263, at 9-10.

276 *Id.* at 9.

277 *Id.*

278 *See* Howard Cohen, *Miami-Dade Commissioner Predicts 'More People Will Lose TheirJobs'*, Miami Herald, Sept. 10, 2009; Charles Rabin & Jennifer Lebovich, *Miami-Dade Mayor Proposes Sweeping Pay Cuts*, Miami Herald, July 16, 2009, at D1.

279 *Id.* at11.

280 *Id.*

281 Seattle Human Rights Comm'n, City of Seattle, Report on Police Accountability and Recommendations 5 (2012), *available at* http://www.seattle.gov/humanrights/Documents/SHRC_PoliceAcctRpt010812.pdf.

282 For example, the current iteration of New York's Civilian Complaint Review Board (CCRB) was established in 1993 because of prevalent concerns about police abuse and brutality. *See* Dennis Hevesi, *14 on Council Propose Removing Review Board from Police Dept.*, N.Y. Times, Jan. 23, 1992, *available at* http://www.nytimes.com/1992/01/23/nyregion/14-on-council-propose-removing-review-board-from-police-dept.html. The CCRB gained subpoena power, although it has never exercised this authority to obtain information from the NYPD. Previous iterations of the CCRB, which more closely resemble review and appellate models, date back to 1953. *History of the CCRB*, N.Y.C. Civilian Complaint Review Bd., http://www.nyc.gov/html/ccrb/html/history.html (last visited Dec. 19, 2012). Similarly, Portland's Independent Police Review Division replaced the Police Internal Investigations Auditing Committee in 2001 after years of persistent criticism that the Committee, established in 1982 without subpoena power, had not been successful in monitoring, reviewing, or reporting on the police internal investigation system. *See* Portland, Or., Ordinance 175652 (May 24, 2001), *available at* http://www.portlandonline.com/auditor/index.cfm?c=27072&a=8101. In Philadelphia, the Police Advisory Commission gained support in 1994 only after civil judgments and settlements against the city in police-misconduct or abuse cases exceeded $10 million a year. Jan Ransom & Phillip Lucas, *Police Advisory Commission Must Cut Through Backlog of Complaints*, Philly.com (Mar. 12, 2012), http://articles.philly.com/2012-03-12/news/31152747_1_pac-backlog-complaints/2.

283 Bobb, *supra* note 263, at 12.

284 *See* N.Y.C. Civilian Complaint Review Bd., 2011 Annual Report 18 (2012), *available at* http://www.nyc.gov/html/ccrb/pdf/ccrbann2011.pdf (finding that the NYPD declined to discipline officers in 16 percent of substantiate cases in 2011; 18 percent in 2010; 27 percent in 2009; 32 percent in 2008; and 35 percent in 2007). Even where the NYPD has sought discipline – *i.e.*, in cases where the CCRB finds there is credible evidence that an officer engaged in misconduct, the department most frequently awards the mildest form of discipline. *Id.* at 19 (finding that officers received "instructions" in 71 percent of the cases in 2011 and 74 percent in 2010).

285 N.Y. City Charter § 440(c)(3).

286 *Id.* at § 440(d)(1).

287 The board reserves its subpoena power for obtaining evidence from third parties, such as medical records from a hospital or surveillance video from a business. *See The Investigative Process*, N.Y.C. Civilian Complaint Review Bd., http://www.nyc.gov/html/ccrb/html/how.html (last visited Mar. 13, 2013).

288 *See* Robert A. Perry, N.Y. Civil Liberties Union, Mission Failure: Civilian Review of Policing in New York City 1994-2006 44 (2007), *available at* http://www.nyclu.org/files/publications/nyclu_pub_mission_failure.pdf; Michael Wilson, *Top Officers Are Said to Ignore Complaint Board's Inquiry*, N.Y. Times, Sept. 15, 2005, *available at* http://www.nytimes.com/2005/09/15/nyregion/15protest.html.

289 David Noriega, *When I Tried Policing the NYPD*, Salon (Aug. 29, 2012, 2:11 PM), http://www.salon.com/2012/08/29/policing_the_police/.

290 When examining "policy" issues, the CCRB has relied on publicly available literature or its own docket of complaints rather than reviewing the NYPD's records. For example, when the CCRB examined the issue of police "stop and frisk" tactics, its report explicitly noted that it did not "describe the Police Department's stop-and-frisk practices," but rather offered "an interesting and useful picture of those individuals who filed complaints with the CCRB after being stopped by the police, the officers involved, the nature of those encounters, and the results of the complaints." Civilian Complaint Review Bd., Street Stop Encounter Report: An Analysis of CCRB Complaints resulting from the New York Police Department's "Stop & Frisk" Practices 1 (2001), *available at* http://www.nyc.gov/html/ccrb/pdf/stop.pdf. For a list of CCRB recommendations since 1998, *see CCRB Reports*, N.Y.C. Civilian Complaint Review Bd., http://www.nyc.gov/html/ccrb/html/reports.html (last visited Mar. 13, 2013).

291 Perry, *supra* note 288, at 7; *see also* David Noriega, *The Thin Blue Lie*, The New Inquiry (Aug. 29, 2012), http://thenewinquiry.com/essays/the-thin-blue-lie/.

292 These are: the Chicago Police Department (Independent Police Review Authority); the Detroit Police Department (Board of Police Commissioners); the Los Angeles Police Department (Police Commission); the Los Angeles Sheriff's Department (Office of Independent Review); the Metropolitan Police Department of Washington, DC (Office of Police Complaints); the Miami Police Department (Civilian Investigative Panel); the Minneapolis Police Department (Civilian Police Review Authority); the New York City Police Department (Civilian Complaint Review Board); the Philadelphia Police Department (Police Advisory Commission); the Portland Police Bureau (Independent Police Review Division); the San Francisco Police Department (Office of Citizen Complaints); and the Seattle Police Department (Office of Professional Accountability).

293 *Private Eyes: Phila. Police Department Needs More Outside Scrutiny*, Philly.com (Aug. 31, 2012) http://articles.philly.com/2012-08-31/news/33522151_1_police-oversight-police-department-police-officers. As of March 2012, the Police Advisory Commission had a backlog of 129 cases as old as 2008. And since its creation in 1994, it has issued just 21 recommendations to the police department in response to citizen complaints. *Id.*

294 *See* SFPD DGO 8.10, *supra* note 128.

295 Bobb, *supra* note 263, at 6.

296 *Id.* at 14.

