WHAT'S WRONG WITH FUSION CENTERS?

ACLU
AMERICAN CIVIL LIBERTIES UNION

WHAT'S WRONG WITH FUSION CENTERS?

Published December 2007

Michael German
Policy Counsel for National Security, ACLU Washington Legislative Office

Jay Stanley
Public Education Director, ACLU Technology and Liberty Program

Acknowledgements:

The authors would like to thank legal intern Anh-Thu Nguyen, of the University of Texas School of Law, for her invaluable assistance on this project. Her research and analysis contributed greatly to the content of this report.

ACLU NATIONAL OFFICE
125 Broad Street, 18th Fl.
New York, NY 10004-2400
(212) 549-2500
www.aclu.org

ACLU WASHINGTON LEGISLATIVE OFFICE
915 15th Street, NW
Washington, DC 20005
(202) 675-2325

Executive Summary

A new institution is emerging in American life: Fusion Centers. These state, local and regional institutions were originally created to improve the sharing of anti-terrorism intelligence among different state, local and federal law enforcement agencies. Though they developed independently and remain quite different from one another, for many the scope of their mission has quickly expanded—with the support and encouragement of the federal government—to cover "all crimes and all hazards." The types of information they seek for analysis has also broadened over time to include not just criminal intelligence, but public and private sector data, and participation in these centers has grown to include not just law enforcement, but other government entities, the military and even select members of the private sector.

These new fusion centers, over 40 of which have been established around the country, raise very serious privacy issues at a time when new technology, government powers and zeal in the "war on terrorism" are combining to threaten Americans' privacy at an unprecedented level.

Moreover, there are serious questions about whether data fusion is an effective means of preventing terrorism in the first place, and whether funding the development of these centers is a wise investment of finite public safety resources. Yet federal, state and local governments are increasing their investment in fusion centers without properly assessing whether they serve a necessary purpose.

There's nothing wrong with the government seeking to do a better job of properly sharing legitimately acquired information about law enforcement investigations—indeed, that is one of the things that 9/11 tragically showed is very much needed.

But in a democracy, the collection and sharing of intelligence information—especially information about American citizens and other residents—need to be carried out with the utmost care. That is because more and more, the amount of information available on each one of us is enough to assemble a very detailed portrait of our lives. And because security agencies are moving toward using such portraits to profile how "suspicious" we look.[1]

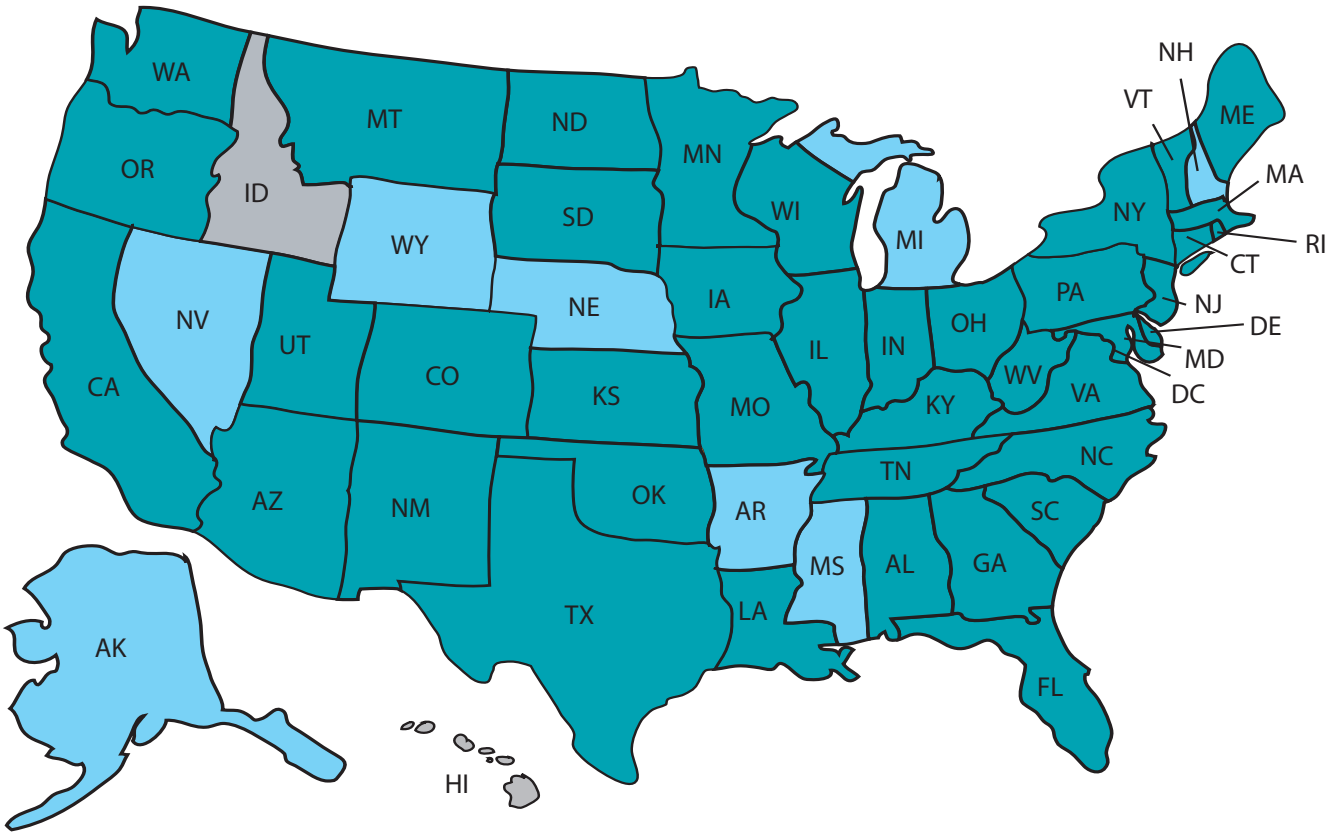
New institutions like fusion centers must be planned in a public, open manner, and their implications for privacy and other key values carefully thought out and debated. And like any powerful institution in a democracy, they must be constructed in a carefully bounded and limited manner with sufficient checks and balances to prevent abuse.

