Recommendations for Fusion Centers

PRESERVING PRIVACY & CIVIL LIBERTIES while PROTECTING AGAINST CRIME & TERRORISM

The CONSTITUTION PROJECT

RECOMMENDATIONS FOR FUSION CENTERS

PRESERVING PRIVACY AND CIVIL LIBERTIES while PROTECTING AGAINST CRIME AND TERRORISM

The CONSTITUTION PROJECT

THE CONSTITUTION PROJECT

Safeguarding Liberty, Justice & the Rule of Law

Created out of the belief that we must cast aside the labels that divide us in order to keep our democracy strong, The Constitution Project (TCP) brings together policy experts and legal practitioners from across the political spectrum to foster consensus-based solutions to the most difficult constitutional challenges of our time. TCP seeks to reform the nation's broken criminal justice system and to strengthen the rule of law through scholarship, advocacy, policy reform and public education initiatives. Established in 1997, TCP is based in Washington, D.C.

The Constitution Project
1200 18th Street, NW
Suite 1000
Washington, DC 20036
Tel 202.580.6920
Fax 202.580.6929

info@constitutionproject.org

www.constitutionproject.org

TABLE OF CONTENTS

PREFACE

The Constitution Project (TCP) is a national, bipartisan think tank that develops consensus-based solutions to some of the most difficult constitutional challenges of our time. Established in 1997, TCP is renowned for its ability to bring together unlikely allies—experts and practitioners from across the political spectrum—in order to promote and safeguard America's founding charter. TCP works on criminal justice and rule of law issues by undertaking scholarship, policy reform and public education initiatives. TCP's Criminal Justice Program seeks to counter a broad-based effort to deny fundamental day-in-court rights and due process protections to those accused of crimes. TCP's Rule of Law Program addresses threats to our constitutional system and our civil liberties.

In 2001, TCP launched the Rule of Law Program's bipartisan Liberty and Security Committee. The Committee brings together members of the law enforcement community, legal academics, former government officials and advocates from across the political spectrum to develop and advance proposals that protect civil liberties as well as our nation's security. The Liberty and Security Committee tackles a variety of issues including the growing threat to individual privacy as a result of rapid technological advancements.

In the aftermath of the September 11 attacks, the government created a network of state and regionally-based fusion centers to detect and defend against potential terrorist threats. Fusion centers are information-sharing hubs that facilitate the exchange of critical information among federal and state law enforcement, intelligence agencies, and sometimes even military officials and private sector entities. Fusion centers have the potential to dramatically strengthen the nation's law enforcement and counterterrorism efforts. However, without effective limits on data collection, storage and use, fusion centers can pose serious risks to civil liberties, including rights of free speech, free assembly, freedom of religion, racial and religious equality, privacy and the right to be free from unnecessary government intrusion.

This report contains six parts. In parts I and II, the report introduces the subject and provides an overview of the structure of fusion centers and the institutional framework within which they operate. In part III, the report highlights civil liberties concerns raised by fusion center data collection. Some fusion centers' policies and training programs have enabled racial, religious and political profiling, and their collection of information for "suspicious activity" reports has threatened constitutional rights of privacy. Part IV outlines and critiques fusion centers' procedures regarding data storage and use. The report explains how fusion centers should rely upon the Fair Information Practice Principles that form the basis for the Privacy Act of 1974 to develop proper safeguards for personally identifiable information, such as through data minimization, use limitations, and audit logs, as well as policies strictly regulating the use of data mining and private sector partnerships. Part V addresses the lack of adequate accountability and redress mechanisms within fusion centers and the need for government transparency. Finally, in part VI, the report offers a set of recommendations to ensure that fusion centers operate effectively while respecting civil liberties and constitutional values. These recommendations include specific limits on collection, storage and use of data, as well as state and federal oversight.

The Constitution Project sincerely thanks the team of attorneys at Latham & Watkins LLP—Daniel Adams, Kevin M. McDonough, Tyler U. Nims, Shervin Rezaie and Miles N. Ruthberg—for their insight and invaluable work in researching and drafting this report. The Constitution Project is also grateful to The Atlantic Philanthropies, Open Society Foundations, CS Fund/Warsh-Mott Legacy, Rockefeller Brothers Fund, Wallace Global Fund, Herb Block Foundation and Bauman Foundation for their support in the creation and publication of this report.

Virginia E. Sloan, President, **Sharon Bradford Franklin**, Senior Counsel
August 2012

Members of The Constitution Project's Liberty and Security Committee Endorsing the Recommendations for Fusion Centers*

CO-CHAIRS:

David Cole, Professor of Law, Georgetown University Law Center

David A. Keene, former Chairman, American Conservative Union

MEMBERS:

Azizah al-Hibri, Professor Emerita, The T.C. Williams School of Law, University of Richmond; Chair, KARAMAH: Muslim Women Lawyers for Human Rights

Bob Barr, former Member of Congress (R-Ga.); CEO, Liberty Strategies, LLC; former 21st Century Liberties Chair for Freedom and Privacy, American Conservative Union; Chairman, Patriots to Restore Checks and Balances; practicing attorney

David E. Birenbaum, Of Counsel, Fried, Frank, Harris, Shriver & Jacobson LLP; Senior Scholar, Woodrow Wilson International Center for Scholars; U.S. Ambassador to the United Nations for U.N. Management and Reform, 1994-1996

Phillip J. Cooper, Professor, Mark O. Hatfield School of Government, Portland State University

Mickey Edwards, Vice President, Aspen Institute; Lecturer, Woodrow Wilson School of Public and International Affairs, Princeton University; former Member of Congress (R-Okla.) and Chairman of the House Republican Policy Committee

Eugene R. Fidell, Of Counsel, Feldesman Tucker Leifer Fidell LLP; Senior Research Scholar in Law and Florence Rogatz Visiting Lecturer in Law, Yale Law School

Michael German, Senior Policy Counsel, American Civil Liberties Union; Special Agent, Federal Bureau of Investigation, 1988-2004; former Adjunct Professor, National Defense University School for National Security Executive Education

Philip M. Giraldi, Contributing Editor for *The American Conservative Magazine*, antiwar.com and *Campaign for Liberty*; Executive Director, Council for the National Interest; former Operations Officer specializing in counterterrorism, Central Intelligence Agency, 1975-1992; United States Army Intelligence

Asa Hutchinson, Senior Partner, Asa Hutchinson Law Group; Undersecretary, Department of Homeland Security, 2003-2005; Administrator, Drug Enforcement Administration, 2001-2003; Member of Congress (R-Ark.), 1997-2001; United States Attorney, Western District of Arkansas,1982-1985

Kate Martin, Director, Center for National Security Studies

Mary O. McCarthy, Consultant, Freedom of Information and Privacy Act; Associate Deputy Inspector General, Investigations, Central Intelligence Agency, 2005-2006; Visiting Fellow, Center for Strategic and International Studies, 2002-2004; Senior Policy Planner, Directorate of Science and Technology, Central Intelligence Agency, 2001-2002; Senior Director, Special Assistant to the President, National Security Council, 1998-2001; Director for Intelligence Programs, National Security Council, 1996-1998; National Intelligence Officer for Warning, (Deputy 1991-1994) 1991-1996

Paul R. Pillar, Visiting Professor and Director of Studies, Security Studies Program, Georgetown University; intelligence officer (positions included Deputy Chief of DCI Counterterrorist Center, National Intelligence Officer for the Near East and South Asia, and Executive Assistant to the Director of Central Intelligence), Central Intelligence Agency and National Intelligence Council, 1977-2005

Peter Raven-Hansen, Glen Earl Weston Research Professor of Law, The George Washington University Law School; Co-Director, National Security and U.S. Foreign Relations Law Program

William S. Sessions, Partner, Holland and Knight LLP; Director, Federal Bureau of Investigation, 1987-1993; Judge, United States District Court for the Western District of Texas, 1974-1987, Chief Judge, 1980-1987; United States Attorney, Western District of Texas, 1971-1974

Neal R. Sonnett, Member, American Bar Association (ABA) Board of Governors; past Chair, ABA Task Force on Treatment of Enemy Combatants and Task Force on Domestic Surveillance in the Fight Against Terrorism; past Chair, ABA Criminal Justice Section; former Assistant United States Attorney and Chief of the Criminal Division for the Southern District of Florida

William H. Taft IV, Of Counsel, Fried, Frank, Harris, Shriver & Jacobson; Legal Advisor, Department of State, George W. Bush administration; Deputy Secretary of Defense, Reagan administration

Colby Vokey, Lieutenant Colonel USMC (Ret.); Attorney, Fitzpatrick Hagood Smith & Uhl LLP; Lieutenant Colonel, U.S. Marine Corps, 1987-2008; lead counsel for Guantanamo detainee Omar Khadr at Military Commissions, 2005-2007

John W. Whitehead, President, The Rutherford Institute

Lawrence B. Wilkerson, Colonel, U.S. Army (Ret.); Adjunct Professor of Government and Public Policy, College of William and Mary; Chief of Staff, Secretary of State Colin L. Powell, 2002-2005

REPORTERS:

Daniel Adams, Associate, Latham & Watkins LLP

Kevin M. McDonough, Senior Associate, Latham & Watkins LLP

Tyler U. Nims, Associate, Latham & Watkins LLP

Shervin Rezaie, Associate, Latham & Watkins LLP

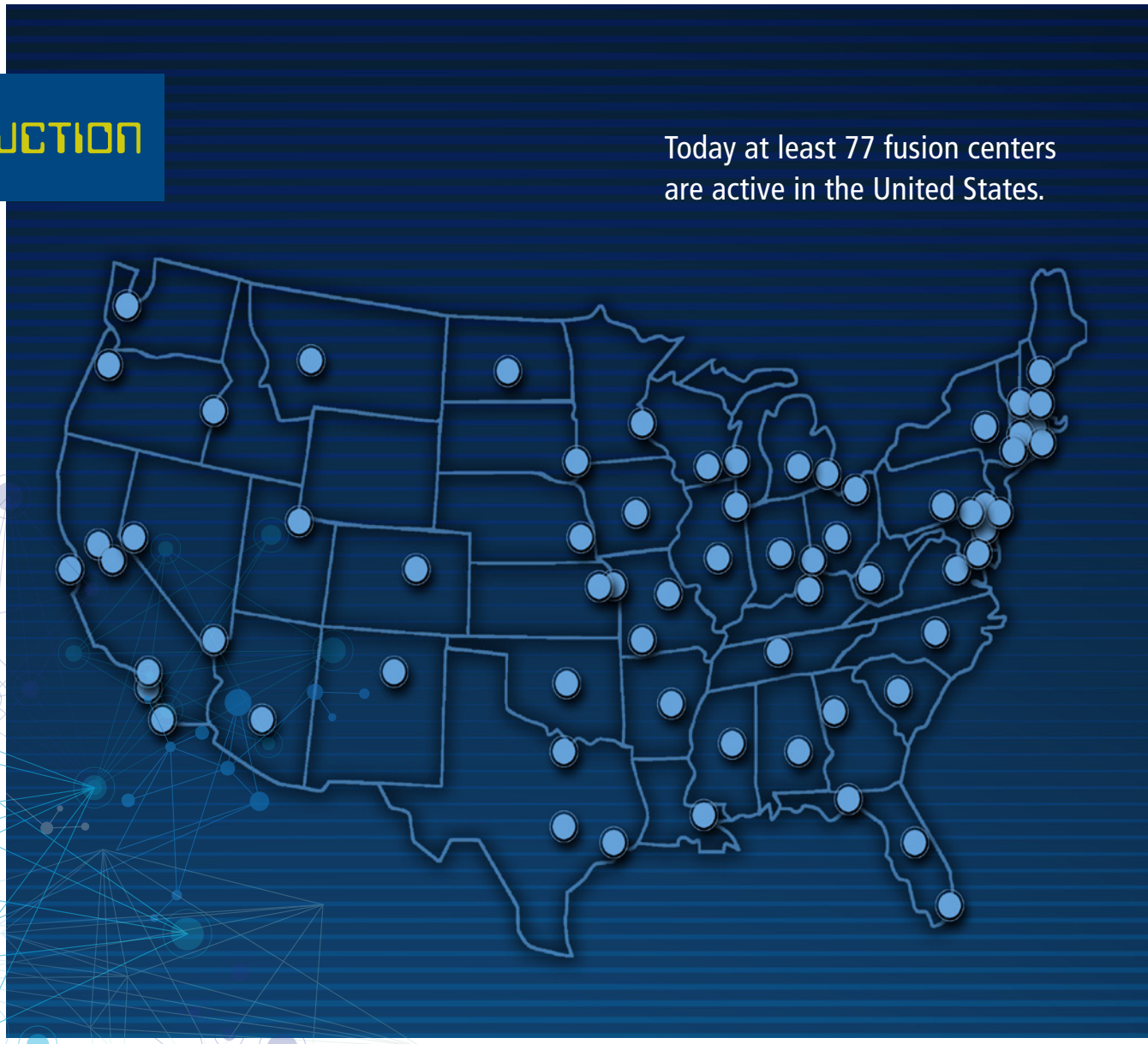
Miles N. Ruthberg, Partner, Latham & Watkins LLP