297 *Id.*

298 Patel, *supra* note 42, at 7.

299 *Id.*

300 Indep. Comm'n on the L.A. Police Dep't, Report of the Independent Commission on the Los Angeles Police Department 171-74, 178 (1991), *available at* http://www.parc.info/client_files/Special%20Reports/1%20

-%20Chistopher%20Commision.pdf, at. In Los Angeles, the Inspector General both performs an investigative function (for example, the department's Use of Force Unit reports to the Inspector General, who is involved in the investigation and adjudication of all officer-involved shootings, head strikes, in-custody deaths, and injuries involving hospitalization), and conducts broader reviews and investigations. *See Mission Statement*, Office of the Inspector Gen., L.A. Police Dep't, http://www.oiglapd.lacity.org/isgig1.htm (last visited Mar. 13, 2013); *The Function and Role of the Board of Police Commissioners,* L.A. Police Dep't, http://www.lapdonline.org/police_commission/content_basic_view/900 (last visited Mar. 13, 2013). The office issues multiple public reports each month auditing the department's policies and performance on a wide range of issues, from use of force incidents to traffic collisions and ethics violations. *See generally Reports*, Office of the Inspector Gen., L.A. Police Dep't, http://www.oiglapd.lacity.org/isgrp1.htm (last visited Mar. 13, 2013). Unlike the LASD's Special Counsel or Seattle's Review Board, the Inspector General has the authority to conduct independent investigations into "sensitive and/or high profile matters," either at the request of the Board of Police Commissioners or the city's Public Safety Bureau. *See Mission Statement*, *supra*.

301 James G. Kolts et al., L.A. Cnty. Sheriff's Dep't, A Report 1 (1992), *available at* http://www.parc.info/client_files/Special%20Reports/3%20-%20Kolts%20Report%20-%20LASD.pdf. The LASD Special Counsel is a good example of the evaluative and performance-based model. The Special Counsel is a lawyer retained by the Los Angeles County Board of Supervisors. Armed with "unfettered access" to all relevant persons, documents and records, the Special Counsel creates public reports that address excessive force and integrity issues on an agency – rather than individual case – level. Bobb, *supra* note 263, at 13. The aim is to "foster a constructive, problem-solving dialog" that aims to "eliminate excessive or unnecessary lethal or non-lethal force" and reduce legal liability for the Sheriff's Department. *Id.*

302 The Board of Supervisors initially selected James Kolts for the purpose of conducting an inquiry and making recommendations for reform. The Kolts Commission, like the Christopher Commission, found that the LASD had "too many officers who have resorted to unnecessary and excessive force," had "not done an adequate job of disciplining them," and had "not dealt adequately with those that supervise them." Kolts et al., *supra* note 301, at 4. Kolts issued a host of recommendations for reform, including calls for "responsible review" of citizen complaints and greater accountability throughout the chain of command. *Id.* The Board of Supervisors responded by making the role of special counsel a permanent arm of the Board. Merrick Bobb, a nationally renowned expert in police oversight and member of the Kolts Commission, became the first such Special Counsel in 1993 and continues to serve in that capacity. Merrick J. Bobb et al., L.A. Cnty. Sheriff's Dep't, 1st Semiannual Report 1 (1993), *available at* http://parc.info/client_files/LASD/1st%20Semiannual%20Report.pdf.

303 Christina Villacorte, *L.A. County screening candidates for sheriff's inspector general job*, L.A. Daily News (April 10, 2013), http://www.dailynews.com/ci_22999138/l-county-screening-candidates-sheriffs-inspector-general-job.

304 Steve Miletich, *ACLU Calls for Police-Policy Reform – Report Urges New Plan For Internal Investigations*, Seattle Times, June 13, 1999, *available at* http://community.seattletimes.nwsource.com/archive/?date=19990613&slug=2966270.

305 Editorial, *Panel Report Outlines Course For Seattle Police*, Seattle Times, Aug. 23, 1999, *available at* http://community.seattletimes.nwsource.com/archive/?date=19990823&slug=2978810; Steve Miletich & Mike Carter, *Report's In: Next Move Is Up to Schell, Stamper – Panel Wants Civilian to Oversee Investigations of Police*, Seattle Times, Aug. 20, 1999, *available at* http://community.seattletimes.nwsource.com/archive/?date=19990820&slug=2978330; Alan Snel & Kimberly A.C. Wilson, *Citizen Oversight of Police Called For – Report Finds Huge Flaws In Internal Investigations*, Seattle-Post Intelligencer, Aug. 20, 1999, at A1. By 2000, the City Council had created the Office of Professional Accountability (based on investigative and quality assurance models), the Office of Professional Accountability Auditor (serving a review and appellate function), and the Office of Professional Accountability Review Board (following evaluative and performance-based models). *See* Seattle, Wash., Ordinance 119,805 (Dec. 21, 1999) (establishing OPA Director); Seattle, Wash., Ordinance 119,816 (Dec. 21, 1999) (creating OPA); Seattle, Wash., Ordinance 119,893 (Mar. 23, 2000) (setting forth duties of OPARB Internal Investigations Auditor); Seattle, Wash., Ordinance 120,728 (Feb. 22, 2002) (further modifying the OPARB).

306 Walker, *supra* note 273, at 136.

307 *Id.*

308 Seattle Human Rights Commission, *supra* note 281, at 6.

309 *Id.* The Seattle Human Rights Commission recently called for legislation authorizing the Review Board to independently investigate claims of police misconduct and function as an "appellate review panel of SPD