Unfortunately, the new fusion centers have not conformed to these vital requirements.

Since no two fusion centers are alike, it is difficult to make generalized statements about them. Clearly not all fusion centers are engaging in improper intelligence activities and not all fusion center operations raise civil liberties or privacy concerns. But some do, and the lack of a proper legal framework to regulate their activities is troublesome. This report is intended to serve as a primer that explains what fusion centers are, and how and why they were created. It details potential problems fusion centers present to the privacy and civil liberties of ordinary Americans, including:

- **Ambiguous Lines of Authority.** The participation of agencies from multiple jurisdictions in fusion centers allows the authorities to manipulate differences in federal, state and local laws to maximize information collection while evading accountability and oversight through the practice of "policy shopping."

FUSION CENTERS BY STATE



- **Private Sector Participation.** Fusion centers are incorporating private-sector corporations into the intelligence process, breaking down the arm's length relationship that protects the privacy of innocent Americans who are employees or customers of these companies, and increasing the risk of a data breach.

- **Military Participation.** Fusion centers are involving military personnel in law enforcement activities in troubling ways.

- **Data Fusion = Data Mining.** Federal fusion center guidelines encourage whole sale data collection and manipulation processes that threaten privacy.

- **Excessive Secrecy.** Fusion centers are hobbled by excessive secrecy, which limits public oversight, impairs their ability to acquire essential information and impedes their ability to fulfill their stated mission, bringing their ultimate value into doubt.

The lack of proper legal limits on the new fusion centers not only threatens to undermine fundamental American values, but also threatens to turn them into wasteful and misdirected bureaucracies that, like our federal security agencies before 9/11, won't succeed in their ultimate mission of stopping terrorism and other crime.

The information in this report provides a starting point from which individuals can begin to ask informed questions about the nature and scope of intelligence programs being conducted in their communities. The report concludes with a list of recommendations for Congress and state legislatures.

The American Civil Liberties Union has prepared this report based upon publicly available materials including congressional testimony, government reports, news articles and independent research. The ACLU attempted to contact every fusion center around the country in an informal survey regarding the level of private sector participation in the centers. Responses were as varied as the fusion centers themselves. Many either did not return calls or refused to provide information. Some were commendably open, willing to discuss their work and the legal authorities that govern their operations. We have also drawn on a report by the Congressional Research Service, which was able to interview a much larger number of fusion center personnel.[2]

INTRODUCTION

The origins of fusion centers... Federal government encouragement of fusion centers... A dark history of abuse of secret intelligence activities... Fusion centers today.

The origins of fusion centers

After 9/11, pressure grew for a larger state role in counterterrorism. At first, the FBI attempted to increase intelligence sharing with state and local law enforcement by expanding their Joint Terrorism Task Forces (JTTFs). But state and local officials continued to feel that the federal government was not sharing enough information to allow them to prevent terrorist attacks.[3]

This frustration with the JTTF system developed because while state and local law enforcement officers participating in JTTFs were given security clearances, secrecy rules prevented these officers from sharing any intelligence they acquired with other state and local colleagues who did not have such clearances. From a police department's point of view, it did them little good to send personnel into a task force only to have them cut off from and, for all practical purposes, no longer working for their departments. At least one city, Portland, Oregon, actually withdrew its officers from the Portland JTTF because of this problem.[4]

Another factor fueling the emergence of fusion centers was a trend within policing of moving away from traditional law enforcement methods toward what was dubbed "intelligence-led policing," or ILP. ILP focuses on the gathering and analysis of "intelligence" in the pursuit of proactive strategies "geared toward crime control and quality of life issues."[5] One law enforcement official described ILP as policing that is "robust enough" to resist "terrorism as well as crime and disorder."[6]

Intelligence fusion centers grew in popularity among state and local law enforcement officers as they sought to establish a role in defending homeland security by developing their own intelligence capabilities. These centers evolved largely independently of one another, beginning in about 2003, and were individually tailored to meet local and regional needs.