THE CONSTITUTION PROJECT STAFF:

Sharon Bradford Franklin, Senior Counsel, Rule of Law Program

*Affiliations are listed for identification purposes only

1. INTRODUCTION



In the aftermath of the September 11, 2001 terrorist attacks, the federal and state governments embarked on a far-ranging effort to detect and defend against potential terrorist threats.[1] One of the central components of this effort has been the creation of a network of state and regionally-based fusion centers that share information among law enforcement and some intelligence agencies. Today at least 77 fusion centers are active in the United States.[2] While these state entities have received substantial support from Congress and the Executive Branch, their roles and missions vary widely and are still being developed. Run properly, fusion centers could play an

important role in addressing terrorist and other criminal threats. Yet fusion centers can also pose serious risks to civil liberties, including rights of free speech, free assembly, freedom of religion, racial and religious equality, privacy, and the right to be free from unnecessary government intrusion. Several fusion centers have issued bulletins that characterize a wide variety of religious and political groups as threats to national security. In some instances, state law enforcement agencies that funnel information to fusion centers have improperly monitored and infiltrated anti-war and environmental organizations. Moreover, the manner in which fusion centers amass and distribute personal information raises the concern that they are keeping files—perhaps containing information that is sensitive or concerns constitutionally protected activities—on people in the United States without proper justification.

The very nature of the fusion center network raises the stakes. In such an interconnected system, fusion centers—even those with the best civil liberties practices—can inadvertently perpetuate or exacerbate the problematic activities of other fusion centers or law enforcement agencies. The breadth of the fusion center network also means that inaccurate or problematic information can be distributed widely across government databases, and perhaps even to private businesses, with potentially disastrous consequences for individuals. Finally, without proper safeguards, links between fusion centers in different states might allow "forum-shopping" law enforcement officials to evade the privacy and domestic surveillance restrictions of their own states by accessing information obtained by fusion centers in other jurisdictions. All of these risks are potentially compounded by the limited transparency and accountability of these institutions.

Further, because fusion centers are new and protean, their role and effectiveness demand further study.[3] Some basic principles, however, are clear. The ability of state and federal agencies to identify potential threats requires the careful identification and analysis of discrete items among mountains of information. Because fusion centers can amass an incredible amount of data, they must ensure that they collect information effectively and judiciously to avoid burying analysts underneath an avalanche of information of negligible value or dubious relation to terrorism or other criminal activity.[4] In addition, the principal benefit of utilizing local law enforcement in this national effort—its close connection to the community—depends on maintaining a cooperative and collaborative relationship with that very community. Casting stigma on individuals for exercising their religion, speaking out or attending group functions risks alienating segments of the community whose cooperation can be critical to counterterrorism and law enforcement efforts.

For these reasons, we, the members of The Constitution Project's Liberty and Security Committee endorsing this report, have undertaken this examination of fusion centers, and offer a set of recommendations to assist policymakers to ensure that fusion centers operate effectively while respecting civil liberties and constitutional values. Part II of this report provides an overview of the structure of fusion centers and the institutional framework within which they operate. Parts III, IV and V identify specific concerns raised by fusion center data collection, data storage and use, and accountability and governance mechanisms. Part VI outlines our specific recommendations for reforms that address civil liberties concerns.

Yet fusion centers can also pose serious risks to civil liberties, including rights of free speech, free assembly, freedom of religion, racial and religious equality, privacy and the right to be free from unnecessary government intrusion.

We hope that these recommendations will facilitate the development of sound rules and best practices to ensure respect for constitutional rights and values. Indeed, fusion centers themselves seek concrete guidance on the practical application of constitutional principles to daily threat assessment.[5] We also hope that they will encourage further consideration of the proper role and mission of fusion centers within the nation's law enforcement and anti-terrorism framework.

II. OVERVIEW

A. What is a Fusion Center? Although they take many forms, fusion centers are essentially information-sharing hubs designed to pool the knowledge and expertise of state, local and federal law enforcement and intelligence agencies, and, in some instances, other government agencies, military officials and private sector entities.[6] Individual fusion centers are independent regional, state or local entities, with no specific federal legal status. They operate primarily on state funding, though they generally receive federal funds and work closely with federal agencies such as the Department of Homeland Security (DHS) and the Department of Justice (DOJ). As a general matter, fusion centers are not established pursuant to specific state legislation or state executive orders, but rather derive their authority from general statutes creating state police agencies or memoranda of understanding among partner agencies.[7] Many fusion centers simply represent extensions of existing intelligence units in state law enforcement agencies.[8]

Fusion centers were originally intended to focus on terrorist threats, but their operational goals have expanded over the past decade. Today, fewer than 15% of fusion centers describe their mission solely as addressing terrorist threats.[9] Most embrace an "all-crimes, all-hazards" approach.[10] Fusion centers thus facilitate the exchange of critical information between federal and state agencies relating to terrorist threats, state and local law enforcement, criminal intelligence and, in many instances, natural disasters and hazards.

To perform this role, fusion centers collect and disseminate a wide array of information. They access information from a diverse spectrum of sources, including databases maintained by federal, state and local government agencies, law enforcement and intelligence files, records of financial transactions and utilities payments and insurance-fraud databases.[11] Many fusion centers also maintain subscriptions to the commercial databases of private information re-sellers. For example, some states buy access to credit reports and others to car-rental databases. Often these databases provide instant access to records on homes, cars and phone numbers.[12] In addition, the federal government encourages fusion centers to collaborate with a wide variety of private actors in sectors such as banking, education, energy, and hospitality and lodging.[13]

Fusion centers often act as clearinghouses for information.[14] In addition to collecting information, they also analyze and re-distribute the information they receive, whether in the "raw" form of reports of suspicious activity or potential infrastructure vulnerabilities, or in the "processed" form of intelligence bulletins.

Mirroring this diverse set of objectives and capacities, the structure of fusion centers varies considerably across jurisdictions. As of June 2012, there were 77 federally-recognized fusion centers in the United States.[15] Fusion centers are staffed by anywhere from 3 to 250 individuals—averaging, in 2008, 27 full-time personnel—the majority of whom are state law enforcement officers and analysts.[16] Fusion centers adopting an all-crimes, all-hazards approach often include officials from the local department of health, fire department, emergency medical services and other public agencies. Federal agencies such as DHS, the Federal Bureau of Investigation (FBI), Immigration and Customs Enforcement, and the National Counterterrorism Center deploy analysts, linguists and agents to many fusion centers.[17] In addition, approximately 30% of fusion centers co-locate with federal agencies or the National Guard, thereby increasing the federal role.[18]

B. Federal Support of Fusion Centers

While fusion centers are not federal entities and have no federal legal status, they are a central element of homeland security policy and receive substantial federal support and guidance.[19] As Secretary of Homeland Security Janet Napolitano put it, "Fusion Centers will be the centerpiece of state, local [and] federal intelligence-sharing for the future."[20] Federal funding matches this rhetoric: between 2004 and 2007, DHS provided $254 million to state and local governments to support fusion centers.[21] Federal funding accounts for 20 to 30 percent of state fusion center budgets.[22]

In addition to financial support, the federal government supports fusion centers by providing guidance, training, technological and logistical assistance and personnel.[23] The Office of Intelligence and Analysis at DHS takes lead responsibility for coordinating with fusion centers, but both DHS and DOJ provide assistance.[24] Together, the two agencies have established guidelines (the "Fusion Center Guidelines") and basic operational standards (the "Baseline Capabilities") for fusion centers.[25] They also provide technological and logistical support to fusion center personnel and help them to obtain federal security clearances.[26] And, as described above, many fusion centers have been assigned federal personnel.

Fusion centers are integrated into federal information-sharing programs. Qualified fusion centers form part of the federal Information Sharing Environment, which is intended to facilitate information sharing among law enforcement and intelligence agencies.[27] Fusion centers staffed by individuals with federal security clearances receive information from a multitude of federal intelligence and law enforcement databases.[28] Fusion centers also transmit information they receive to these databases.[29] Compliance with certain privacy and civil liberties policies is required for participation in the Information Sharing Environment.[30] Recently—and commendably—DHS has conditioned its grant funding for fusion centers on certification that the fusion centers have privacy and civil rights protections that are as comprehensive as the federal Privacy Guidelines for the Information Sharing Environment.[31]

> Today, fewer than 15% of fusion centers describe their mission solely as addressing terrorist threats.

C. Proposed Federal Fusion Center

In late 2010, DHS proposed creating a federal fusion center intended to collect and analyze information related to "all-threats and all-hazards, law enforcement activities, intelligence activities, man-made disasters and acts of terrorism, natural disasters and other information collected or received from federal, state, local, tribal and territorial agencies and organizations; foreign governments and international organizations; domestic security and emergency management officials; and private sector entities or individuals."[32] At present, little is known about the specific purpose and design of this proposed fusion center, but it has drawn protests from groups concerned about its impact on civil liberties and technology privacy.[33]

III. DATA COLLECTION

Fusion Centers and their personnel are tasked with wide-ranging investigative and intelligence-gathering activities, including information collection and the identification of potentially suspicious groups or behavior. Concerns about constitutional rights to privacy, equal protection and freedom of expression are always present when law enforcement agencies collect information on people in the United States. These concerns are magnified in the case of fusion centers, given the amount of data that they can aggregate and their role as hubs in an information-sharing network. In particular, the nature of fusion centers raises concerns that information may be improperly accessed by or stored in fusion center databases, and that individuals might be subject to unwarranted scrutiny based on innocuous activities or their political or religious beliefs or racial status. Cooperation and information sharing are essential to effective policing, but troubling anecdotal reports indicate that some fusion centers have disregarded constitutional limitations on law enforcement activity and may have infringed upon the rights of U.S. citizens and residents. In addition, new systems of collecting and disseminating reports of suspicious activity observed by local law enforcement officials could result in the creation of vast databases of information compiled on individuals without reasonable suspicion that these individuals are linked to terrorism or any other criminal activity.

A. Risks of Racial, Religious and Political Profiling

While information sharing is vital to keeping the United States safe from terrorist threats, efforts by fusion centers to monitor and share information about individuals in the United States implicate fundamental constitutional rights of freedom of speech, freedom of religion, freedom of association and equal protection under the law. As discussed below, a number of disturbing reports indicate that some fusion center and state and federal law enforcement personnel have targeted individuals for suspicion based on characteristics such as religion, political beliefs and race. Profiling on these grounds is neither effective nor consistent with constitutional values. In addition, the information-sharing function of fusion centers has the potential to multiply the harm caused by profiling, because improperly acquired information in one fusion center can readily be disseminated to other fusion centers, law enforcement agencies and federal intelligence agencies.

1. Constitutional Principles

Profiling based on religious, racial or political grounds is inconsistent with constitutional principles and values. Investigating individuals on these protected grounds implicates the First and the Fourteenth Amendments to the U.S. Constitution, among other constitutional provisions.[34]

The First Amendment protects the rights of individuals to express their religious and political beliefs and to associate freely to share those beliefs. Freedom of association, religion and expression are such bedrock values that even laws and policies that merely discourage or "chill" these activities, rather than restrict them outright, are prohibited.[35] Based on this principle, the Supreme Court and other courts have recognized that intrusive government surveillance of "expressive" activities, such as political or social activism, can violate the First Amendment.[36]

...a number of disturbing reports indicate that some fusion center and state and federal law enforcement personnel have targeted individuals for suspicion based on characteristics such as religion, political beliefs and race.