disciplinary cases involving allegations of police misconduct, force-related incidents, and biased policing." Seattle Human Rights Commission, *supra* note 281, at 8; *see also* Office of Professional Accountability Review Bd., Transparency, Accountability, Effectiveness and Independence: Recommendations Regarding Civilian Oversight of the Seattle Police Department 4 (2012), *available at* http://www.seattle.gov/council/OPARB/reports/2012oparb_recommendations.pdf. The recommendation follows a 2011 Justice Department investigation that found "a pattern or practice of constitutional violations regarding the use of force that result from structural problems, as well as serious concerns about biased policing." Civil Rights Div., Dep't of Justice, & U.S. Attorney's Office for the W. Dist. Of Wash., Investigation of the Seattle Police Department 2 (2011), *available at* http://www.justice.gov/crt/about/spl/documents/spd_findletter_12-16-11.pdf. In addition to problems with training and supervision, the DOJ report faulted the Office of Professional Accountability for outsourcing investigations to precinct supervisors. *Id.* at 5. "Indeed, none of the uses of force our review finds to be excessive were referred to OPA for its review." *Id.* Nonetheless, the DOJ found that "the structure of OPA is sound, and the investigations OPA itself conducts generally are thorough." *Id.* A subsequent federal lawsuit and consent decree, approved in July 2012, reiterated the Justice Department's assessment of OPA but also implemented strict reporting requirements for use of force incidents and created a Community Police Commission to serve as an advisory board. *See* Settlement Agreement & Stipulated [Proposed] Order of Resolution at ¶¶ 3-12, 91-118, 164, United States v. City of Seattle, No. 12-CV-1282 (W.D. Wash. Jul. 27, 2012), *available at* http://www.justice.gov/crt/about/spl/documents/spd_consentdecree_7-27-12.pdf (entered with modifications by Stipulation and Order for Modification and For Entry of Preliminary Approval of the Parties' Settlement Agreement and Stipulated Order of Resolution, United States v. City of Seattle, No. 12-CV-1282 (W.D. Wash. Sept. 21, 2012), *available at* http://www.justice.gov/crt/about/spl/documents/spd_orderapprovingsettlement_9-21-12.pdf).

310 Procedures and Tactics Publication, *supra* note 128, at 11, 15-16 (implementing Seattle, Wash., Ordinance No. 108333). The most recent audit revealed no violations of the law. *See* Letter from John Diaz, Chief, Seattle Police Dep't, to Mayor Michael Patrick McGinn (May 19, 2011) [hereinafter May 2011 Audit Letter], *available at* http://clerk.seattle.gov/~CFS/CF_311606.pdf.

311 Procedures and Tactics Publication, *supra* note 128, at 16.

312 *Id.* at 16-17.

313 Office of the Inspector Gen., L.A. Police Comm'n, Anti-Terrorism Intelligence section Audit, Fiscal Year 2009-2010 (2012) [hereinafter "LA OIG Report 2009-2010"], *available at* http://www.oiglapd.lacity.org/Reports/ATIS_FY09-10_1-19-12.pdf; Office of the Inspector Gen., L.A. Police Comm'n, Anti-Terrorism Intelligence section Audit, Fiscal Year 2008-2009 (2009), *available at* http://www.oiglapd.lacity.org/Reports/A-T_IntellSecfy08-09_4-9-09.pdf; Office of the Inspector Gen., L.A. Police Comm'n, Anti-Terrorism Intelligence section Audit, Fiscal Year 2006-2007 (2007), *available at* http://www.oiglapd.lacity.org/Reports/ATIS_phase1_3-6-07.pdf.

314 LA OIG Report 2009-2010, *supra* note 313, at 5-7. These audits did not address the LAPD's controversial use of suspicious activity reporting or its relationship with regional and statewide fusion centers. However, a Special Order issued by Chief Charlie Beck in August 2012 now directs the Inspector General to conduct an annual audit of LAPD's SAR program. *See* L.A. Police Dep't, Special Order No.__: Reporting Suspicious Activity Potentially Related to Foreign or Domestic Terrorism – Revised; And Suspicious Activity Report Notebook Divider, Form 18.30.03 – Revised 1 (Aug. 16, 2012) [hereinafter Beck Special Order], *available at* http://www.lapdpolicecom.lacity.org/082812/BPC_12-0358.pdf.

315 *See generally* LAPD SAR Audit, *supra* note 137.

316 *Id.* at 5-7; *see also* Stop LAPD Spying Coalition, To Observe and to Suspect: A People's Audit of the Los Angeles Police Department's Special Order 1 at 1-2 (2013), *available at* http://stoplapdspying.org/wp-content/uploads/2013/03/PEOPLES-AUDIT-FINAL.pdf.

317 In addition to San Francisco, Los Angeles, Washington, D.C., and Seattle, the Chicago Police Department has conducted intelligence audits pursuant to a 1982 consent decree. It required the Chicago Police Commission to hire an independent auditor every five years. *See* Alliance to End Repression, 561 F. Supp. at 569. But since the decree was dissolved in 2009, the department has not established independent audit procedures for investigation of First Amendment conduct.

318 *See* Yolanda Branch, Office of the D.C. Auditor, Audit of the Metropolitan Police Department's

Investigations and Preliminary Inquiries Involving First Amendment Activities (2012), *available at* http://dcauditor.org/sites/default/files/DCA232012.pdf. Despite its title, this audit contains no data on the use of preliminary inquiries. This is particularly troubling for three reasons. First, the number of reported "investigations" based on reasonable suspicion between 2005 and 2011 was extremely low (27), suggesting that the police may be relying instead on "preliminary inquiries" as the preferred mechanism for information gathering. *Id.* at13. Second, the audit found that officers had not received any training on conducting preliminary inquiries. *Id.* at 18. And third, the audit recognized that the department has no standard operating procedures for preliminary inquiries. *Id.* at 19.

319 Procedures and Tactics Publication, *supra* note 128, at 15-16.

320 *See, e.g.,* David Boerner, Police Intelligence Auditor, Report of Police Intelligence Audit Pursuant to Seattle Municipal Code 14.12 (Feb. 22, 2011), *available at* http://clerk.seattle.gov/~CFS/CF_311543.pdf; David Boerner, Police Intelligence Auditor, Report of Police Intelligence Audit Pursuant to Seattle Municipal Code 14.12 (Aug. 22, 2011), *available at* http://clerk.seattle.gov/~CFS/CF_311750.pdf; David Boerner, Police Intelligence Auditor, Report of Police Intelligence Audit Pursuant to Seattle Municipal Code 14.12 (Jan. 10, 2012), *available at* http://clerk.seattle.gov/~public/meetingrecords/2012/pscrt20120404_2a.pdf; David Boerner, Police Intelligence Auditor, Report of Police Intelligence Audit Pursuant to Seattle Municipal C ode 14.12 (Dec. 13, 2012), *available at* http://clerk.ci.seattle.wa.us/~CFS/CF_312732.pdf.

321 Alliance to End Repression, 561 F.Supp. at 569.

322 *See* Faiza Patel & Andrew Sullivan, Brennan Ctr. for Justice, A Proposal for an NYPD Inspector General 3-4 (2012), *available at* http://www.brennancenter.org/publication/proposal-nypd-inspector-general.