This growth took place in the absence of any legal framework for regulating fusion centers' activities. This lack of regulation quickly led to "mission creep," in which fusion centers originally justified as anti-terrorism initiatives rapidly drifted toward an "all-crimes, all-hazards" policy "flexible enough for use in all emergencies."[7] The leadership at some fusion centers has admitted that they switched to an "all-hazards" approach so they could apply for a broader range of grants, and because

> it was impossible to create 'buy in' amongst local law enforcement agencies and other public sectors if a fusion center was solely focused on counterterrorism, as the center's partners often didn't feel threatened by terrorism, nor did they think that their community would produce would-be terrorists.[8]

This expansion of the articulated mission of fusion centers reflects an evolving search for purpose, bounded on one side by the need not to duplicate the mission of existing insti-

tutions such as federal agencies and state Emergency Operations Centers, and on the other by the desire to do something that is actually useful.

Federal encouragement of the growth of fusion centers

As fusion centers proliferated, national efforts at bolstering, defining and standardizing these institutions on the part of governors and the federal government began to intensify.[9] The federal government began providing facilities, manpower and financial resources to fuel the growth of these state and local intelligence centers. In 2006, the departments of Justice and Homeland Security produced a report, "Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era," which outlined the federal government's vision for the centers, and sought to encourage and systematize their growth. "Intelligence sharing among states and jurisdictions will become seamless and efficient when each fusion center uses a common set of guidelines," the agencies proclaimed.[10]

The Guidelines defined a fusion center as a "collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity."[11] These goals are laudable and appropriate for any law enforcement intelligence operation, as we all want the police to be able to effectively protect us from criminals and terrorists. But the federal government intends for fusion centers to broaden their sources of data "beyond criminal intelligence, to include federal intelligence as well as public and private sector data."[12]

A dark history of abuse of secret intelligence powers

Expanding the scope of an intelligence agency's mission in that way, particularly when done in secret, is an invitation to abuse. And there is a long, nasty history of abuse surrounding vaguely defined, pro-active "intelligence" as carried out by domestic law enforcement agencies at the local, state and federal level. Law enforcement personnel and agencies have actively joined with corporations to track, surveil and harass the labor, anti-war, civil rights and other movements pushing for social and political change.

Urban police forces long maintained political intelligence units (also known as Anti-Subversive Squads, or Red Squads), which spied upon and sabotaged numerous peaceful groups—often in utterly illegal ways—throughout the twentieth century. For its part, the FBI ran a domestic intelligence/counterintelligence program called COINTELPRO that quickly grew from a legitimate effort to protect national security into an effort to suppress political dissent through illegal activities. Frequent targets were groups that criticized the FBI itself. The Senate panel that investigated COINTELPRO (the "Church Committee") in the 1970s found that a combination of factors led law enforcers to become law breakers. But the crucial factor was their easy access to damaging personal information as a result of the unrestrained collection of domestic intelligence.[13]

The Church Committee found that part of the problem with COINTELPRO was that no one outside the FBI was ever supposed to know it existed.[14] No one could object to activities they weren't aware of and, as investigators found, "the absence of disapproval" was "interpreted by the Bureau as sufficient authorization to continue an activity."[15] Secrecy created a haven from the public eye where abuse could flourish.

Fusion centers today

Nevertheless, efforts to build fusion centers have continued, often in seeming ignorance or disregard of this dark history. Today there are 43 state, local and regional fusion centers in operation around the United States, with at least 15 more in development. No two fusion centers seem to be exactly alike, either in form or function, so it is difficult to con-

duct a generalized assessment of their value as compared to the potential risks they pose. In addition, they operate in considerable secrecy, so it is difficult for the public to evaluate what any particular fusion center does, much less what the network of fusion centers across the country is doing.

It is clear that not all fusion centers are engaging in improper or worrisome activities, and not all fusion center functions raise civil liberties or privacy concerns. But the statements and activities of some, combined with the push to standardize and weave together these state institutions, do raise questions about the overall direction in which they are headed. In particular, the federal government's vision as outlined in its Guidelines raises many concerns, as does the continuing lack of a legal framework to regulate the centers' activities.