The Fourteenth Amendment forbids each state government from "deny[ing] to any person within its jurisdiction the equal protection of the laws"[37] and therefore prohibits government institutions and employees from discriminating against individuals on the basis of race, ethnicity, national origin, or religion.[38] The Fifth Amendment provides similar safeguards against discrimination by the federal government. Based on these constitutional protections, law enforcement may not use race, religion and other protected characteristics as grounds for determining whom to target for investigation.[39] By the same token, information about an individual that is already contained in a fusion center database should not be shared with another government entity on the sole basis that the individual belongs to a particular race or ethnicity or practices a particular religion.[40]

2. Reports of Political, Racial and Religious Profiling

Despite these constitutional principles, there have been numerous anecdotal reports of incidents in which fusion centers have targeted individuals in the United States for surveillance and investigation based solely on beliefs and characteristics that are protected by the First and Fourteenth Amendments. Although federal guidance to fusion centers cautions against profiling, these incidents demonstrate that significant additional guidance,

training and oversight are crucial to ensure that fusion centers and other law enforcement agencies do not engage in racial, religious and political profiling.[41]

Recent reports from across the country bear testament to the potential for problematic profiling at fusion centers, particularly regarding bulletins and intelligence reports circulated by fusion centers. These are a few examples:

- The February 2009 "Prevention Awareness Bulletin," circulated by a Texas fusion center, described Muslim lobbying groups as "providing an environment for terrorist organizations to flourish" and warned that "the threats to Texas are significant."

  The bulletin called on law enforcement officers to report activities such as Muslim "hip hop fashion boutiques, hip hop bands, use of online social networks, video sharing networks, chat forums and blogs."[42]

- A Missouri-based fusion center issued a February 2009 report describing support for the presidential campaigns of Ron Paul or third party candidates, possession of the iconic "Don't Tread on Me" flag and anti-abortion activism as signs of membership in domestic terrorist groups.[43]

- The Tennessee Fusion Center listed a letter from the American Civil Liberties Union (ACLU) to public schools on its online map of "Terrorism Events and Other Suspicious Activity." The letter had advised schools that holiday celebrations focused exclusively on Christmas were an unconstitutional government endorsement of religion.[44]

- The Virginia Fusion Center's 2009 Terrorism Risk Assessment Report described student groups at Virginia's historically black colleges as potential breeding grounds for terrorism and characterized the "diversity" surrounding a military base as a possible threat.[45]

Other reports, although they do not involve fusion centers *per se*, provide additional troubling examples of profiling and demonstrate the manner in which problematic incident reports can spread through linked databases. For example, from 2005 to 2007, the Homeland Security and Intelligence Division of the Maryland State Police secretly monitored a wide range of anti-war, anti-death penalty, animal rights and bike lane activists, even going so far as to employ undercover operatives to infiltrate meetings. The surveillance lasted for several years, despite the fact that no evidence of criminal activity was ever uncovered. Even more troubling, the police characterized these groups and individuals as terrorists and security threats in state files which were subsequently transmitted to federal databases. All told, data characterizing 53 peaceful activists (including two nuns) as "terrorists" was transmitted to at least seven federal and state agencies, including the National Security Agency.[46] In a similar incident, Pennsylvania state homeland security officials reportedly hired contractors to draft intelligence bulletins on a wide range of protest movements and activities, including a gay and lesbian festival, Tea Party meetings, an anti-British Petroleum candlelight vigil and the screening of an environmentalist documentary film. These intelligence bulletins were distributed to both law enforcement personnel and the security offices of private companies.[47] In an example of potential profiling on other grounds, reporters analyzing suspicious activity reports generated by the private security offices at Minnesota's Mall of America and shared with the local police department and the Minnesota state fusion center revealed that nearly two-thirds of the reports involved minorities.[48] According to the Mall's security director, his office is the Minnesota fusion center's "number-one source of actionable intelligence."[49]

Reports of training sessions provided to fusion center personnel and local law enforcement officers by so-called "counterterrorism experts" also raise serious questions about compliance with constitutional protections against profiling on religious grounds. According to recent press accounts, the flood of federal money flowing to local enforcement for homeland security efforts has produced a cottage industry of counterterrorism trainers of dubious provenance.[50] As outlined in the reports, some of these trainers engage in fear-mongering that displays dramatic ignorance of both the subject they purport to teach and the constitutional rights of Americans.

According to an article in *The Washington Post*, one instructor told fusion center personnel to monitor Muslim student groups and mosques and, if possible, to tap their phones.[51] The same instructor told an interviewer that to prevent Muslims from seeking to impose *sharia* law in the United States, police officers "have to look at the entire pool of Muslims in a community."[52] Another instructor warns local law enforcement officials that Muslims want the "Islamic flag [to] fly over the White House."[53] One self-proclaimed expert on Islamic terrorism, who regularly teaches courses to law enforcement personnel across the country, told Florida law enforcement officers to assume that all Muslims lie to disguise the true, violent nature of Islam. He also claimed as fact that a Muslim wearing a headband means that he is willing to be a martyr, and that a Muslim using a long Arabic name that is spelled differently on different forms of ID provides "probable cause to take them in."[54] None of these claims, of course, are true. This sort of misbegotten, misleading training encourages civil liberties violations. National security experts warn that it also compromises police effectiveness by distracting law enforcement officers from actual threats and by poisoning relationships between police and the communities that can be their best sources of information.[55]

In sum, these reports show that fusion centers must take serious steps to ensure that they do not violate the Constitution by investigating, storing or sharing information about—or by issuing bulletins or intelligence reports that advise other law enforcement agencies to investigate—individuals or groups based solely on protected grounds such as race, ethnicity, religion and political expression. These steps include establishing structures for effective oversight and providing clear guidance, in the form of both written policies and training, to fusion center personnel about the rights protected by the First and Fourteenth Amendments. Another step is to ensure that individuals who train fusion center and law enforcement personnel are themselves competent and knowledgeable about their subject matter and the constitutional strictures that govern law enforcement activity.

B. Suspicious Activity Reports and Privacy

The DHS plans to use fusion centers to form a national network for collecting and sharing local law enforcement reports of suspicious, potentially terrorism-related activity. This effort is known as the Nationwide Suspicious Activity Reporting (SAR) Initiative.[56] While information sharing can be important for law enforcement, the program also has the potential to infringe upon constitutional rights of privacy and fundamental notions of appropriate government collection of information. In particular, the loose definition of "suspicious activity" under these plans could result in the creation of government databases that store files on individuals who have no link to terrorism or any other criminal activity.

This sort of misbegotten, misleading training encourages civil liberties violations.

1. Constitutional and Federal Privacy Law

The collection and storage of information about individuals by the government implicates the privacy rights of Americans. Privacy is a broad concept that is susceptible to many definitions, but at its core, the right to privacy protects what Supreme Court Justice Louis Brandeis described as "the right to be let alone."[57] The National Research Council describes privacy as "an individual's freedom from excessive intrusion in the quest for information and an individual's ability to choose the extent and circumstances under which his or her beliefs, behaviors, opinions and attitudes will be shared with or withheld from others."[58] While the right to privacy is not specifically enumerated in the Bill of Rights and its exact contours are subject to debate, it is protected in various forms by the First, Third, Fourth, Fifth and Fourteenth Amendments and is fundamental to the concept of a democratic society under limited government. At least ten state constitutions expressly protect the right to privacy, and courts in many more states have found the right to privacy implicit in state constitutions.[59]

Constitutional protections of privacy are supplemented by federal and state statutes. Many federal and state laws and regulations, including the Privacy Act of 1974,[60] require government agencies

and officials to respect individual privacy. While law enforcement agencies are excepted from many Privacy Act protections and the Act does not apply to the states,[61] law enforcement data collection is governed by federal statutes, including the Electronic Communications Privacy Act[62] and Fair Credit Reporting Act,[63] as well as by state statues. Perhaps the most important privacy restriction on fusion centers, however, is federal regulation 28 C.F.R. Part 23.

28 C.F.R Part 23 prohibits state law enforcement agencies that receive federal funding from collecting or maintaining personal information about individuals in criminal intelligence databases unless "there is *reasonable suspicion* that the individual is *involved in criminal conduct* and the information is *relevant to that criminal conduct or activity.*"[64] The "reasonable suspicion" standard requires that a law enforcement official gathering data about an individual be aware of information giving him or her a basis to believe that there is a reasonable possibility that the individual is involved in a definable criminal activity.[65] The Supreme Court has explained that "reasonable suspicion" is founded on "specific and articulable facts" rather than "inarticulate hunches."[66]

2. Suspicious Activity Reports

The Suspicious Activity Reporting Initiative enlists fusion centers in a national network to collect and analyze reports of suspicious activity that might be related to terrorist threats. Notably, the DOJ interprets 28 C.F.R Part 23 to exclude suspicious activity reports because they consist of "tips and leads data"—defined as an "uncorroborated report or information . . . that alleges or indicates some form of criminal activity"—and thus do not meet the statutory definition of criminal intelligence information that is subject to 28 C.F.R. Part 23. The structure of the reporting system and the criteria for suspicious activity raise the concern that this system could result in the amassing of government files on individuals without adequate justification, particularly if DOJ defines suspicious activity reports in a manner in which they are not governed by 28 C.F.R. Part 23.[67]

The suspicious activity reporting system begins with police officers and private citizens reporting incidents that they believe are potentially indicative of terrorism-related activity. These reports are then forwarded from the local law enforcement agency to the state or regional fusion center. At the fusion center, the reports are logged into the fusion center's database and analyzed to determine whether there is a "potential nexus to terrorism."[68] If the fusion center makes that determination, the report could then be shared with the Information Sharing Environment and/or the FBI's eGuardian system, where they would be accessible by federal intelligence and law enforcement agencies and other fusion centers. In March 2011, the DOJ released a manual to train fusion center employees on how to vet suspicious activity reports and determine whether they meet the criteria for wider distribution.[69] Guidance provided by the federal office responsible for overseeing the Information Sharing Environment emphasizes that its "*behavior-focused approach* to identifying suspicious activity requires that factors such as race, ethnicity, national origin or religious affiliation should not be considered as factors that create suspicion."[70]

Nonetheless, the definitions of suspicious behavior used by the federal government and police forces are wide-ranging and include behavior that may be completely innocuous. For instance, the Los Angeles Police Department (LAPD) Special Order 11, praised by the Office of the Director of National Intelligence as a "national model,"[71] calls upon LAPD officers to report "suspicious activities" that encompass non-criminal conduct

such as using binoculars, taking notes, drawing diagrams and "espousing extremist views."[72] The ACLU criticized the LAPD, expressing concern that "overbroad reporting authority gives law enforcement officers justification to harass practically anyone they choose, to collect personal information and to pass such information along to the intelligence community."[73] Special Order 11 was superseded by Special Order 1 in January 2012. While the new policy adopts a narrower definition of "suspicious activities," it has been criticized by civil liberties organizations and other advocacy groups.[74] The federally published standards for suspicious activity reports, like the LAPD Special Orders, describe conduct that might not meet the "reasonable suspicion" standard. For example, "observation through binoculars" and "taking notes" could provide grounds for a suspicious activity report.[75] As of the date of this report, the LAPD has agreed to amend its policy, although the new standards have not yet been released.

An example of an actual suspicious activity report described in *The Washington Post* illustrates some of the problematic aspects of the reporting system. An officer observed a man snapping photos of a police fire boat and a ferry with a cell phone camera. The man made a phone call and was eventually joined by two other adults and two small children, all of whom then boarded the ferry. The report of this activity was passed along to the regional fusion center. Authorities would not address what happened to the report after it reached the fusion center, but even if the fusion center concluded that it was harmless, it would still be forwarded to the FBI. At the FBI, the report would either be used to start a full-fledged investigation or be deemed irrelevant, in which case the FBI would leave the report in its suspicious activity reporting database, eGuardian. The most likely outcome, however, would be that no decision would be made and a file would remain open on the individual in question. Over time, more information could be added to the file, including employment and financial history, phone numbers, addresses and any other potentially useful information.[76] In another real-life example, a suspicious activity report generated by the private security team of a large shopping center based on nothing more suspicious than a cell phone accidently left on a cafeteria table resulted in a visit by the FBI to the cell phone owner's home. The investigation concluded that a 72-year-old man who operated a kiosk in the shopping center simply forgot his phone on the table during a break.[77]

These types of practices raise civil liberties and privacy concerns, particularly in cases in which suspicious activity reports are forwarded to the FBI or shared with other agencies. These concerns are heightened when law enforcement officials receive inadequate or problematic training such as the inaccurate and misleading instructions described above concerning Muslim-American communities.