323 ISE Annual Report, *supra* note 17, at 90.

324 **New York:** Oversight of the New York State Intelligence Center (NYSIC) rests with the NYSCI director, a captain in the New York State Police. N.Y. State Intelligence Ctr., Information and Intelligence Privacy Policy 4 (2010), *available at* http://www.nfcausa.org/files/DDF/NYSIC%2bPRIVACY%2bPOLICY-FINAL%2bDRAFT-10182010.pdf. The privacy policy states that "NYSIC will conduct periodic audit and inspection of the information contained in its ISE-SAR shared space." *Id.* at 38. The audits may be conducted by either an independent auditor or NYSIC staff. *Id.* As of March 2013, NYSIC officials had not conducted any such audit, but told the Brennan Center that they planned to do so in the future. NYSIC officials also said they hope to partner with another fusion center and conduct reciprocal audits.

Chicago: The regional Crime Prevention and Information Center (CPIC) in Chicago is led by a commander in the Chicago Police Department. The CPIC commander appoints a privacy officer "to assist in enforcing the provisions of [the privacy policy] and who, in addition to other responsibilities, will receive reports regarding alleged errors and violations of the provisions of this policy." Chi. Police Dep't's Crime Prevention Info. Ctr., ISE-SAR Evaluation Environment Initiative Privacy, Civil Rights, and Civil Liberties Protection Policy 2 (n.d.), *available at* http://www.aclu-il.org/wp-content/uploads/2012/08/ACLU-letter-to-CPD-of-12-11-re-CPIC.pdf. The privacy policy states that "CPIC will conduct periodic audit and inspection of the information contained in its ISE-SAR shared space." However, the audits may be conducted by independent auditor or CPIC staff. *Id.* at 9. The Brennan Center is unaware of any independent audits conducted by CPIC. The Illinois State Police operate the Statewide Terrorism & Intelligence Center (STIC). The state police are responsible for "monitoring the use of all STIC data sources to guard against inappropriate or unauthorized use"; "investigat[ing] misuse of STIC data and conduct[ing] or coordinat[ing] audits concerning the proper use and security of STIC data by users." *See* Statewide Terrorism & Intelligence Center, Ill. State Police, Privacy Police 22 (2010), *available at* http://www.aclu-il.org/wp-content/uploads/2012/08/STIC-Privacy-Policy-4-10-searchable.pdf. STIC's privacy officer is a lieutenant with the Illinois State Police and there is no provision for independent audits. *Id.* at 20 n.21.

Los Angeles, LA County, and San Francisco: The California state fusion center and all regional components, including those in Los Angeles and San Francisco, all operate under a single privacy policy. Cal. State Terrorism Threat Assessment Ctr., Information Privacy Policy 1 (n.d.), *available at* http://www.nfcausa.org/files/DDF/CaliforniaSTTASPrivacyPolicy1.pdf. Each fusion center designates a "privacy official" who is responsible for "handling reported errors and violations and, in accordance with specific direction and authorization" and serves as "the focal point for ensuring that the center adheres to this policy and the provisions of the Information Sharing

Environment Privacy Guidelines." *Id.* at 17. The privacy policy states that "STTAS Components will periodically conduct audits and inspections of the information contained in its information systems." *Id.* at 15. However, the audits may be conducted by either "a designated representative of the agency or by a designated independent party." *Id.* The Brennan Center is unaware of any independent audit examining the records of any fusion center in California. However, the Northern California Regional Intelligence Center told the Brennan Center that it plans to partner with another STTAS component to conduct reciprocal audits. Such reciprocal audits are a step toward independent oversight, but still miss the mark.

Philadelphia: The Delaware Valley Intelligence Center (DVIC) is a regional fusion center serving the Philadelphia area. The DVIC director appoints a privacy officer who is responsible for receiving reports and coordinating complaint resolution regarding alleged errors or violations with a privacy policy committee. Del. Valley Intelligence Ctr., *supra* note 128, at 4. The privacy policy requires annual audits of the information and intelligence retained by DVIC, but such audits may be conducted by either an independent party or a representative of DVIC. *Id.* at 16. The Brennan Center is unaware of any independent audit conducted by DVIC. Some reports have incorrectly indicated that the DVIC is still under construction and does not yet exist. *See, e.g.,* David Henry, *Is Philly's Anti-Terrorism Center a Waste of Your Money*, WPVI-TV (Nov. 19, 2012), http://abclocal.go.com/wpvi/story?section=news/special_reports&id=8891872. In reality, the center currently exists as a small office staffed 12 hours a day by one federal agent and 12 to 20 officers from the Philadelphia Police Department's Homeland Security Unit. Jonathan Tamari, *Federal Report Cites Unfinished Philadelphia Counterterrorism Center as Flawed*, Phila. Inquirer, Oct. 5, 2012, *available at* http://articles.philly.com/2012-10-05/news/34261225_1_regional-intelligence-center-federal-money-fusion-centers. DVIC is in the process of renovating a new 40,000-square-foot facility, which has been under construction since 2006 and has cost $2.3 million in federal funds. *Id.* The state level fusion center, known as the "Pennsylvania Criminal Intelligence Center" (PaCIC), has a designated privacy officer who is also the Analytical Intelligence Section Commander. Pa. Criminal Intelligence Ctr., Pa. State Police, Privacy Policy 14 (n.d.), *available at* http://www.nfcausa.org/files/DDF/PennsylvaniaPaCICApprovedPrivacyPolicy02-11_3.pdf. The privacy officer also leads a Privacy Policy Committee, which is responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system, among other things. *Id.* The privacy policy requires periodic audits to assess compliance with the policy and applicable law, conducted by fusion center staff under the direction of the privacy officer. *Id.* at 15. It also requires periodic audits of the "information contained in the justice information system" to be conducted by a designated independent party or a representative of the Pennsylvania State Police. *Id.* at 16. It is unclear whether such audits have ever been conducted.