Kentucky Governor Ernie Fletcher tours Kentucky's fusion center.

The Problems With Fusion Centers

I. Ambiguous lines of authority allow for "policy shopping."

II. Private sector participation in fusion centers risks privacy and security.

III. Military participation in fusion centers violates fundamental tenets of liberty.

IV. Data fusion = Data mining, which is bad for privacy and bad for security.

V. Excessive secrecy undermines the mission of fusion centers.

I. AMBIGUOUS LINES OF AUTHORITY

One problem with fusion centers is that they exist in a no-man's land between the federal government and the states, where policy and oversight is often uncertain and open to manipulation. There appears to be at least some conscious effort to circumvent public oversight by obscuring who is really in charge of these fusion centers and what laws apply to them. In struggling to answer the seemingly simple question of who is in charge of fusion centers at a recent congressional hearing, a Department of Homeland Security official could only offer that "fusion centers are in charge of fusion centers."[16] One analyst reportedly described his fusion center as the "wild west," where officials were free to "use a variety of technologies before 'politics' catches up and limits options."[17]

Federal involvement in the centers continues to grow. Most fusion centers developed as an extension of existing law enforcement intelligence units and as a result they have sometimes been described as "state police intelligence units on steroids."[18] But exactly who is providing those steroids is key to determining who will control them in the future. Fusion centers are still primarily staffed and funded by state authorities, but:

- The federal government is playing an essential role in the development and networking of fusion centers by providing financial assistance, sponsoring security clearances, and providing personnel, guidance and training.[19]
- The FBI has over 200 agents and analysts assigned to 36 fusion centers and plans to increase this commitment in the future.[20]
- As of December 2006, the DHS alone has provided over $380 million in federal funds to support fusion centers.[21]
- At least one fusion center, the Maryland Coordination and Analysis Center (MCAC), was initiated and led by federal authorities and was only recently turned over to the control of state officials.
- Thirty percent of ostensibly state-controlled fusion centers are physically located within federal agency workspace.[22]

Federal authorities are happy to reap the benefits of working with the fusion centers without officially taking ownership. Fusion center supporters argue that the federal government can use the "800,000 plus law enforcement officers across the country" to

"function as the 'eyes and ears' of an extended national security community."[23] Homeland Security Director Michael Chertoff, while denying that the federal government had any intention of controlling fusion centers, declared that "what we want to do is not create a single [fusion center], but a network of [centers] all across the country."[24]

Policy shopping

The presence of representatives from federal, state and local agencies at fusion centers and the ambiguity over who controls them can lead to a practice of "policy shopping," in which officials pick and choose from overlapping sets of laws so they can collect and use personal information as freely as possible, while avoiding privacy laws, open-records acts, and civil liability.

Some states, for example, have much stronger privacy or open-records laws than the federal government,[25] while in other states they are weaker. Fusion centers can manipulate who "owns" the records, or where they are "held" to thwart public oversight. If a particular state or locality has unusually broad privacy protection laws, the cooperating authorities can simply arrange for fusion center participants from that jurisdiction to have access to the data without actually "hosting" it. A Texas fusion center analyst's description of this scheme was described by a reporter:

> Of particular interest to many at the meeting was the way the Center accesses and uses data from local agencies; it does not host the data, but rather refreshes them regularly. That means analysts are not subject to the Freedom of Information Act (FOIA) or being dragged into court.[26]

Shielding fusion centers from public scrutiny may seem convenient from a pinched, bureaucratic perspective, but it is potentially disastrous for private citizens trying to pin down responsibility for mistaken information that is turning their lives upside down. Professionalism in law enforcement means not viewing privacy and FOIA laws as mere obstacles to be defeated, or "politics," but recognizing them as crucial checks and balances that must be respected to ensure accountability.

In addition to rules and jurisdictions, technology can also be manipulated to make more information accessible to the fusion centers, while limiting what information is retained for public accountability. The Maryland fusion center doesn't host any of its own data but rather uses a tool called the Digital Information Gateway (DIG), which allows MCAC to "connect with individual law enforcement, public health, public safety, and related databases throughout the Mid-Atlantic region."[27] MCAC representatives told the ACLU they only use DIG to connect to other law enforcement databases at this time. But that kind of data-mining tool could easily allow a fusion center to engage in widespread data retrieval and analysis across jurisdictions without producing any retained documentation or data that could be subject to freedom of information laws or oversight investigations.

From a privacy point of view, it does not matter where data is "hosted" or "stored" or "owned." All that matters is who has access to it. (See section on data mining, below.)

The networked fusion center approach promises the Department of Homeland Security all the benefits of a nationwide intelligence collection and analysis capability with none of the headaches that come from privacy laws, open-records statutes and other necessary elements of a democratic government.