Ultimately, while an individual taking pictures of a ferry or a cell phone sitting on an abandoned table might warrant an initial inquiry, it certainly does not justify the creation of a government file linking that individual to terrorism. Such a file might easily have serious consequences. It might be accessed by law enforcement or intelligence agencies—or perhaps released to private sector entities—with potentially severe ramifications, including placement on a no-fly list, loss of employment or serious reputational harm. To limit these consequences, files that link individuals to allegations of terrorism should not be held in government databases unless those files are based on information that rises to the level of "reasonable suspicion" of criminal activity. This standard also has the benefit of familiarity to law enforcement personnel because it is the same standard required for conducting a *Terry* stop,[78] performing a protective sweep of a home during the execution of a search warrant,[79] or frisking the passenger of a vehicle.[80]

…files that link individuals to allegations of terrorism should not be held in government databases unless those files are based on information that rises to the level of "reasonable suspicion" of criminal activity.

IV. DATA STORAGE AND USE

Fusion centers store personal information about Americans and may have access to a vast range of government databases. They can access and share information from state and local criminal record systems, as well as federal intelligence and law enforcement databases. They can also gain access to personal information, including unlisted phone numbers, insurance claims, car rental information, drivers' license photographs and credit reports, through commercial databases owned by "information resellers."[81] While access to information is necessary to achieve the anti-terrorism and anti-crime goals of fusion centers, policymakers must balance the desirability of the free flow of information against the risks that information will be abused or shared inappropriately.

A. Fair Information Practice Principles

Since the early 1970s, in response to the growing use of computerized record systems, government agencies in the United States (and later Europe) developed a series of reports, guidelines and codes that have given rise to a set of widely-accepted "Fair Information Practice Principles."[82] Today, these principles guide the treatment of government-held records containing personally identifiable information and form the basis of state and federal privacy laws and international treaties.[83]

Personally identifiable information refers to information that can be used to identify a specific individual. In an age where vast amounts of information can be accessed and cross-checked online, the range of information that can be used to specifically identify an individual has grown. With this in mind, the White House Office of Management

and Budget defines "personally identifiable information" as "information that can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."[84] For the purposes of this discussion, "personally identifiable information" is any personal information that is linked or linkable to an individual.[85]

The Fair Information Practice Principles have been expressed in a number of different formulations, but at their core they call upon governments that maintain personal records about individuals to afford those individuals the following rights:

- **Notice and Awareness** of the purpose of data collection, and how such information is used;
- **Consent** to the collection of personal information and **Choice** as to how it is used;
- **Access and Participation** in the process of data collection and use, including the right to correct errors;
- **Data Security and Integrity** adequate to protect the information against loss or misuse; and
- **Redress and Accountability** for injury resulting from the loss or misuse of personal information, to give meaning and effect to the previous principles.[86]

These principles form the basis of the Privacy Act of 1974, a federal statute that governs federal databases that contain records of personally identifiable information on U.S. citizens or lawful permanent residents.[87] While the federal Privacy Act does not apply to state and local entities and federal law enforcement databases are specifically exempted from some Privacy Act protections,[88] the Privacy Act and Fair Information Practice Principles provide a sound framework for the manner in which fusion centers should handle the information that they store and access. Indeed, the Fusion Center Guidelines advise fusion centers to abide by Fair Information Practices,[89] and several state fusion centers explicitly refer to the Fair Information Practice Principles in their own privacy and civil liberties policies.[90]

Given the need for confidentiality in certain fusion center operations, the application of the Fair Information Practice Principles outlined above may be limited in some respects. Nonetheless, the Fair Information Practice Principles of notice and awareness, consent and choice, access and participation, integrity and security, and redress and accountability should guide all fusion centers, as far as possible, in the manner in which they access, store and share information.

B. Data Minimization and Use Limitations

Two additional privacy principles that are directly applicable to fusion centers are data minimization and use limitation.[91] Data minimization refers to the principle that personally identifiable information should be utilized for a specified purpose and retained only so long as necessary to fulfill that purpose. The 28 C.F.R. Part 23 provisions restricting information in criminal intelligence databases to information relevant to an individual's suspected criminal conduct is an example of data minimization.[92] So too is the 28 C.F.R. Part 23 requirement for the periodic review of information and the destruction of any information which is misleading, obsolete or otherwise unreliable and the requirement that any recipient agencies be advised of such changes which involve errors or corrections. All information retained as a result of this review must reflect the name of the reviewer, date of review and explanation of decision to retain. Information retained in the system must be reviewed and validated for continuing compliance with system submission criteria before the expiration of its retention period, which in no event shall be longer than five years.[93]

> In an age where vast amounts of information can be accessed and cross-checked online, the range of information that can be used to specifically identify an individual has grown.

Fusion centers should adopt similar data minimization practices. Given the sensitivity of the information that they retain and the ease with which intelligence and law enforcement officials across the country can access this information, fusion centers should review the information in their files more frequently than every five years.

Use limitation refers to the principle that personally identifiable information should only be used for the purpose for which it was collected. In other words, personally identifiable information gathered by fusion centers should only be directed towards law enforcement or intelligence purposes. Similarly, it should only be shared with agencies that intend to use the information for the purposes for which it was gathered. Consistent with this aim, the Markle Task Force on National Security in the Information Age recommended that information sharing networks require "a user to provide a predicate in order to access data under an authorized

use standard. To establish a predicate, an analyst seeking information would need to state a mission- or threat-based need to access the information for a particular purpose."[94] Use limitation is also found in 28 C.F.R. Part 23, which only permits sharing when there is a need to know and a right to know the information in the performance of a law enforcement activity. Additionally, the information may only be shared with law enforcement authorities that agree to follow procedures regarding information receipt, maintenance, security and dissemination which are consistent with the principles of 28 C.F.R. Part 23.[95]

C. Audit Logs

As the Fair Information Practice Principles make clear, any effective and safe repository of personally identifiable information must ensure the security and integrity of data and the accountability of users of that data. Data security is particularly significant in the context of fusion centers, which access a wide range of databases. In certain instances, fusion centers do not operate databases themselves, but rather access information from the databases of other agencies and institutions at the state, local and federal levels.

However, wherever data is ultimately stored, fusion centers must incorporate safeguards and accountability measures for the data that they can access. Unfortunately, anecdotal reports indicate that there is some confusion on these points among fusion center employees. One analyst explained that his fusion center "does not host the data, but rather refreshes [it] regularly. That means analysts are not subject to Freedom of Information Act or being dragged into court."[96] Fusion center personnel and other intelligence and law enforcement officials may also believe that the principles of accountability and data integrity and security do not apply when they are accessing personal information from commercial "information reseller" services.[97]

Yet, when personally identifiable information is accessible online or over a network, the location where that information is hosted, stored or owned has little to do with the potential for its misuse. All who have access to that information for governmental purposes should be held accountable.

One simple solution to promote data security and user accountability—and thus the protection of civil liberties—is the use of immutable audit logs to monitor individuals and entities that access information. These logs record network activity, such as the nature of queries for information, the user making the query, the information accessed, and the date and time of these activities.[98]

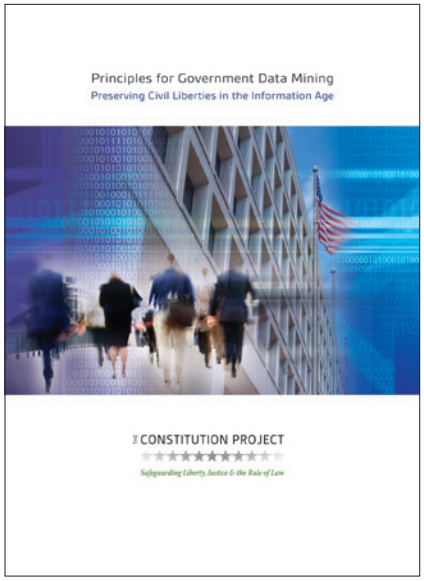
Immutable audit logs serve many purposes. They improve the ability to detect privacy violations and the unauthorized access of sensitive information, and facilitate audits of databases and organizations to ensure compliance with legal restrictions. Because they cannot be altered or edited, they provide valuable proof of unauthorized behavior, improving the ability of system administrators to punish transgressors.[99] Consequently, they deter users who would otherwise access and use information improperly.[100] By increasing data security and accountability, audit logs help promote public trust in government and trust between institutional users.[101] They might also protect against intrusion into databases by hackers or other unauthorized outsiders.

Anecdotes from the 2008 presidential campaign illustrate both the privacy risks posed by government databases and the use of audit logs to track potential violations of information privacy. In early 2008, a State Department auditing system determined that private contractors had improperly accessed the passport files of presidential candidates Hillary Clinton, Barack Obama and John McCain. Several of the contractors were disciplined for their actions.[102] Later in the election season, Ohio state government employees made a number of intrusive searches in state databases for information regarding Joe Wurzelbacher, the public John McCain supporter more commonly known as "Joe the Plumber." Audits of these searches enabled investigators to determine that a number were legitimate, but also that several were unauthorized and improper. Several employees reportedly were disciplined, one resigned, and another was placed under criminal investigation.[103]

Immutable audit logs, which have been widely recommended by government agencies,[104] national security think-tanks,[105] and even the former General Counsel of the National Security Agency,[106] should form a central component of fusion center data security policies. For example, the National SAR Initiative Federated Search capability utilizes such an audit trail.[107] Given the networked nature of fusion centers, these audit logs should apply equally to proprietary databases and outside databases hosted by federal, local and other state entities. They should also apply to the access of commercial databases, which increasingly contain sensitive and private personal information. Furthermore, 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.

D. Data Mining

The vast range of information that can be gathered, aggregated and analyzed through an interconnected network of fusion centers gives rise to the possibility that fusion centers might be used to facilitate data mining by federal or state authorities. Data mining generally refers to the use of statistical analysis and modeling to discern patterns or relationships in large aggregations of data.[108]



These techniques have numerous applications, from program evaluation to fraud detection to criminal investigation and counterterrorism. The Constitution Project's Liberty and Security Committee addressed the issues raised by data mining in our 2010 report *Principles for Government Data Mining*.[109] As we explained in that report, while data mining programs possess the potential to provide unique insights, they can pose serious risks to civil liberties, particularly in the criminal prevention and counterterrorism contexts. For example, inaccurate data or imprecise modeling risks both missing evidence of impending criminal acts or terrorism and falsely accusing innocent persons.[110] Data mining programs might also utilize constitutionally problematic criteria, such as race or religion, or be directed towards constitutionally impermissible ends.[111] If fusion centers engage in or facilitate data mining, they should take particular care to address these dangers.[112]

E. Private Sector Partnerships

Private sector entities often work closely with fusion centers. For example, the security director for a large shopping center in Minnesota told Congress that his office was the "number one source of actionable intelligence in the state" and had provided more information regarding suspicious activities to the state fusion center than any other source.[113] Some large corporations even have employees specifically assigned to fusion centers.[114]

The federal government encourages a close relationship between the private sector and fusion centers. These relationships, particularly with entities in sectors like energy, transportation, communications and health care, can play an important role in ensuring that fusion centers are able to assess threats to critical infrastructure and respond effectively.[115] According to the Fusion Center Guidelines, published jointly by the DHS and DOJ, "[t]he private sector is a crucial component of fusion centers."[116] A supplement to the Fusion Center Guidelines explains that "[f]usion centers . . . shall develop, implement and maintain a plan and procedures for sharing information with owners of [critical infrastructure and key resources] and, in general, the private sector, in a coordinated manner."[117]

These relationships raise concerns, however, in light of the highly sensitive material that fusion centers gather, store and access. While the federal government has encouraged fusion centers to welcome private sector representatives into their facilities—and even to station private sector personnel inside fusion centers on a full-time basis[118]—these partnerships suggest that sensitive, personally identifiable information might be shared with individuals lacking the appropriate clearance levels or public mission. Instances of inappropriate information sharing with private sector entities have already been reported. For example, intelligence bulletins prepared by the Pennsylvania Office of Homeland Security on a number of innocuous protest activities, such as the screening of an environmentalist documentary film, reportedly were shared with security officers of private companies.[119] Access by private sector individuals to the sensitive information held by fusion centers seriously impinges on privacy and could cause unjustified reputational harm. Such disclosures might also risk compromising ongoing investigations.

Access by private sector individuals to the sensitive information held by fusion centers seriously impinges on privacy and could cause unjustified reputational harm.