Houston: The Houston Police Department operates the Houston Regional Intelligence Service Center Hous. Reg'l Intelligence Serv. Ctr., Privacy Policy: Privacy, Civil Rights, and Civil Liberties Policy 3 (2009), *available at* http://www.nfcausa.org/files/DDF/Privacy%20Policy%20HRISC%20September%2009%20SSNP%20.pdf; *see also* Hous. Police Dep't, FY2012 Core Services Assessment 20-22 (2011) *available at* http://www.houstontx.gov/council//1/csad/hpd-csa.pdf. A police sergeant is responsible for overseeing compliance with the center's privacy policy and responding to public complaints concerning privacy civil rights, and civil liberties violations. Hous. Reg'l Intelligence Serv. Ctr., *supra*, at 5. And the Houston Police Department is responsible for conducting compliance audits according to departmental procedure. *Id.* at 10. The Texas Department of Public Safety operates the state's primary fusion center, the Texas Fusion Center. The state privacy policy requires annual audits of fusion center records, but that responsibility falls to a privacy officer appointed by the general counsel for the Department of Public Safety. Tx. Fusion Ctr., Privacy, Civil Right, and Civil Liberties Policy 2, 15 (2010), *available at* http://www.dps.texas.gov/docs/TxFCPrivacyPolicy113010.pdf. The privacy officer is an attorney from the Department of Public Safety. *Id.* at 2. A 2011 state law created a "Fusion Center Policy Council" within the Texas Department of Public Safety, designed to assist the state in monitoring the activities of all fusion centers in Texas. Tex. Gov't Code Ann. § 421.083 (West 2013). The Council, however, is composed entirely of representatives from the fusion centers. *Id.*

Washington, D.C.: The Washington Regional Threat & Analysis Center (WRTAC) is the regional fusion center for Washington, D.C.. An executive board of directors is responsible for appointing a privacy officer whose duties include receiving reports and coordinating complaint resolution regarding alleged errors or violations of the center's privacy policy. Wash. Regional Threat and Analysis Ctr., *supra* note 128, at 2. The privacy policy requires annual audits of the information and intelligence maintained by WRTAC, and commendably, it specifies that the audit "will be conducted by a designated independent panel." *Id.* at 19.

Miami & Miami-Dade: The director of the Southeast Florida Fusion Center (SEFFC), part of the Miami-Dade Police Department, appoints a privacy officer to assist in enforcing the privacy policy and receive reports regarding

alleged errors and violations. Se. Fla. Fusion Ctr. *supra* note 128. An intelligence analyst supervisor or police sergeant at SEFFC is responsible for conducting periodic audits of the information contained in the center's ISE-SAR shared space. *Id.* at 10. With respect to the state-run Florida Fusion Center, the general counsel for the Florida state police serves as the privacy officer. Fla. Fusion Ctr., *supra* note 128, at 15. Responsibility for periodic audits, however, falls to an inspector general. *Id.* at 6. The inspector general is "organizationally aligned" with the police, but must transmit all final reports to an independent auditor general. *See Office of Inspector General*, Fla. Dep't of Law Enforcement, www.fdle.state.fl.us/oig/ (last visited Mar. 14, 2013); Fla. Stat. Ann. § 20.055(5)(f) (2011). The Florida Fusion Center also has a "Constitutional Protections and Privacy Advisory Board," although it is unclear whether it is active or who its members are. In theory, it "collaborates with community privacy advocacy groups" and is "comprised of three members not actively associated or employed by the [Florida Fusion Center]." Fla. Fusion Ctr., *supra* note 128, at 5. It is empowered to periodically review fusion center policies for protecting civil rights and civil liberties and to make recommendations to the fusion center's Executive Advisory Board. *Id.* In addition, the Board "may be consulted" in "any independent inquiry into complaints" alleging a violation of the privacy policy and offer "recommended corrective action." *Id.* at 6.

Detroit & Dearborn: The Detroit and Southeast Michigan Information and Intelligence Center (DSEMIIC) is a component of the Detroit Police Department. In addition to the City of Detroit, it includes representatives from surrounding Macomb, Monroe, Oakland, St. Clair, Washtenaw and Wayne Counties. Oakland Cnty. Bd. of Comm'rs, Minutes 116 (Feb. 16, 2012), *available at* https://www.oakgov.com/boc/Documents/minutes/12_min/12_02_16.pdf; *see generally The State of Northern Border Preparedness: A Review of Federal, State, and Local Coordination: Hearing Before the H. Comm. on Homeland Sec., Subcomm. On Emergency Preparedness, Response, & Commc'ns* (statement of Captain W. Thomas Sands, Deputy State Director, Emergency Management and Homeland Security, Michigan State Policy, Emergency Management and Homeland Security Division), *available at* http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Sands.pdf. DSEMIIC is a node for the state's primary fusion center, the Michigan Intelligence Operations Center (MIOC). The MIOC privacy policy applies to all nodes, including DSEMIIC. Mich. Intelligence Operations Ctr., MIOC Privacy Policy 1 (2011), *available at* https://www.michigan.gov/documents/msp/MIOCprivacypolicy_355596_7.pdf. The fusion centers are "guided by an agency-designated privacy committee that liaises with community privacy advocacy groups to ensure that privacy and civil rights are protected. ..." *Id.* at 2-3. The fusion center director appoints a privacy officer who leads the privacy committee and handles reports regarding alleged errors and violations of the provision of the privacy policy. *Id.* at 3; *see also* Detroit & Se. Mich. Info. Ctr., Draft Privacy Policy 5 (n.d.), *available at* http://www.nfcausa.org/files/DDF/DetroitPrivacyPolicy.pdf (establishing an advisory board led by an appointed privacy officer). The MIOC privacy policy states that "an independent entity designated by the Director of the [Michigan State Police]" will conduct an annual audit of the information contained in MIOC's criminal intelligence system. Mich. Intelligence Operations Ctr., *supra*, at 12; Detroit & Se. Mich. Info. Ctr., *supra*, at 15 (requiring an "independent panel" to conduct annual audits). In practice, however, it is unclear if either fusion center has actually conducted such an audit.

Seattle: The Washington State Fusion Center (WSFC) has an executive board that is responsible for "ensuring that audit and oversight mechanisms are in place to ensure compliance" with the fusion center privacy policy. Wash. State Fusion Ctr., Privacy Policy 2 (2009), *available at* http://www.nfcausa.org/files/DDF/WSFCPrivacyPolicy.pdf. The executive board is comprised of fusion center participants, including: the Washington State Patrol Chief, the FBI Seattle Field Division Special Agent-In-Charge, the Seattle Police Department Chief, the King County Sheriff, the U.S. Attorney for the Western Washington District, the U.S. Attorney for the Eastern Washington District, the Washington State Homeland Security Advisor, and two representatives from the Washington Association of Sheriffs and Police Chiefs. DHS-DOJ Fusion Process Technical Assistance Program & Servs., Washington State Fusion Center and the Pacific Northwest Region: Building a Critical Infrastructure / Key Resource Information Sharing Capability 1 (2009), *available at* http://www.regionalresilience.org/Portals/0/reports%20and%20AARs/DHS-DOJ%20Fusion%20Center%20Background.pdf. The executive board must "ensure that an annual audit is conducted to review compliance with WSFC information systems requirements and the WSFC Privacy Policy," although there is no public record of such audits being conducted. *See* Wash. State Fusion Ctr., *supra*, at 6.