Federal law

Title 28 of the Code of Federal Regulations, Part 23, governs what information can be put in a law enforcement database and how it can be used. The regulation states that all

criminal intelligence systems "shall collect information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity."[28] And the law limits the dissemination of law enforcement intelligence to situations in which "there is a need to know and a right to know the information in the performance of a law enforcement activity."[29]

This provision should limit what types of information fusion centers could exchange with non-law enforcement fusion center participants, and with each other. Indeed, many fusion center personnel contacted by the ACLU stated emphatically that they complied with this law, and that they planned to remain compliant by not incorporating private sector personnel within their fusion centers. CRS even reported that some fusion center personnel were concerned that sharing law enforcement information with DHS, which often employs non-law enforcement contractors, might violate the statute.[30] These law enforcement officers should be commended for their professionalism.

However, it is worrying that the federal Guidelines report does not account for this law when it advocates for the expanded scope of data to be collected at fusion centers. And indeed as fusion centers start sharing databases they appear to be looking for ways to circumvent these regulations. A California fusion center representative complained that compliance tasks required to manage law enforcement data sharing regulations "require an enormous amount of work," then suggested that by establishing "memorandums of understanding with data sharing in mind, they can move data from one database to another without worrying about someone else's data warehouse policies."[31]

II. PRIVATE SECTOR PARTICIPATION

Fusion centers are poised to become part of a wide-ranging trend of recent years in the United States: the creation of a "Surveillance-Industrial Complex" in which security agencies and the corporate sector join together in a frenzy of mass information gathering, tracking and routine surveillance.[32]

One of the goals of fusion centers is to protect the nation's "critical infrastructure"—85% of which is owned by private interests.[33] And one of the "value propositions" justifying federal support for fusion centers is increased government access to "non-traditional information sources."[34] The Guidelines emphatically encourage fusion centers to invite a wide range of public safety, public works, social services and private sector entities to participate in the fusion process (see box).

A Wide Range of Information

The DOJ Fusion Center Guidelines include a 6-page list—which it says is "not comprehensive"—of potential types of information fusion centers could incorporate. Some of the sources included on the list were:

- Private sector entities such as food/water production facilities, grocery stores and supermarkets, and restaurants.
- Banks, investment firms, credit companies and government-related financial departments.
- Preschools, day care centers, universities, primary & secondary schools and other educational entities providing information on suspicious activity.
- Fire and emergency medical services in both the public and private sector such as hospitals and private EMS services.
- Utilities, electricity, and oil companies, Department of Energy.
- Private physicians, pharmaceutical companies, veterinarians.
- The gaming industry, sports authority, sporting facilities, amusement parks, cruise lines, hotels, motels, resorts and convention centers.
- Internet service and e-mail providers, the FCC, telecom companies, computer and software companies, and related government agencies.
- Defense contractors and military entities.
- The U.S. Postal service and private shipping companies.
- Apartment facilities, facility management companies, housing authorities.
- Malls, retail stores and shopping centers.
- State and child welfare entities.
- Governmental, public, and private transport entities such as airlines and shipping companies.

While it is entirely appropriate for law enforcement to confer with private entities for specific, well-defined purposes, breaking down the arms-length relationship between government and the private sector by incorporating private entities into fusion centers is a bad idea. Several features of public-private fusion centers raise red flags:

- **"Critical infrastructure" is not defined in the DOJ Guidelines.** Rather, it is left to the discretion of state and local officials to determine who would be invited to participate in fusion center activities. That opens the possibility that political considerations could determine who gains access to fusion center information.

- **Some private entities foresee an active role in all aspects of the intelligence process**—and they want access to classified materials. An executive with Boeing (which has an analyst assigned to the Seattle fusion center) testified that the private sector "has the ability to effectively acquire, interpret, analyze and disseminate intelligence information—which may originate in the private sector."[35] He argued that giving private sector participants like Boeing "access to all information both classified and unclassified, which potentially or actually threatens them, is vital."[36]

- **Some fusion centers hire private companies to store and analyze the data they collect.** For example, in the wake of the influx of evacuees after Hurricane Katrina, the Texas Department of Homeland Security contracted with Northrop Grumman Corporation for a $1.4 million database project that would bring together a wide variety of law enforcement and government data, as well as consumer dossiers gathered by the private data company ChoicePoint.[37] The project was intended to create a "global search capability" over all this unstructured data, which would then be made available to the Texas Fusion Center. According

to the Texas Observer the project failed due to concerns over the security of the data: "it was not clear who at Northrop had access to the data, or what had become of it."[38]

Private-sector involvement is a bad idea

It is a bad idea to give private companies access to classified materials and other sensitive law enforcement information. While law enforcement officers undergo rigorous training, are sworn to serve their communities, and are paid public salaries; private companies and their employees are motivated to maximize profits. Potential risks include:

1. **A private company could use classified information to gain an unfair business advantage against its competitors.** Participation in fusion centers might give Boeing access to the trade secrets or security vulnerabilities of competing companies, or might give it an advantage in competing for government contracts. Expecting a Boeing analyst to distinguish between information that represents a security risk to Boeing and information that represents a business risk may be too much to ask.