The flow of information in the opposite direction, from the private sector to fusion centers, is also potentially problematic. Private entities are usually privy to personal information about their employees and the individuals and organizations with whom they do business. Close relationships with fusion centers might facilitate the flow of this information into fusion center databases—and into the network of intelligence and law enforcement databases—without the proper legal requirements and processes.[120]

At present, the sole privacy-related policy guidance regarding cooperation between the private sector and fusion centers discusses methods to limit the risk that fusion centers will improperly disclose proprietary private sector data to outsiders or to regulatory agencies.[121] Yet from the civil liberties perspective, the use to which fusion centers might put private sector data and the movement of sensitive information from fusion centers to the private sector raise even more serious concerns.

Fusion centers should ensure that they do not share personally identifiable information with private individuals or entities unless necessary to carry out legitimate law enforcement functions. They must also take care not to access personally identifiable information in the possession of private sector entities without possessing an appropriate basis and following the appropriate procedures for seeking that information.

V. ACCOUNTABILITY

One of the most pressing concerns regarding fusion centers is accountability.[122] Accountability is crucial to both protecting privacy and civil liberties and ensuring that institutions operate effectively.[123] Yet, several features of fusion centers contribute to a lack of accountability. First, the rapid pace of advances in information technology and the nation's limited experience with the fusion center concept may make it difficult for policymakers to understand the nature and consequences of fusion center activity. Some fusion center employees may be aware of the latitude that can result from this lack of understanding; in the words of one analyst, fusion centers are "a sort of 'wild west' . . . in that they can use a variety of technologies before 'politics' catches up and limits options."[124] The wide variety of fusion center structures and the diverse legal regimes to which they are subject also complicate oversight. It is not always clear whether these governance structures are effective[125] or whether the fusion centers abide by the relevant legal regimes.[126] And while the federal government exercises limited oversight of fusion centers, there are reports of federal agencies pushing states to flout or alter their laws at the expense of civil liberties. Finally, the secrecy that surrounds fusion centers makes public oversight of their activities more difficult. The following sections identify areas of concern and suggest reforms that would enhance accountability.

A. Mission Statements

Although fusion centers are intended to be a cornerstone of domestic anti-terrorism efforts, their goals and efficacy are not always clear. Without a clearly defined purpose, fusion centers may suffer from "mission drift." For example, fusion centers were originally focused solely on preventing terrorism. In recent years, however, most have been re-purposed to address general criminal activity and natural disasters as well as terrorist threats. This change in focus might mean that the methods and procedures that they employ are not necessarily well-suited to their new missions. Shifting metrics for success associated with the different functions of fusion centers can also complicate evaluating their performance.

To address this issue, each fusion center should develop a clear mission statement that sets forth the purpose of the fusion center and the metrics upon which its performance should be evaluated. These mission statements should be made widely available so that the public can better understand and evaluate the goals and performance of the fusion center. Additional study of the proper role for fusion centers, as called for below, would help guide the development of mission statements and metrics for accountability.

B. Transparency

Openness is a foundational principle of democratic government. Citizens rely on their knowledge of government to make informed decisions about how it should operate. Openness is also an important means of ensuring that government officials abide by the laws that govern their conduct and respect civil rights and civil liberties. In the oft-quoted words of Supreme Court Justice Louis Brandeis, "Sunshine is said to be the best disinfectant; electric light the most efficient policeman."[127]

> ...the secrecy that surrounds fusion centers makes public oversight of their activities more difficult.

While national security concerns legitimately impact what information may be disclosed about terrorist threats, this is not sufficient to explain the fact that little information is publicly available about the actual practices and activities of individual fusion centers. Indeed, in some instances, federal agencies like the FBI have reportedly required states to exempt fusion centers from their open government laws as a condition to allowing those fusion centers access to important federal law enforcement databases—a troubling practice that implicates issues of federalism as well as transparency.[128]

Fusion centers can gather and access vast amounts of information about people living in the United States—information that can cause real harm when improperly collected or shared. As noted above, certain fusion centers have already been implicated in problematic activities. And the history of domestic surveillance by law enforcement organizations in the United States in the 20th century confirms the risk that law enforcement may infringe on constitutional rights and values when tasked with "national security" operations but left unwatched and unregulated.[129]

Of course, the law enforcement activities of fusion centers require a degree of confidentiality, lest criminals and terrorists adjust their tactics to avoid detection or innocent persons be wrongfully

tarred with suspicion. There will thus be some limits to the level of transparency that is advisable for fusion centers. Nonetheless, there are practical benefits to increased transparency. Announcing fusion center policies and practices to the public might make fusion centers more effective by increasing public trust and thus promoting public cooperation.[130]

With these goals in mind, fusion centers should emphasize public outreach, as federal guidance documents advise.[131] They

should publish important information online, including broad descriptions of their activities, budgets and staffing, in an easily understandable and accessible format. Of particular importance, fusion centers should make the public aware of their policies for protecting privacy by publishing them online. Some fusion centers, including those based in Alabama, Minnesota, Texas and Virginia, have already taken this commendable step.[132] Others, such as the Minnesota Joint Analysis Center, have taken the additional and commendable step of publishing audits of their adherence in practice to privacy policies.[133]

C. Redress Mechanisms

Government databases that contain sensitive personal information should provide redress for individuals who believe that the databases contain inaccurate information about them.[134] An effective redress mechanism ensures the accuracy of database information and affords the opportunity for corrective action in the event of errors.[135]

Incorrect information in fusion center databases can have serious consequences for innocent individuals. Given the nature of investigations into criminal and terrorist activity, individuals subject to inaccurate information might, for example, find themselves subject to repeated, intrusive investigation or placed on watch-lists that interfere with their ability to travel or enjoy other basic rights.[136] For example, the DOJ Inspector General has already found significant inaccuracies in the federal Terrorist Screening Center watchlist.[137] In the words of the Inspector General, "inaccurate, incomplete and obsolete information increases the chances of innocent persons being stopped or detained during an encounter because of being misidentified as a watchlist identity."[138] The same concern holds true for information that is stored in or funneled through fusion centers.

Meaningful redress mechanisms are vital because they provide individuals with the opportunity to dispel unwarranted suspicion that interferes with fundamental rights and protected activities. To that end, fusion centers should develop procedures by which individuals can review and correct or challenge information possessed by a fusion center, if necessary. Federal guidance documents encourage redress mechanisms,[139] and certain fusion centers have already taken steps to adopt such mechanisms.[140] For example, the Alabama and Texas fusion centers have issued privacy policies that state that individuals are allowed access to personal information held by the fusion center (subject to certain restrictions), and that the fusion center will refer requests for access to information originated from another agency, or complaints about the accuracy of such information, to the originating agency.[141] Neither privacy policy, however, provides a clear description of the process for seeking correction of mistaken information or of the applicable appeals process.[142] These gaps should be addressed in Alabama and Texas, and redress procedures should be strengthened and made independent nationwide. Federal guidance on redress mechanisms is similarly broadly phrased and lacks specific instruction on the nuts-and-bolts of appropriate redress procedures.

The Liberty and Security Committee's report *Promoting Accuracy and Fairness in the Use of Government Watch Lists* provides specific recommendations for crafting redress mechanisms in the counterterrorism context.[143] Features of an effective redress mechanism that accounts for the secrecy necessarily demanded by the national security context might include public notice of the procedures for seeking redress and the review of questionable material by an independent, security-cleared arbiter. Another potential feature might be a two-tracked process, with one set of procedures for relatively easy-to-resolve cases of alleged mistaken identity and another more rigorous set of procedures for cases involving allegations of insufficient justification for inclusion in fusion center databases.[144] Given that some degree of confidentiality and secrecy is necessary to fusion center operations, in certain situations allowing individuals access to database information would be inappropriate. The rules for redress mechanisms should take this into account, perhaps by restricting review of personal information when the disclosure of information would interfere with an ongoing investigation or endanger the safety of another individual.

Another important characteristic of an effective redress mechanism is interoperability between systems. Given the networked nature of the fusion center environment, in which information is shared among numerous agencies, the negative consequences of inaccurate information may appear to be caused by the actions of one agency when in fact they stem from inaccurate information in databases maintained by another agency. The rules governing fusion centers should take account of this fact by ensuring that there are procedures for transferring petitions for redress from the agency where they are received to the agency that maintains the records that have generated the petition.[145] In addition, when error corrections are made, it is critical that they be disseminated to all databases containing the original erroneous information.

D. State Oversight

Fusion centers are designed to share information across state borders, but the primary responsibility for ensuring that fusion centers collect, access and share information responsibly belongs to the states themselves. States bear responsibility for safeguarding the rights of their residents, particularly when the threat to those rights comes from state-based institutions like fusion centers.[146]

First and foremost, states should require fusion centers to abide by state open government and privacy laws. Individual states often pass legislation more protective of privacy rights and more stringent with respect to public disclosure than similar federal statutes. Despite the fact that these laws, like the federal Privacy Act, generally contain limited exemptions for law enforcement agencies, there are a number of disturbing examples of federal authorities pressuring states to completely exempt fusion center and other anti-terrorism personnel from compliance with state privacy laws and other state laws governing the activities of law enforcement agencies.

> "... obsolete information increases the chances of innocent persons being stopped or detained during an encounter because of being misidentified as a watchlist identity."
>
> *DOJ Inspector General*

In Virginia, for example, state legislators introduced a bill to exempt the Virginia Fusion Center from state open government laws, reportedly at the behest of federal authorities.[147] The bill ultimately passed, but only after the scope of the exemption was narrowed to address the criticism of free press and civil liberties advocates.[148] Similar problems have been reported in California, where secret agreements between the San Francisco Police Department and the FBI apparently allowed San Francisco police officers participating in an FBI-led Joint Terrorism Task Force to conduct investigations without reasonable suspicion—in violation of local law. The existence of these agreements was even kept secret from the Police Commission, the body charged with overseeing police affairs.[149] In Oakland, local officers were apparently directed by the FBI to question Muslim-Americans pursuant to an agreement so secret that the FBI reportedly refused to provide a copy to the Oakland Police Department itself.[150]

These efforts raise civil liberties concerns and implicate questions of the proper allocation of power between the federal government and the states, particularly given the fact that the vast majority of fusion centers have shifted from an exclusive focus on terrorism to an "all-crimes" or "all-threats" approach. Moreover, federal efforts to circumvent state privacy and open government laws have the potential to undermine the democratic accountability of state governments.

Second, states should enact legislation specifically directed towards fusion center accountability and the protection of civil liberties. One component of such legislation would be the institutionalization of periodic audits or assessments of the fusion center's impact on privacy rights. These audits might be based on the Privacy Impact Assessments required for federal databases.[151] Commendably, some fusion centers have already adopted such auditing practices.[152] Another important feature of fusion center legislation would be the appointment of a privacy and civil liberties watchdog. Depending on the size and scope of the fusion center, this watchdog might range from a single individual to a committee composed of stakeholders including law enforcement representatives, members of the bar, representatives of public defenders organizations and civil liberties advocates. At least one state fusion center has a privacy oversight committee that includes civilian civil liberties advocates, although this committee is not mandated by statute.[153] Finally, fusion center legislation should include limits on the retention and use of data as well as other best-practices for safeguarding civil liberties.[154]

E. Federal Oversight

Because fusion centers are state and local entities that operate independently from one another, their missions, tactics, resources and operating standards vary significantly. In some respects, the protean and decentralized nature of fusion centers is a source of strength, because each fusion center has the institutional knowledge and flexibility necessary to adapt and respond to the unique demands of its jurisdiction. The decentralized nature of fusion centers, however, may carry significant costs in the area of civil liberties. In an environment where partners are sharing data with serious civil liberties implications, the bad practices of one partner can render all partners complicit in abuses.[155]

For this reason, the federal government should play an active role in ensuring that fusion centers respect civil liberties. The DHS requirement that fusion centers certify they have privacy and civil liberties protections consistent with the Privacy Guidelines for the Information Sharing Environment in order to receive federal funding is an excellent first step. But the federal government has both the resources and institutional experience to do more. Given the federal government's constitutional responsibilities and the fundamental role that fusion centers are expected to play in federal national security policy, the federal government has a duty to ensure that fusion centers respect civil liberties. Moreover, because state and local law enforcement officers often engage in counterterrorism work at the behest of the federal government and with the support of significant federal funding, the federal government has a responsibility to ensure that proper constitutional safeguards and proper training programs are in place. Indeed, many fusion centers themselves have expressed the desire for greater federal guidance and coordination.[156]

First, in order to more effectively monitor compliance with civil liberties rules, the DHS and DOJ should coordinate to establish a federal audit function. These agencies should audit fusion centers on a periodic basis to ensure that they are in compliance with privacy and civil liberties rules.