Portland: The Oregon Terrorism Information Threat Assessment Network is a state-level fusion center. Its designated privacy officer is an attorney for the fusion center who is appointed by the Chief Counsel of the Oregon Department of Justice Criminal Division. Or. Terrorism Info. Threat Assessment Network, Privacy Policy 2 (2011), *available at* http://www.nfcausa.org/files/DDF/OR%20TITAN%20Fusion%20Center%20Privacy%20Policy_FINAL_17FEB2011.pdf. He or she "receives reports regarding alleged errors and violations of the provisions

of the policy, receives and coordinates complaint resolution under the Center's redress policy, and serves as the liaison for the Information Sharing Environment, ensuring that privacy protections are implemented …." *Id.* The privacy policy requires audits, but not independent audits. *Id.* at 18 ("The Oregon TITAN Fusion Center will adopt and follow procedures and practices to ensure and evaluate the compliance of its users and the system itself with the provisions of this Privacy Policy and applicable law. This will include logging access to these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits will be mandated at least annually and a record of the audits will be maintained by the Privacy Officer or Center Director the Center."). An internal "Executive Advisory Committee" is also required to "conduct or coordinate audits and inspections of the information contained in information systems located at the Center's headquarters." *Id.* at 19. The Brennan Center was unable to locate any record of such audits.

Minneapolis & St. Paul: The Minnesota Joint Analysis Center (MNJAC) is a state-level fusion center. It has a privacy officer that is a member of the MNJAC staff as well as a Privacy Policy Committee tasked with ensuring the protection of privacy and civil rights. Minn. Joint Analysis Ctr., Privacy Policy 6-7 (2011), *available at* https://dps.mn.gov/divisions/bca/bca-divisions/investigations/Documents/MNJAC%20Privacy%20Policy%20approved%20122011%20final.pdf. An "Oversight Group," composed of representatives from each agency participating in the fusion center, is responsible for overseeing MNJAC operations and "conducting or coordinating annual and random internal or external audits, including audits by the legislative auditor, and for investigating misuse of MNJAC's information systems." *Id.* at 23. MNJAC has taken the commendable step of contracting an independent auditor to review its operations and publish audit reports online. *See, e.g.*, John J. Wilson, Inst. for Intergovernmental Research, Data Compliance Audit Report for the Minnesota Joint Analysis Center 1 (2010), *available at* https://dps.mn.gov/divisions/bca/Documents/MNJAC%20Data%20Compliance%20Audit%20Report.pdf.

325 U.S. Gen. Accounting Office, *supra* note 256, at 10.

326 *See generally* DHS/DOJ Fusion Process Technical Assistance Program and Services, Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template 9 (2010), *available at* www.it.ojp.gov/docdownloader.aspx?ddid=1269.

327 *Id.* at 9, 28-29.

328 Internal fusion center audits are more susceptible to manipulation by individuals, especially if the audit is not independent or the results are likely to reflect negatively on a fusion center's reputation. *See* Data Privacy and Integrity Advisory Comm., U.S. Dep't of Homeland Sec., Privacy Policy Recommendations for a Federated Information-Sharing System 10 (2011), *available at* http://www.dhs.gov/xlibrary/assets/privacy/dpiacwhitepaperdhsinformationsharingpolicyconsiderations2011_draft.pdf. By contrast, a centralized, external audit process is less susceptible to manipulation, better positioned to recognize aberrations or abuses, and more effective at standardizing the interpretation of laws and policies that apply to all components. *Id.* at 11.

329 The following fusion centers have audit requirements: the New York State Intelligence Center; the Chicago Crime Prevention and Information Center; the Los Angeles Joint Regional Intelligence Center; the Northern California Regional Intelligence Center, the California State Terrorism Threat Assessment Center; the Washington Regional Threat & Analysis Center, the Delaware Valley Intelligence Center, the Pennsylvania Criminal Intelligence Center, the Houston Regional Intelligence Service Center; the Texas Fusion Center; the Southeast Florida Fusion Center; the Florida Fusion Center; the Detroit and Southeast Michigan Information and Intelligence Center; the Michigan Intelligence Operations Center; the Washington State Fusion Center; the Oregon Terrorism Information Threat Assessment Network; and the Minnesota Joint Analysis Center.

330 *Cf.* Recommendations for Fusion Centers, *supra* note 14, at 16 (recommending than "an independent auditor should review fusion center audit logs at least once every two years and issue a report describing data-security practices and any abuses or unauthorized access.").

331 *See, e.g.*, Wilson, *supra* note 324.

332 Fla. Fusion Ctr., *supra* note 128, at 4-5.

333 The Northern California Regional Intelligence Center plans to partner with another fusion center in California in order to audit each other's files. While such reciprocal audits are certainly a step in the right direction, they do not replace the need for an outside, independent auditor. It is also difficult to see how this model could be replicated when fusion centers operate under different state laws.

334 ISE Annual Report, *supra* note 17, at 12. According to DHS, such audits reduce the risk of inappropriate information sharing. Data Privacy and Integrity Advisory Comm., *supra* note 328, at 11.

335 2012 Senate HSGAC Fusion Center Report, *supra* note 8, at 36.

336 28 C.F.R. § 23.20(c) ("In an interjurisdictional intelligence system, the project is responsible for establishing the existence of reasonable suspicion of criminal activity either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.").

337 The Intelligence Reform and Protection Act of 2004, as amended, mandates that the ISE must incorporate "strong mechanisms to enhance accountability and *facilitate* oversight, including audits." Intelligence Reform and Terrorism Prevention Act, Pub. L. No. 108-458 § 1016(b)(2)(I), 118 Stat. 3638 (emphasis added). And privacy guidelines issued in 2006 require agencies participating in the ISE to implement mechanisms to *enable* an adequate audit. Major Crimes Div., *supra* note 251, at 4-5. But no federal agency has an obligation to actually *conduct* such an audit and one has never been conducted. There is also no obligation to ensure that the participating agencies have conducted their own audits. A 2012 DHS memorandum simply "presume[s]" that audits are a part of current practice before going on to weigh the pros and cons of audits performed by component agencies as opposed to a centralized function. Memorandum from Richard Purcell, Chair, U.S. Dep't of Homeland Sec. Privacy and Integrity Advisory Comm., to Janet Napolitano, Sec., U.S. Dep't of Homeland Sec., & Mary Ellen Callahan, Chief Privacy Officer, U.S. Dep't of Homeland Sec. 11-12 (Jan. 31, 2012), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_dpiac_report_2011_01.pdf.