2. **Private information in the hands of companies could be funneled to the government** without proper legal process. The types of information that could be provided to law enforcement from private entities that own or control "critical infrastructure" could endanger the privacy of ordinary Americans who work for or do business with these companies. Boeing, for example, is the fourth largest employer in Washington State.[39] For law enforcement to gain access to the breadth of information that a large employer like Boeing could make available would violate the principle that law enforcement only gather information on us when it has a reasonable suspicion of wrongdoing and proper legal process.

3. **Companies become an extension of the surveillance state.** Telecommunications companies contracted with the NSA to assist with its warrantless intelligence collection efforts,[40] and they contracted with the FBI to circumvent the Electronic Communications Privacy Act by using "exigent letters."[41] The cozy working relationships that developed between law enforcement agents and their "partners" in the private sector facilitated this blatantly illegal conduct, according to a report from the Inspector General of the Justice Department.[42] Rather than being chastened by the scandal resulting from that audit, the FBI requested another $5 million in their 2008 budget to pay the telecoms to warehouse data they would not otherwise keep, just in case the FBI might have a reason to request it later.[43]

4. **Private partnerships provide opportunities for the government to mask illicit activities.** Private companies could be used to as proxies to conduct activities that the government would otherwise be prohibited from engaging in. For example, the ACLU is currently suing a Boeing subsidiary, Jeppesen Dataplan, for, among other services, falsifying flight plans to disguise CIA "extraordinary rendition" torture flights.[44]

5. **Companies can glean personal information from security requests.** Just as internet service providers retain records of their customers' web searches for business intelligence purposes,[45] the private companies participating in fusion centers could mine the records of incoming government requests to create new prediction tools to identify other individuals who might be of interest to investigators. These new tools could then be marketed to other fusion centers,

or worse, to other clients, including private individuals, other commercial interests, and even foreign governments.

6. **Government information could be abused by companies.** From a security standpoint, the more people who have access to sensitive information, the more chances there are of a security breach—particularly where employees' loyalties lie with a private company rather than the community. Companies participating in fusion centers could be tempted to use their access to sensitive information to retaliate against company critics, competitors or troublesome employees, or to gain an advantage in difficult labor battles.

7. **Private participation could lead to private retaliation.** Private-sector access to inside information from fusion centers could lead to people unfairly being fired from a job, evicted from an apartment or denied a loan. What protections could be built to prevent this from happening? The Church Committee report on the FBI's COINTELPRO program is full of stories in which private sector actors cooperated with the FBI in firing, expelling or harassing Americans who were merely advocating for social change.[46]

8. **Employees of companies assigned to fusion centers could be asked to spy on their neighbors, clients, co-workers or employees.** Such concerns are not misplaced. The Bush Administration proposed nationalizing this very concept in 2002 through its "TIPS" program; Congress blocked it due to public outcry but it has resurfaced around the country in various guises.[47] One Kansas police department, for example, already trains maintenance and rental staffs of apartment complexes, motels and storage facilities to look for things like "printed terrorist materials and propaganda."[48] And a recent *Washington Post* article quoted a federal official staffing a fusion center as saying, "You need to educate cops, firefighters, health officials, transportation officials, sanitation workers, to understand the nature of the threat." While the official said these individuals were trained not to be "super-spies," he followed with a caveat: "constitutionally, they see something, they can report it."[49]

III. MILITARY PARTICIPATION

One of the more disturbing developments with fusion centers is the participation of active-duty military personnel. Longstanding American tradition, as enshrined in an 1878 law known as the Posse Comitatus Act, prohibits the U.S. military from acting in a law enforcement capacity on U.S. soil, except under express authority of Congress.[50] Yet military personnel are participating in many of these fusion centers with little debate about the legality of this activity or the potential effects this may have on our society.

The Maryland Coordination and Analysis Center (MCAC), for example, includes an active-duty U.S. Army soldier, whose mission is limited to military force protection, according to MCAC personnel. But it was not clear from the interview with the MCAC representatives what laws authorize Army participation in fusion centers, even at this limited level, or what oversight mechanisms exist to ensure that the military personnel assigned to the fusion center do not become involved in other intelligence or law enforcement activities. After all, the stated purpose of fusion centers is to share intelligence and increase coordination among participants.