Second, federal funding for fusion centers is currently intermingled with funding streams for general state and local law enforcement activity. In order to increase accountability and transparency, federal funds that are directed towards fusion centers should be separate and distinguishable from general law enforcement funds.

Third, all federal funding for state fusion centers should be predicated on demonstrated civil liberties best practices. Compliance with federal and state civil liberties guidelines should be assessed by periodic audits, and funding should be contingent on successful completion of the audit process. Compliance should be measured not by the strength of the civil liberties policies as written, but by their efficacy in practice. In addition, federal funds for fusion centers should also be conditioned upon states enacting legislation that provides for periodic state audits of fusion centers and subjects fusion centers to state privacy and open government laws.

Fourth, federal agencies should use their expertise and resources to provide fusion center personnel with additional training by qualified trainers regarding civil liberties and privacy issues. They should also work together to expand upon existing privacy and civil liberties guidelines. The guidance currently available discusses privacy and civil liberties at a high level,[157] as many commentators both within and without the government have noted, but does not provide practical instruction.[158] Civil liberties guidance should translate principles into practical advice and address operational concerns regarding data collection, retention and dissemination. For example, future training programs and guidance should present specific hypothetical situations that demonstrate the complexities of these decisions and offer insight to fusion center personnel on the specific conduct that does or does not provide the appropriate basis for a suspicious activity report, investigation or information-sharing with other law enforcement and intelligence entities.

Finally, Congress should commission a study by an independent group—perhaps the Government Accountability Office or Congressional Research Service—to evaluate the performance and sustainability of fusion centers and their impact on civil liberties.

…because state and local law enforcement officers often engage in counterterrorism work at the behest of the federal government and with the support of significant federal funding, the federal government has a responsibility to ensure that proper constitutional safeguards and proper training programs are in place.

VI. FUSION CENTER RECOMMENDATIONS

A. Data Collection Recommendations

Profiling and Data Collection:

1. Fusion centers should establish guidelines that clearly prohibit their personnel from engaging in racial and religious profiling. In determining when to collect and share information, the guidelines should focus on behaviors that raise a reasonable suspicion of criminal activity or evidence of wrongdoing. Race, national origin, ethnicity and religious belief should not be considered as factors that create suspicion, and should only be used as factors in alerts if they are included as part of a specific suspect's description. The guidelines should also specify that political association and the peaceful exercise of constitutionally protected rights may not be relied upon as factors that create suspicion of wrongdoing.
2. Fusion centers should ensure that their personnel are properly trained on the constitutional rights of free expression, assembly, religion and equal protection.
3. Fusion centers should ensure that individuals who instruct their personnel on intelligence analysis and terrorist threats are competent and well-qualified, and have themselves been trained in the constitutional rights discussed above.

Suspicious Activity Reporting:

4. Fusion centers should carefully analyze suspicious activity reports to determine whether there is a likely connection to criminal or terrorist activity, and should only retain and disseminate suspicious activity reports if they demonstrate reasonable suspicion of such activity.

B. Data Storage and Use Recommendations

Data Minimization:

1. Fusion centers should periodically review the information in their files to determine whether that information is accurate and of continuing relevance. Data retained by fusion centers should be purged five years after its collection unless its continued relevance can be demonstrated.
2. Fusion centers should collect and retain only the minimum amount of personally identifiable information necessary to

serve their law enforcement purposes. Fusion centers should only use this personally identifiable information for the law enforcement purpose for which the information was collected.

Audit Logs:

3. Fusion centers should ensure that immutable audit logs track all database activity.
4. Independent auditors should review fusion center audit logs every two years and publish reports describing the use of fusion center databases and any abuses or unauthorized access.

Data Mining:

5. As set forth in The Constitution Project's report *Principles for Government Data Mining*, fusion centers should act carefully to ensure that constitutional rights and values are respected if they engage in data mining or if the information in their databases is used for data mining by other government entities.

Private Sector Partnerships:

6. Fusion centers should carefully limit the information that they disseminate to private sector entities. Personally identifiable information should only be shared with private sector entities to the extent necessary to carry out legitimate law enforcement or national security functions.
7. Fusion centers should not collect information from private sector sources that they would otherwise be restricted by law from obtaining.

C. Accountability Recommendations

Mission Statement:

1. Fusion centers should develop clear mission statements that express their purpose and the criteria upon which their performance can be evaluated. Further study of the proper goals and methods of fusion centers would be useful for the development of these mission statements and accountability criteria.

Transparency:

2. Fusion centers should engage local communities by publicly explaining their mission, budget and staffing.
3. Fusion centers should publicize their privacy policies and the results of their compliance audits.

Redress:

4. Fusion Centers should be equipped with effective redress processes by which individuals can, if necessary, review and correct or challenge information possessed by a fusion center.
5. Redress processes should provide for the availability, where appropriate, for review of complaints by an independent, security-cleared arbiter, with a right of appeal to a higher-level independent state or local authority.
6. Redress processes should be well-publicized.
7. Redress processes should ensure that corrections are disseminated across databases.

State Oversight:

8. State governments should ensure that fusion centers are subject to state privacy, open government and anti-domestic surveillance laws, regardless of federal pressure to the contrary.
9. States should require periodic audits of fusion center privacy practices and that fusion centers privacy practices be subject to review by an oversight board or officer.

Federal Guidance and Oversight:

10. The federal government should regularly audit fusion centers for compliance with privacy guidelines and report its findings to the appropriate congressional committee of jurisdiction.
11. Federal funding for fusion centers should be separate and distinguishable from general funding for state and local law enforcement activities.
12. Federal funding for fusion centers should be contingent upon:
    a. States enacting legislation that (i) subjects fusion centers to periodic state audits of their civil liberties practices, and (ii) requires fusion centers to comply with state privacy, open government and anti-domestic surveillance laws; and
    b. Continued compliance with federal and state privacy and civil liberties guidelines, as assessed by periodic federal audits.
13. The federal government should provide fusion centers with increased civil liberties training and detailed and specific guidance regarding the practical implementation of privacy protections.
14. Congress, DHS or DOJ should commission an independent study of fusion center performance, sustainability and impact upon civil liberties.

ENDNOTES

1. *See generally* National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report (2004); *DHS Intelligence Programs and the Effectiveness of State and Local Fusion Centers, Hearing Before the Subcomm. on Homeland Sec. of the House Comm. on Appropriations*, 111th Cong. (Mar. 4, 2010).

2. U.S. Department of Homeland Security, Fusion Center Locations and Contact Information, http://www.dhs.gov/files/programs/gc_1301685827335.shtm.

3. *See, e.g.*, Homeland Security Policy Institute, *Counterterrorism Intelligence: Fusion Center Perspectives*, Counterterrorism Intelligence Survey Research, June 2012, http://www.gwumc.edu/hspi/policy/HSPI%20Counterterrorism%20Intelligence%20-%20Fusion%20Center%20Perspectives%206-26-12.pdf (conducted survey study "to evaluate how well the fusion centers are fulfilling their mandate…[and] to extract and build upon lessons of practitioners." Study concluded fusion centers fail to effectively translate collected information into intelligence through analysis and threat assessment and calls for "increased investments in the analytical and critical thinking skills of those working in the centers").

4. *See* John Rollins, Cong. Research Serv., Fusion Centers: Issues and Options for Congress 30 (Jan. 18, 2008) (describing fusion center officials' remarks that "their staff could spend all day, every day reviewing all the information posted on [database] systems, and still not be confident they had seen all relevant and/or unique data").

5. U.S. Gov't Accountability Off., Information Sharing: Federal Agencies Are Helping Fusion Centers Build and Sustain Capabilities and Protect Privacy, but Could Better Measure Results 30-31 (Sept. 2010) ("GAO Report").

6. Federal legislation defines "fusion center" as "a collaborative effort of 2 or more Federal, State, local, or tribal government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity." Implementing Recommendations of the 9/11 Commission Act of 2007, 6 U.S.C. § 124h(j)(1) (2006).

7. Rollins, *supra* note 4, at 19-20.

8. *DHS Intelligence Programs, supra* note 1 (statement of David E. Price, Rep. of N.C.).

9. Rollins, *supra* note 4, at 21-22.

10. *Id.*

11. *Id.* at 29-30; Robert O'Harrow, Jr., *Centers Tap Into Personal Databases*, Wash. Post, Apr. 2, 2008, at A1, http://washingtonpost.com/wp-dyn/content/article/2008/04/01/AR2008040103049.html.

12. O'Harrow, Jr., *supra* note 11.

13. U.S. Dep't of Just., Bureau of Just. Assistance, Fusion Center Guidelines: Developing & Sharing Information and Intelligence in a New Era C-1 (Aug. 2006) ("Fusion Center Guidelines").

14. *See, e.g.*, Jason Hancock, *Iowa's Intelligence Fusion Center "Connects the Dots,"* Iowa Indep., July 29, 2008, http://iowaindependent.com/2983/iowas-intelligence-fusion-center-connects-the-dots.

15. U.S. Department of Homeland Security, Fusion Center Locations and Contact Information, http://www.dhs.gov/files/programs/gc_1301685827335.shtm. Fusion centers have proliferated rapidly in recent years; nearly half of the fusion centers currently recognized by DHS and DOJ were created after 2006. *The Future of Fusion Centers: Potential Promise and Dangers: Hearing Before the Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment of the H. Comm. on Homeland Sec.*, 111th Cong. 111-15 (Apr. 1, 2009) (statement of Robert Riegle, State & Local Program Office, Office of Intelligence & Analysis).

16. Rollins, *supra* note 4, at 34.

17. *Id.* at 47.

18. *Id.* at 35-36; American Civil Liberties Union, Policing Free Speech: Police Surveillance and Obstruction of First Amendment-Protected Activity 10-11 (June 29, 2010).

19. *See, e.g.*, 2010 National Security Strategy 20, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (calling on the federal government to "continue to integrate and leverage state and major urban area fusion

centers that have the capability to share classified information; establish a national framework for reporting suspicious activity; and implement an integrated approach to our counterterrorism information systems . . . We are improving information sharing and cooperation by linking networks to facilitate Federal, state, and local capabilities to seamlessly exchange messages and information, conduct searches, and collaborate.").

20. Janet Napolitano, Secretary, Dep't of Homeland Sec., Remarks to the National Fusion Center Conference in Kansas City, Mo. (Mar. 11, 2009) (transcript available at http://www.dhs.gov/ynews/speeches/sp_1236975404263.shtm).

21. U.S. Dep't of Homeland Sec., Off. of Inspector Gen., DHS' Role in State and Local Fusion Centers is Evolving 7 (Dec. 2008), http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_09-12_Dec08.pdf.

22. Rollins, *supra* note 4, at 34.

23. *DHS Intelligence Programs, supra* note 1 (Mar. 4, 2010) (statement of Capt. William Harris, Del. St. Police) (summarizing the extent of DHS assistance).

24. Department of Homeland Security, State and Major Urban Area Fusion Centers, http://www.dhs.gov/files/programs/gc_1156877184684.shtm.

25. Fusion Center Guidelines, *supra* note 13; Global Just. Info. Sharing Initiative, Baseline Capabilities for State and Major Urban Area Fusion Centers: A Supplement to the Fusion Center Guidelines (Sept. 2008) ("Baseline Capabilities"), http://www.it.ojp.gov/documents/baselinecapabilitiesa.pdf.

26. Rollins, *supra* note 4, at 26.

27. Information Sharing Environment, What is ISE?, http://www.ise.gov/what-ise.

28. *See* Rollins, *supra* note 4, at 27, 29-30 (explaining that fusion centers receive information from "a plethora of competing federal information sharing systems. . . . including, but not limited to, the HSIN and its sister systems HSIN-Secret and HSDN, Law Enforcement Online (LEO), Federal Protective Service (FPS) portal, Regional Information Sharing Service (RISS), among others"); *see also* Spencer S. Hsu and Robert O'Harrow Jr., *DHS to Replace 'Duplicative' Anti-Terrorism Data Network*, Wash. Post, Jan. 18, 2008.

29. Rollins, *supra* note 4, at 30.

30. U.S. Dep't of Homeland Sec., Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment (Dec. 2006) ("ISE Privacy Guidelines"), http://ise.gov/sites/default/files/PrivacyGuidelines20061204.pdf.

31. *See* Harley Geiger, *Fusion Centers Get New Privacy Orders Via DHS Grants*, Ctr. for Democracy & Tech., Dec. 15, 2009, http://www.cdt.org/blogs/harley-geiger/fusion-centers-get-new-privacy-orders-dhs-grants.