338 Office of the Inspector Gen., U.S. Dep't of Justice, The Department of Justice's Terrorism Task Forces iv (2005), *available at* http://www.justice.gov/oig/reports/plus/e0507/final.pdf.

339 Fed. Bureau of Investigation, U.S. Dep't of Justice, Joint Terrorism Task Force: Standard Memorandum of Understanding Between the Federal Bureau of Investigation and Houston Police Department (2007) [hereinafter Houston JTTF MOU] (on file with Brennan Center).

340 The City of Detroit responded to a Brennan Center freedom of information request by stating that it "does not possess such a record," but only because it did not retain a copy: "Based on information provided by a DPD personnel [sic], although the DPD was required to sign the MOU, the Department did not retain a copy of the agreement." Letter from Ellen Ha, Senior Assistant Corp. Counsel, Governmental Affairs Section, Detroit Police Dep't, to Michael Price, Counsel, Liberty & Nat'l Sec. Program, Brennan Ctr. for Justice (Apr. 26, 2012) (on file with the Brennan Center).

341 Most police departments detail just a handful of officers to their local JTTF. In New York, however, the size of this contingent increased dramatically after 9/11, jumping from 17 to 130 officers. *Kelly May 18, 2004 Testimony*, *supra* note 54, at 4; *see also* Raymond Kelly, Comm'r, N.Y.C. Police Dep't, Address at the Council on Foreign Relations Meeting: The Post-9/11 NYPD: Where Are We Now? (Apr. 22, 2009), *available at* www.cfr.org/homeland-security/post-911-nypd-we-now/p19198. By some accounts, this was Commissioner Kelly's attempt to "pack" the JTTF with loyal officers who would feed information to the revamped Intelligence Division and give the NYPD greater control over Task Force operations. Comiskey, *supra* note 14, at 18; Craig Horowitz, *The NYPD's War on Terror*, N.Y. Mag., Feb. 3, 2003, *available at* http://nymag.com/nymetro/news/features/n_8286/index1.html ("One of Kelly's earliest moves was to pump up the number of detectives from 17 to 125, a huge commitment that the FBI matched. Kelly's intensity and his willingness to push the envelope were demonstrated early on when he tried to muscle control of the JTTF away from the FBI."). But it is not clear that Kelly's plan had the intended effect. Recent reports indicate a rift between the JTTF and the Intelligence Division, with NYPD JTTF officers "in total sync" with the FBI while Intelligence Division officials are "running their own pass patterns." E-mail to Fred Burton, V.P. of Intelligence, Stratfor Global Intelligence (Nov. 30, 2011), *available at* http://wikileaks.org/gifiles/docs/915038_re-alpha-note-feedback-fbi-nypd-tensions-highlighted-in.html.

342 *See generally* Fed. Bureau of Investigation, U,S. Dep't of Justice, Joint Terrorism Task Force Memorandum of Understanding (MOU), *available at* http://www.it.ojp.gov/fusioncenterguidelines/joint_terrorism_task_force_mou.pdf (generic JTTF MOU).

343 Or. Rev. Stat. § 181.575 (2011) (Information Not to be Collected or Maintained). By contrast, the Attorney General Guidelines governing FBI investigations do not require a criminal predicate in order to collect information about activities protected by the First Amendment. Emily Berman, *supra* note 7, at 22.

344 *See, e.g.*, Fed. Bureau of Investigation, U.S. Dep't of Justice, Joint Terrorism Task Force: Memorandum of Understanding Between the Federal Bureau of Investigation (Portland) and the Portland Police Department (2000) , *available at* http://www.portlandonline.com/shared/cfm/image.cfm?id=329922 ("[I]n situations where the statutory or common law of Oregon is more restrictive than comparable Federal law, the investigative methods employed by state and local law enforcement agencies shall conform to the requirements of such Oregon statutes or common law."); Fed. Bureau of Investigation, U.S. Dep't of Justice , Joint Terrorism Task Force: Memorandum of Understanding Between the Federal Bureau of Investigation (Portland) and the Portland Police Department (2002) (same), *available at* http://www.portlandonline.com/shared/cfm/image.cfm?id=329912.

345 *See* Am. Civil Liberties Union of Or., ACLU Backgrounder: Joining the FBI Joint Terrorism Task Force Is Still a Bad Idea 2 (2011) [hereinafter ACLU Backgrounder], *available at* http://aclu-or.org/sites/default/files/JTTF_Backgrounder_Feb_2011_0.pdf; *City of Portland Withdraws From JTTF!*, Am. Civil Liberties Union of Or. (Apr. 28, 2005), http://aclu-or.org/content/city-portland-withdraws-jttf-2005.

346 ACLU Backgrounder, *supra* note 345, at 3.

347 *City of Portland Withdraws From JTTF!*, *supra* note 345.

348 Portland, Or., Resolution Substitute 36315 (April 26, 2005), *available at* http://www.portlandonline.com/shared/cfm/image.cfm?id=329904.

349 Portland, Or., City Council Resolution 36,859 (2011), http://www.portlandonline.com/auditor/index.cfm?a=349687&c=54882. The resolution enjoyed the support of all five members of the Portland City Council, including Mayor Adams, as well as the ACLU of Oregon. Press Release, Am. Civil Liberties Union of Or., Portland City Council Passes JTTF Substitute Resolution; ACLU Supports with Reservations (Apr. 28, 2011), *available at* http://aclu-or.org/content/portland-city-council-passes-jttf-substitute-resolution-aclu-supports-reservations.

350 Portland, Or., *supra* note 349.

351 *Id.*

352 *Id.*

353 *Id.* A copy of the Resolution is included with the Standard Operating Procedure used by the Criminal Intelligence Unit of the PPB when working with the JTTF. Portland Police Bureau, *supra* note 80, at 4-7.

354 City and Cnty. of S.F. Human Rights Comm'n, Community Concerns of Surveillance, Racial and Religious Profiling of Arab, Middle Easter, Muslim, and South Asian Communities and Potential Reactivation of SFPD Intelligence Gathering 16 (2011), *available at* http://www.safesf.org/wp-content/uploads/2012/02/SF-Human-Rights-Commission-Report-Community-Concerns-of-Surveillance-Racial-and-Religious-Profiling-of-Arab-Middle-Eastern-Muslim-and-South-Asian-Communities-and-Potential-Reactivation-of-SFPD-Intelligence-Gathering1.pdf.