Many fusion centers also incorporate National Guard troops, and at least one fusion center (in North Dakota) is located within National Guard facilities.[51] Other fusion centers

use the Law Enforcement Information Exchange (LInX), a law enforcement intelligence sharing system developed by the Department of the Navy for use in areas of strategic importance to the Navy.[52]

The involvement of military personnel is especially dangerous at a time when government officials are using hyperbolic rhetoric about the threat of terrorism to scare Americans into abandoning their civil liberties. For example, Major General Timothy J. Lowenberg, the Adjutant General of Washington State's National Guard, which participates in the Washington Joint Analytical Center, told Congress:

> We are a nation at war! That is the "ground truth" that must drive all of our data collection, information sharing and intelligence fusion and risk assessment actions... Today, all American communities, large and small, are part of a new and frighteningly lethal 21st Century global battle space.[53]

Officials who regard American communities as battlegrounds in a "war" can be tempted to dispense with "inconvenient" checks and balances. Americans have long been suspicious, for very good reasons, of the idea of deploying military assets on U.S. soil, and have long considered the Posse Comitatus Act to be one of the touchstones of American liberty. Allowing that bedrock principle to erode would be a radical step in the wrong direction.

IV. DATA FUSION = DATA MINING

The Justice Department's 2006 Guidelines envision fusion centers doing more than simply sharing legitimately acquired law enforcement information across different branches of our burgeoning security establishment. The Guidelines encourage compiling data "from nontraditional sources, such as public safety entities and private sector organizations" and fusing it with federal intelligence "to anticipate, identify, prevent, and/or monitor criminal and terrorist activity."[54] This strongly implies the use of statistical dragnets that have come to be called data mining.

The inevitable result of a data-mining approach to fusion centers will be:

- Many innocent individuals will be flagged, scrutinized, investigated, placed on watch lists, interrogated or arrested, and possibly suffer irreparable harm to their reputation, all because of a hidden machinery of data brokers, information aggregators and computer algorithms.[55]

- Law enforcement agencies will waste time and resources investing in high-tech computer boondoggles that leave them chasing false leads—while real threats go unaddressed and limited resources are sucked away from the basic, old-fashioned legwork that is the only way genuine terror plots have ever been foiled.

The Guidelines set forth a comprehensive vision for how these new institutions should operate:

> Data fusion involves the exchange of information from different sources, including law enforcement, public safety, and the private sector. When combined with appropriate analysis, it can result in meaningful and actionable intelligence and information.[56]

At a fusion center, the report says, threat assessments and information related to public safety, law enforcement, public health, social services and public works could be 'fused'

with federal data containing personally identifiable information whenever a "threat, criminal predicate, or public safety need is identified."[57] Subsequent analysis and dissemination of criminal/terrorist information, intelligence and other information would "ideally support efforts to anticipate, identify, prevent, and/or monitor criminal and terrorist activity."[58]

The head of the Delaware Information Analysis Center (DIAC): Delaware State Police Captain Bill Harris, explained that

> The fusion process is to take law enforcement information and other information—it could be from the Department of Agriculture, the Department of Transportation, the private sector—and fuse it together to look for anomalies and push information out to our stakeholders in Delaware who have both a right and a need to know.[59]

Rather than being constrained by the law regarding what they can collect, Capt. Harris appeared to feel constrained only by resources: "I don't want to say it's unlimited, but the ceiling is very high... When we have the money, we'll start going to those other agencies and say, 'Are you willing to share that database and what would it cost.'"[60]

The broad language used to describe fusion is eerily reminiscent of the Total Information Awareness program, a controversial Pentagon data-mining program that Congress shut down in 2003 because of its implications for the privacy of innocent Americans. These programs envision:

A) Compiling information from as broad a variety of sources as possible;

B) Proactively identifying unknown risks from among the population at large by sifting through that data; and

C) Looking for patterns "that can be used to predict and prevent future criminal activity."[61]

Data mining is not good for security

Perhaps the most fundamental problem with data mining is that, as many experts have pointed out, it won't work, and investing in data-mining technologies will drain finite homeland security resources, which makes it bad for security.