32. Privacy Act of 1974; Department of Homeland Security Office of Operations Coordination and Planning—003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion System of Records, 75 Fed. Reg. 69,689 (Nov. 15, 2010).

33. *See, e.g.*, Electronic Privacy Information Center, Comments to the Department of Homeland Security: "Systems of Records Notice" DHS-2010-0052 and "Notice of Proposed Rulemaking" DHS-2010-0053 (Dec. 15, 2010); Letter from the Yale L. Sch. Media Freedom and Information Access Practicum to Mary Ellen Callahan, Chief Privacy Officer, Dep't of Homeland Sec. (Dec. 15, 2010).

34. Constitutional concerns based on rights of privacy and freedom from unwarranted search and seizure are discussed in Section III.B.1., *infra.*

35. *See, e.g., Lamont v. Postmaster General*, 381 U.S. 301, 306-07 (1965) (invalidating a Federal law requiring recipients of "communist political propaganda" to specifically authorize the delivery of each such piece of mail); *see also* Stephen H. Sachs, Review of Maryland State Police Covert Surveillance of Anti-Death Penalty and Anti-War Groups From March 2005 to May 2006 63-66 (2008); The Constitution Project, Principles for Government Data Mining: Preserving Civil Liberties in the Information Age 14-15 (2010), http://www.constitutionproject.org/pdf/DataMiningPublication.pdf.

36. *See NAACP v. Alabama*, 357 U.S. 449, 462 (1958) ("Inviolability of privacy in group association may in many circumstances be indispensable to the freedom of association, particularly where a group espouses dissident beliefs."); *Riggs v. City of Albuquerque*, 916 F.2d 582 (10th Cir. 1990); *Presbyterian Church v. United States*, 870 F.2d 518 (9th Cir. 1989); *Alliance to End Repression v. City of Chicago*, 627 F. Supp. 1044 (N.D. Ill. 1985); *cf. Boy Scouts of America v. Dale*, 530 U.S. 640, 648 (2000) (explaining that

infringement of First Amendment rights "may take many forms, one of which is intrusion into the internal structure or affairs of an association") (internal quotations omitted).

37. U.S. Const. amend. XIV, § 1.

38. *See* Info. Sharing Envir., Civil Rights and Civil Liberties Protection: Guidance 8 (Aug. 11, 2008) ("Civil Rights Guidance"), http://www.ise.gov/sites/default/files/CR-CL_Guidance_08112008.pdf.

39. *Whren v. United States*, 517 U.S. 806, 813 (1996); *United States v. Armstrong*, 517 U.S. 456, 464 (1996); *see also* Principles for Government Data Mining, *supra* note 35, at 15.

40. Civil Rights Guidance, *supra* note 38, at 8.

41. *See generally* David Rittgers, *We're All Terrorists Now*, CATO @ Liberty, Feb. 2, 2011, http://www.cato-at-liberty.org/we%E2%80%99re-all-terrorists-now/; Associated Press, *FBI pulls flawed training aids related to Muslims*, Huffington Post, March 30, 2012, http://www.huffingtonpost.com/huff-wires/20120330/us-fbi-training/.

42. North Central Texas Fusion System, *Prevention Awareness Bulletin*, Feb. 19, 2009, http://aclu-wa.org/sites/default/files/attachments/North%20Central%20Texas%20Fusion %20System.pdf.

43. *See* T.J. Greaney, *"Fusion Center" Data Draws Fire Over Assertions: Politics, Banners Seen As Suspect,* Columbia Daily Trib., Mar. 14, 2009, http://www.columbiatribune.com/news/2009/mar/14/fusion-center-data-draws-fire-over-assertions/.

44. Jeff Woods, *ACLU Calls Anti-Terrorism Agency Map Placement "Disturbing"*, Nashville City Paper, Dec. 21, 2010, http://nashvillecitypaper.com/content/city-news/aclu-calls-anti-terrorism-agency-map-placement-disturbing.

45. Commonwealth of Virginia, Dep't of State Police, Virginia Fusion Center, 2009 Virginia Terrorism Threat Assessment 9, 17 (Mar. 2009), http://www.rawstory.com/images/other/vafusioncenterterrorassessment.pdf; *see also* ACLU, *Fusion Center Declares Nation's Oldest Universities Possible Terrorist Threat,* Apr. 6, 2009, http://www.aclu.org/technology-and-liberty/fusion-center-declares-nation-s-oldest-universities-possible-terrorist-threat.

46. Nick Madigan, *Spying Uncovered: Documents Show State Police Monitored Peace and Anti-Death Penalty Groups,* Baltimore Sun, July 18, 2008, http://www.baltimoresun.com/news/maryland/bal-te.md.spy18jul18,0,5659230.story?page=1; Lisa Rein and Josh White, *More Groups Than Thought Monitored in Police Spying,* Wash. Post, Jan. 4, 2009; *see generally* Sachs, *supra* note 35.

47. Marc Levy, *Pennsylvania Protest Reports: Governor 'Appalled,' Shuts Down Practice*, Huffington Post, Sept. 15, 2010, http://www.huffingtonpost.com/2010/09/15/pennsylvania-protest-repo_n_717393.html; Philip Leggiere, *Fusion Centers: Tough Tightrope,* HSToday.us, Jan. 3, 2011, http://www.hstoday.us/channels/dhs/single-article-page/fusion-centers-tough-tightrope/5f5b0dba05b0b05de6e08306d5932892.html.

48. G.W. Schulz, Andrew Becker, Daniel Zwerdling, *Mall of America Visitors Unknowingly End up in Counterterrorism Reports,* Center for Investigative Reporting, Sept. 7, 2011, http://americaswarwithin.org/articles/2011/09/07/mall-america-visitors-unknowingly-end-counterterrorism-reports; *Under Suspicion at the Mall of America,* National Public Radio, Sept. 7, 2011, http://www.npr.org/2011/09/07/140234451/under-suspicion-at-the-mall-of-america.

49. Schulz, et al., *supra* note 48.

50. Megan Stalcup and Joshua Craze, *How We Train Our Cops to Fear Islam,* Wash. Monthly, Mar./Apr. 2011, http://www.washingtonmonthly.com/features/2011/1103.stalcup-craze.html.

51. Dana Priest and William M. Arkin, *Monitoring America*, Wash. Post, Dec. 20, 2010, http://projects.washingtonpost.com/top-secret-america/articles/monitoring-america/.

52. *Id.*

53. *Id.*

54. Stalcup and Craze, *supra* note 50.

55. *See, e.g., id;* Priest and Arkin, *supra* note 51; Samuel J. Rascoff, *The Law of Homegrown (Counter) Terrorism,* 88 Tex. L. Rev. 1715, 1738 n.106 (citing Tom R. Tyler, *et al., Legitimacy and Deterrence Effects in Counter-Terrorism Policing: A Study of Muslim Americans,* 44 Law & Soc'y Rev. (2010) for the proposition that "fair police procedures influence the perceived legitimacy of law enforcement and the willingness of people to cooperate with them"); Spencer Ackerman, *Obama Orders Government to Clean Up Terror Training,* Wired.com, Nov. 29, 2011, http://www.wired.com/dangerroom/2011/11/obama-islamophobia-review/.

56. *See* Jerome Bjelopera, Cong. Research Serv., Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress (Dec. 28, 2011).

57. *Olmstead v. United States,* 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting); *see* Principles for Government Data Mining, *supra* note 35, at 12; Nat'l Res. Council, Protecting Individual Privacy in the Struggle Against Terrorists 27-29 (Nat'l Acad. Press 2008) (explaining that "privacy may refer to protecting the confidentiality of information; enabling a sense of autonomy, independence, and freedom to foster creativity; wanting to be left alone; or establishing enough trust that individuals in a given community are willing to disclose data under the assumption that they will not be misused").

58. Protecting Individual Privacy, *supra* note 57, at 27.

59. National Conference of State Legislatures, Privacy Protections in State Constitutions, http://www.ncsl.org/default.aspx?tabid=13467.

60. 5 U.S.C. § 552a (2011).

61. *See* Electronic Privacy Information Center, The Privacy Act of 1974, http://epic.org/privacy/1974act/.

62. 18 U.S.C. § 2510 *et seq.* (2011).

63. 15 U.S.C. § 1681 *et seq.* (2011).

64. 28 C.F.R. § 23.20(a) (emphasis added).

65. 28 C.F.R. § 23.20(c).

66. *Terry v. Ohio*, 392 U.S. 1, 21 (1968).

67. *See* Bjelopera, *supra* note 56, at 8-11.

68. Information Sharing Environment Functional Standard Suspicious Activity Reporting Version 1.5, at 9, http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-dhswide-sar-ise-appendix.pdf; *see also* Priest and Arkin, *supra* note 51.

69. U.S. Department of Justice, Bureau of Justice Assistance, Nationwide SAR Initiative Annual Report 2010 12 (2011).

70. Functional Standard 1.5, *supra* note 68, at 7 (emphasis in original).

71. Siobhan Gorman, *LAPD Terror Tip Plan May Serve as Model,* Wall St. J., Apr. 15, 2008, at A3.

72. Findings and Recommendations of the Suspicious Activity Report Support and Implementation Project (SAR Project Report), June 2008 at 43-44; Functional Standard 1.5, *supra* note 68, at 29; Bjelopera, *supra* note 56, at 8.

73. Mike German and Jay Stanley, *Fusion Center Update,* American Civil Liberties Union, July 2008, at 2, http://www.aclu.org/pdfs/privacy/fusion_update_20080729.pdf.

74. *See* Letter from American Civil Liberties Union, Council on American-Islamic Relations, Asian Pacific American Legal Center, Coalition for Human Immigrant Rights of Los Angeles, South Asian Network & Sikh American Asian Legal Defense Fund to LAPD Chief Beck and Deputy Chief Dowling (Mar. 2, 2012), http://www.aclu-sc.org/lapd-should-halt-destructive-suspicious-activity-reporting-policies/.

75. Functional Standard 1.5, *supra* note 68, at 8-10; *see also* Priest and Arkin, *supra* note 51.

76. Priest and Arkin, *supra* note 51.

77. *From the Mall of America Reports: Saleem and Najam Qureshi,* Center for Investigative Reporting, Sept. 7, 2011, http://americaswarwithin.org/articles/2011/09/07/mall-america-reports-saleem-and-najam-qureshi.

78. *Terry v. Ohio,* 392 U.S. 1, 21 (1968).

79. *Maryland v. Buie,* 494 U.S. 325, 337 (1990).

80. *Arizona v. Johnson*, 555 U.S. 323, 323 (2009).

81. O'Harrow, Jr., *supra* note 11.

82. *See, e.g.,* Federal Trade Commission, Fair Information Practice Principles, http://www.ftc.gov/reports/privacy3/fairinfo.shtm; *see also* White House, Consumer Data Privacy in a Networked World: A Framework For Protecting Privacy and Promoting Innovation in the Global Digital Economy (2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

83. *See* The Constitution Project, Guidelines for Public Video Surveillance: A Guide to Protecting Communities and Preserving Civil Liberties 12 (2006) (describing the Fair Information Practice Principles in further detail), http://www.constitutionproject.org/pdf/Video_Surveillance_Guidelines_Report_w_Model_Legislation4.pdf.

84. Memorandum from Clay Johnson III, Deputy Director for Mgmt., Off. of Mgmt. & Budget, to the Heads of Executive Departments and Agencies regarding Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 2007), at 1 n.1, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.

85. *See* Gov't Accountability Office, Homeland Security: Continuing Attention to Privacy Concerns is Needed as Programs are Developed (Statement of Linda D. Koontz, Director, Info. Mgmt Issues) 1 n.1 (March 21, 2007), http://www.gao.gov/new.items/d07630t.pdf.

86. *See* Guidelines for Public Video Surveillance, *supra* note 83, at 12; *see also* Fair Information Practice Principles, *supra* note 82; Memorandum from Hugo Teufel III, Chief Privacy Officer, U.S. Dep't of Homeland Sec., regarding The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security (Dec. 29, 2008) ("DHS Memorandum No. 2008-01"), http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf (describing the Fair Information Practice Principles as a set of eight principles: Transparency; Individual Participation; Purpose Specification; Data Minimization; Use Limitation; Data Quality and Integrity; Security; and Accountability and Auditing).

87. 5 U.S.C. § 552a.

88. *See* Protecting Individual Privacy, *supra* note 57, at 156-59.