355 *Id.*; SFPD DGO 8.10, *supra* note 128 at 1, 3.

356 S.F., Cal., Ordinance 120046 § 1(g) (Jan. 9, 2012) (proposed), *available at* http://www.safesf.org/wp-content/uploads/2012/02/Proposed-Safe-SF-Civil-Rights-Ordinance.pdf.

357 S.F., Cal., Admin. Code § 2A.74 (2012), *available at* http://www.amlegal.com/nxt/gateway.dll/California/administrative/chapter2aexecutivebranch?f=templates$fn=default.htm$3.0$vid=amlegal:sanfrancisco_ca$anc=JD_2A.74. The Board of Supervisors initially approved a much stronger version of the ordinance. *See* S.F., Cal., *supra* note 356. But Mayor Ed Lee vetoed the legislation. Steven T. Jones, *Lee Veto Protects the SFPD's Ability to Spy on You*, S.F. Bay Guardian (Apr. 11, 2012), http://www.sfbg.com/politics/2012/04/11/lee-veto-protects-sfpds-ability-spy-you.

358 S.F., Cal., *supra* note 357; Steven T. Jones, *Mayor Lee Signs Watered-Down Limits on SFPD Spying*, S.F. Bay Guardian (May 9, 2012, 4:56 PM), http://www.sfbg.com/politics/2012/05/09/mayor-lee-signs-watered-down-limits-sfpd-spying. SFPD Chief Greg Suhr presented the first public report in January 2013, but it was roundly criticized for its lack of detail. Steven T. Jones, *Activists Slam Hollow Report of SFPD-FBI Spying*, S.F. Bay Guardian (Jan. 31, 2013, 4:33 PM), http://www.sfbg.com/politics/2013/01/31/activists-slam-hollow-report-sfpd-fbi-spying. Suhr then issued an apology for the sparse report and pledged to work with activists to develop a more detailed report. Steven T. Jones, *Suhr Apologizes for Sparse Spying Report, Pledges More Info*, S.F. Bay Guardian (Feb. 1, 2013, 5:54 PM), http://www.sfbg.com/politics/2013/02/01/suhr-apologizes-sparse-spying-report-pledges-more-info.

359 In addition to Portland and San Francisco, Miami-Dade may be the only other jurisdiction in the Brennan Center survey with a policy requiring officers assigned to the local JTTF to comply with local rules. However, the Brennan Center was unable to verify this information. In response to an open records request, the Miami-Dade Police Department stated that FBI requirements prevented it from releasing a copy of its memorandum with the JTTF. At the same time, the department issued a written response stating that "MDPD Task Force Officers must not, in the course of their assignments, violate any of the policies set forth by the MDPD's Departmental Manual." Letter from Glen Stoltzenberg, Major, Miami-Dade Police Dep't, to R. Kyle Alagood, Brennan Ctr. for Justice (May 24, 2012) (on file with the Brennan Center).

360 In Houston, a memorandum in effect since 2007 cites the FBI guidelines as a "controlling document" with only a caveat that any conflict with state or local law "will be jointly resolved." Houston JTTF MOU, *supra* note 339. This leaves Houston officers assigned to the JTTF with little practical guidance. By comparison, a previous memo from 1993 clearly stated that "personnel of the HPD shall be required to utilize only those investigative techniques consistent with their given standards and procedures." Hous. Counterterrorism Task Force, Memorandum of Understanding 1 (1993) (on file with the Brennan Center). It also mandated that "[t]o the extent that HPD standards and procedures impose any greater restrictions upon the use for their informants and cooperating witnesses, such personnel shall be bound by those restrictions." *Id.* at 4-5. Police in Chicago, Philadelphia, Washington, D.C., and Minneapolis all operate under language identical to the 2007 San Francisco MOU. The St. Paul Police Department adheres to an MOU that is even less specific, although the department was in the process of negotiating a new agreement as of March 2012. The existing MOU states any "[p]roblems or difficulties which may arise" will be "mutually addressed…at the lowest possible administrative level." Minneapolis Joint Terrorism Task Force, Memorandum of Understanding 1-2 (n.d.) (on file with the Brennan Center). And the Los Angeles Police Department permits officers assigned to a multi-agency task force to engage in the investigative methods authorized for the agency heading that task force, "as long as those methods do not violate current laws." Intradepartmental Correspondence from Charlie Beck, Chief, L.A. Police Dep't, to the Honorable Board of Police Comm'rs, Amendment to Major Crimes Division Standards and Procedures 15 (Mar. 17, 2010) (on file with the Brennan Center). Without additional guidance, there remains a risk that local officers will be unsure of which set of current laws they must follow.

STAY CONNECTED TO THE BRENNAN CENTER

Visit our website at **www.brennancenter.org.**
Sign up for our electronic newsletters at **www.brennancenter.org/signup.**

Latest News | Up-to-the-minute info on our work, publications, events, and more.

Voting Newsletter | Latest developments, state updates, new research, and media roundup.

Justice Update | Snapshot of our justice work and latest developments in the field.

Fair Courts | Comprehensive news roundup spotlighting judges and the courts.

Twitter | www.twitter.com/BrennanCenter
Facebook | www.facebook.com/BrennanCenter

NEW AND FORTHCOMING BRENNAN CENTER PUBLICATIONS

What the Government Does with Americans' Data
Rachel Levinson-Waldman

Foreign Law Bans: Legal Uncertainties and Practical Problems
Faiza Patel, Amos Toh, and Matthew Duss

A Proposal for an NYPD Inspector General
Faiza Patel and Andrew Sullivan

Domestic Intelligence: Our Rights and Our Safety
Faiza Patel, editor

Reforming Funding to Reduce Mass Incarceration
Inimai Chettiar, Lauren-Brooke Eisen, and Nicole Fortier

Early Voting: What Works
Diana Kasdan

Federal Judicial Vacancies: The Trial Courts
Alicia Bannon

The Case for Voter Registration Modernization
Brennan Center for Justice

How to Fix Long Lines
Lawrence Norden

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

BRENNAN
CENTER
FOR JUSTICE

at New York University School of Law

161 Avenue of the Americas
12th Floor
New York, NY 10013
646-292-8310
www.brennancenter.org