89. Fusion Center Guidelines, *supra* note 13, at 41-42.

90. *See*, e.g., Alabama Fusion Center, Privacy Policy Version 3.0, at Section A, http://www.nfcausa.org/files/DDF/AlabamaFusionCenterPrivacyPolicy.pdf; Texas Fusion Center, Privacy, Civil Rights, and Civil Liberties Policy (Revised 2010-11-30), at Section A.2, http://www.txdps.state.tx.us/docs/TxFCPrivacyPolicy113010.pdf; Minnesota Joint Analysis Center, Privacy Policy, at 6, 8, http://www.nfcausa.org/files/DDF/MNJACPrivacyPolicyApproved022311Final.pdf.

91. The DHS treats data minimization and use limitation as Fair Information Practice Principles. *See* DHS Memorandum No. 2008-01, *supra* note 86, at 4.

92. 28 C.F.R. § 23.20(a).

93. 28 C.F.R. § 232.0(h).

94. Markle Found., Nation at Risk: Policy Makers Need Better Information to Protect the Country 7 (March 2009).

95. 28 C.F.R. § 232.0(e).

96. Adena Schutzberg, *MetaCarta Users Tap Unstructured Data for New Geographic Uses,* Directions Mag., May 30, 2007, http://www.directionsmag.com/articles/ metacarta-users-tap-unstructured-data-for-new-geographic-uses/122889. State employees are not subject to the federal Freedom of Information Act, but would be subject to state law analogues.

97. *See* Continuing Attention to Privacy Concerns is Needed, *supra* note 85, at 13 (noting that "accountability was not ensured, as the agencies did not generally monitor usage of personal information from resellers; instead, they relied on end users to be responsible for their own behavior").

98. *See* Markle Found., Implementing a Trusted Information Sharing Environment: Using Immutable Audit Logs to Increase Security, Trust, and Accountability 1 (Feb. 2006).

99. In order to be effective, audit logs must be immutable. *Id.* at 2.

100. Implementing a Trusted Information Sharing Environment, *supra* note 98, at 1; Stewart Baker, *Realistic Privacy Protection in the Information Age*, Volokh Conspiracy, July 4, 2009, http://volokh.com/2010/07/04/realistic-privacy-protection-in-the-information-age/.

101. Implementing a Trusted Information Sharing Environment, *supra* note 98, at 3.

102. *Passport Files of Candidates Breached,* Associated Press, Mar. 21, 2008, http://www.msnbc.msn.com/id/23736254/ns/politics-decision_08/.

103. *See* Baker, *supra* note 100.

104. Continuing Attention to Privacy Concerns is Needed, *supra* note 85, at 18 (endorsing "the use of electronic audit logs that cannot be changed by individuals").

105. Implementing a Trusted Information Sharing Environment, *supra* note 98.

106. *See* Baker, *supra* note 100.

107. *See* Nationwide SAR Initiative Annual Report 2010, *supra* note 69, at 6.

108. *See* Continuing Attention to Privacy Concerns is Needed, *supra* note 85, at 8; Principles for Government Data Mining, *supra* note 35, at 7.

109. Principles for Government Data Mining, *supra* note 35, at 8-11.

110. *Id.* at 11.

111. *Id.* at 12-16.

112. Principles for Government Data Mining considers in further detail the issues raised by data mining and provides a set of data mining best practices. *Supra* note 35.

113. G.W. Schulz, *What's the Minnesota Joint Analysis Center?*, MinnPost.com, Sept. 1, 2009, http://www.minnpost.com/stories/2009/09/01/11232/whats_the_minnesota_ joint_ analysis_center.

114. *See* Am. Civil Liberties Union, What's Wrong With Fusion Centers 12 (Dec. 2007).

115. As the Congressional Research Service puts it, "a comprehensive understanding of the risks to the state/region is impossible to attain without a viable relationship and consistent information flow between the center and the private sector entities within the center's jurisdiction . . . ." Rollins, *supra* note 4, at 54.

116. Fusion Center Guidelines, *supra* note 13, at 17.

117. Baseline Capabilities, *supra* note 25, at 15.

118. Fusion Center Guidelines, *supra* note 13, at 18, 29-30.

119. Levy, *supra* note 47; Leggiere, supra note 47.

120. *See* What's Wrong With Fusion Centers, *supra* note 114, at 13; *see also* Rollins, *supra* note 4, at 56 ("Some are concerned that as fusion centers and the IC agencies codify relationships, there is increased potential for misuse of private sector data.").

121. Fusion Center Guidelines, *supra* note 13, at 31 (discussing Non-Disclosure Agreements with private entities). It appears that such disclosures have occurred in the past. *See* U.S. Gov't Accountability Off., Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information 5-6 (March 17, 2006) ("DHS said that sensitive but unclassified information disseminated to its state and local partners had, on occasion, been posted to public Internet sites or otherwise compromised, potentially revealing possible vulnerabilities to business competitors.").

122. *See, e.g.*, Fair Information Practice Principles, *supra* note 82.

123. *See* Protecting Individual Privacy, *supra* note 57, at 184.

124. Schutzberg, *supra* note 96.

125. *See, e.g.*, Fusion Center Perspectives, *supra* note 3.

126. *See, e.g.*, Rollins, *supra* note 4, at 84.

127. Louis D. Brandeis, *What Publicity Can Do*, Harper's Weekly, Dec. 20, 1913.

128. *See* Section V.D, *infra.*

129. *See, e.g.*, Hancock, *supra* note 14; What's Wrong With Fusion Centers, *supra* note 114, at 7; Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, U.S. Senate, 94th Cong., Final Report on Supplemental Detailed Staff Reports on Intelligence Activities and the Rights of Americans (Book III), S. Rep. No. 94-755, at 10 (1976).

130. *See* Stalcup and Craze, *supra* note 50; Priest and Arkin, *supra* note 51; Rascoff, supra note 55.

131. *See, e.g.*, Fusion Center Guidelines, *supra* note 13, at 41; Baseline Capabilities, *supra* note 25, at 26.

132. *See, e.g.*, Ala. Privacy Policy, *supra* note 90; Tex. Privacy Policy, *supra* note 90; Minn. Privacy Policy, supra note 90; Virginia Fusion Center, Virginia Fusion Center (VFC) Privacy Policy, http://www.nfcausa.org/ (follow "Privacy Policies" hyperlink; then follow "Virginia Fusion Center" hyperlink).

133. *See, e.g.,* Desyl L. Peterson, Data Practices Audit Report for the Minnesota Joint Analysis Center (Jan. 29, 2010); John J. Wilson, Data Compliance Audit Report for the Minnesota Joint Analysis Center (June 1, 2010).

134. *The Future of Fusion Centers: Potential Promise and Dangers: Hearing Before the Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment of the H. Comm. on*

Homeland Sec., 111th Cong. 111-15 (Apr. 1, 2009) (testimony of David Gersten, Deputy Director for Programs and Compliance, Off. for Civ. Rts. & Civ. Liberties, U.S. Dep't of Homeland Sec.) ("I think we should offer redress. The organizations involved in fusion centers should be accountable to provide information if they have accessed information or somehow been privy to information about a specific person . . . .").

135. *See* Fair Information Practice Principles, *supra* note 82 (discussing the importance of access and participation).

136. *See* U.S. Dep't of Justice, Office of the Inspector General, Follow-up Audit of the Terrorist Screening Center i (Sept. 2007) (explaining that all U.S. terrorist watch lists are integrated and "assist in the screening of individuals who, for example, apply for a visa, attempt to enter the United States through a port-of-entry, attempt to travel internationally on a commercial airline, or are stopped by a local law enforcement officer on a traffic violation").

137. *See* Follow-up Audit of the Terrorist Screening Center, *supra* note 136, at i, iii, xi-xviii, 12-43; *see generally* The Constitution Project, Promoting Accuracy and Fairness in the Use of Government Watch Lists (2007), http://www.constitutionproject.org/pdf/53.pdf.

138. *See* Follow-up Audit of the Terrorist Screening Center, *supra* note 136, at iii.

139. *See, e.g.*, Baseline Capabilities, *supra* note 25, at 29-30.

140. *See, e.g.*, Ala. Privacy Policy, *supra* note 90, at 10-11; Tex. Privacy Policy, *supra* note 90, at 11-13.

141. *Id.*

142. *Id.*

143. Promoting Accuracy and Fairness in the Use of Government Watch Lists, *supra* note 137, at 32-40.

144. *See id.* at 37-38.

145. *See* Info. Sharing Envir., Key Issues Guidance A3-A4 (Feb. 11, 2008) for a discussion of this problem; *see also* Koontz, *supra* note 85, at 4-5.

146. *See* Rollins, *supra* note 4, at 84 ("There were a number of legal issues discovered in the course of research. Because they involve state law, there is likely no federal remedy . . . .").

147. Richard Quinn, *Secrecy Bill for State Anti-Terror Agency Has Some Crying Foul*, Virginian-Pilot (Norfolk), Feb. 18, 2008, http://hamptonroads.com/2008/02/secrecy-bill-state-antiterror-agency-has-some-crying-foul; Letter from Marc Rotenberg, Exec. Director, Elec. Privacy Info. Ctr., and John A. Verdi, Director, Elec. Privacy Info. Ctr. Open Gov't Project, to Va. State Sens. (Feb. 26, 2008), http://epic.org/privacy/fusion/Letter_to_Senate_02_25_08.pdf; *see generally* Electronic Privacy Information Center, EPIC v. Virginia Department of State Police: Fusion Center Secrecy Bill, http://epic.org/privacy/virginia_fusion.

148. *See* Richard Quinn, *Changes to Bill Limit Fusion Center's Exemptions to Subpoena*, Virginian-Pilot (Norfolk), Feb. 27, 2008, http://hamptonroads.com/2008/02/changes-bill-limit-fusion-centers-exemptions-subpoena.

149. Brent Begin, *SFPD Officers Working With FBI Given More Leeway to Gather Intelligence*, S.F. Examiner, Apr. 6, 2011, http://www.sfexaminer.com/local/2011/04/sfpd-officers-working-fbi-given-more-leeway-gather-intelligence.

150. Alan Schlosser and Veena Dubal, *Terrorism, Transparency and Oregon Law: Paying Too High a Price to Rejoin a Terror Task Force*, Oregonian (Portland), Apr. 5, 2011, http://www.oregonlive.com/opinion/index.ssf/2011/04/terrorism_transparency_and_ore.html.

151. *See* Continuing Attention to Privacy Concerns is Needed, *supra* note 85, at 6-7.

152. *See, e.g.*, Data Practices Audit Report for the Minnesota Joint Analysis Center, *supra* note 133; Data Compliance Audit Report for the Minnesota Joint Analysis Center, *supra* note 133.

153. *See* Dan Haugen, *You Don't Know MNJAC: Anti-Terror Fusion Center Grapples With Security Flaw, New Privacy Policy*, Minn. Indep. (St. Paul), July 28, 2008.

154. *See* Part IV and Part V Sections A and B, *supra.*

155. *See* Markle Found., Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment 67 (July 2006) (explaining, in the context of network security, that "[f]ederation . . . introduces a lowest-common-denominator risk: all partners are exposed to the least capable or least competent partner's security practices").

156. Rollins, *supra* note 4, at 41 (explaining that, while many fusion centers have found federal assistance programs, including training, "to have some utility[,] [o]thers believe that . . . a more sustained form of fusion center mentorship, based on a national fusion center strategy, would add additional value").

157. *See, e.g.*, Fusion Center Guidelines, *supra* note 13; Baseline Capabilities, *supra* note 25; *see also* ISE Privacy Guidelines, *supra* note 30.

158. *See, e.g.*, Continuing Attention to Privacy Concerns is Needed, *supra* note 85, at "Introduction" ("Recently issued privacy guidelines developed by the Office of the Director of National Intelligence provide only a high level framework for privacy protection."); *Privacy and Information Sharing for Counterterrorism, Hearing Before the President's Privacy and Civil Liberties Oversight Board*, George W. Bush White House (Dec. 5, 2006) (statement of James X. Dempsey, Policy Director, Ctr. for Democracy & Tech., Markle Found. Task Force on Nat'l Sec. in the Info. Age), http://www.cdt.org/testimon/20061205dempsey.pdf; Rollins, *supra* note 4, at 40 (noting that one regional fusion center director complained that the Fusion Center Guidelines "did not address technical aspects of operating a fusion center").

1200 18th Street, NW
Suite 1000
Washington, DC 20036
Tel 202.580.6920
Fax 202.580.6929
info@constitutionproject.org
www.constitutionproject.org