- Soon after 9/11 Gilman Louie, the head of the CIA's venture capital arm In-Q-Tel, warned against a "data-mining or profiling" approach to counterterrorism, which he described as "too blunt an instrument" to be a primary tool of surveillance. "I think it's very dangerous to give the government total access," he said.[62]

- The Association for Computing Machinery has said that data-mining approaches "suffer from fundamental flaws that are based in exceedingly complex and intractable issues of human nature, economics and law. . . As computer scientists and engineers we have significant doubts that the computer-based" approach will be effective.[63]

- In a recently published analysis, data mining pioneer Jeff Jonas and Jim Harper of the CATO Institute explained that while data mining has many useful purposes in other applications, it is poorly suited for predicting or preventing acts of terrorism:

> It would be unfortunate if data mining for terrorism discovery had currency within national security, law enforcement, and technology circles because pursuing this use of data mining would waste taxpayer dollars, needlessly infringe on privacy and civil liberties, and misdirect the valuable time and energy of the men and women in the national security community.[64]

Experts say that data mining can be effective where there is substantial amount of relevant data, a manageable universe of false negatives and a negligible cost to false positives. Direct mailers use data mining frequently to target advertising, and financial institutions often use data mining to screen for fraud. But these techniques rely on an analysis of thousands, if not millions of relevant transactions every day, and as Jonas and Harper point out, "terrorism does not occur with enough frequency to enable the creation of valid predictive models."[65] Moreover, as we have seen, what little data does exist, such as that making up the terrorist watchlists, is incomplete and riddled with errors.[66]

A drain on investigative resources

As a little simple math shows, even a hypothetical data-mining system that is 99% accurate—impossibly high by anyone's standards—will generate disabling numbers of false positives trying to identify a hypothetical terrorist population of 1,000 individuals (see box).[67]

Hypothetical numbers show data mining doesn't add up

Number of non-terrorists living in US	300,000,000
Number of terrorists living in US	1,000
Accuracy in identifying terrorists as terrorists	99.00%
Accuracy at identifying innocent as innocent	99.00%
# of terrorists who will be caught	990
# of innocent people who will be "caught"	3,000,000

Even determining the relevance of data pertaining to terrorism cases can be little more than guesswork. James Pavitt, the former Deputy Director for Operations of the CIA, warned against expecting anything near precision from the intelligence community: "If we are right 40 to 50 percent of the time we're batting pretty well."[68] No data-mining project relying on incomplete, erroneous and irrelevant data could ever succeed.

Aggregating information is bad for security and bad for privacy

As we have seen (see text box page 14), the Guidelines envision fusion centers bringing together a vast array of information from diverse sources. That is what "fusion" means.

All this data has already become a problem for the fusion center analysts buried under reams of irrelevant information. Fusion center officials, according to CRS, "remarked that their staff could spend all day, every day reviewing all the information posted on [competing federal information sharing systems] and still not be confident they had seen all relevant and/or unique data."[69] Meanwhile, the important information can easily be missed.

Fusion is also invasive of privacy by its very nature. Americans routinely share their private information with different parties—stores, banks, doctors, friends, the government—but they don't expect the details they share with one party will become available to all the others. Compartmentalization is a vital part of privacy (indeed, it is the core difference between privacy and *secrecy*, which is what you have when *no one* knows your details).

That is one reason why the Privacy Act of 1974 imposed restrictions on the authority of the federal government (though not the states) to merge databases (unfortunately that act is now so riddled with exceptions that it offers citizens very little protection).[70]

Compartmentalization is all the more important today when our lives are more and more entangled with computers, the Internet, electronic gadgets, cameras and computer chips, which capture and store our every interaction with them. The result is that mountains of data about our daily lives is being recorded and stored on the servers of government agencies and multinational corporations.[71]

The Justice Department Guidelines do stipulate that because of privacy concerns, it is "not the intent of fusion centers" to combine personal information into "one system or warehouse." The data would be maintained separately by the individual fusion center participants, which will "allow information from all sources to be readily gathered, analyzed, and exchanged" whenever a "threat, criminal predicate, or public safety need is identified." And data would be maintained in accordance with privacy laws and policies.[72]

There are several problems with this policy, however:

- The fact that information is "held" separately by various fusion participants, rather than held in one warehouse, is a distinction without a difference. For the user, a distributed database is completely indistinguishable from a single centralized one. Millions of people experience that phenomenon every day when they use Internet search engines that seamlessly seek out information that is "held" on millions of separate computers. If a fusion center's operators have our records available to them, we don't care what the database architecture is.

- The fact that information would only be compiled when there is a "threat" or a "public safety need is identified" hardly represents much of a limit on the freedom of fusion center analysts to collect whatever they want, and is a significantly lower bar than what is required by federal law.[73]

- Nor does the fact that the centers would comply with privacy laws provide much comfort. As we have seen, U.S. law limits the sharing of criminal intelligence information—but the vision of the Guidelines does not seem to account for that fact. And more broadly, American privacy laws are highly inadequate when it comes to responding to today's technology, and many highly invasive information practices are simply not yet covered by any laws.[74]

- Talk of "risk-based, information-driven prevention" suggests the generation of "risk scores" on individuals based on mass computer crunching of information about individuals—a vision akin to what we have seen elsewhere in the security establishment in recent years.[75] It is a very dangerous idea for the government to begin ranking of its own citizens according to their supposed trustworthiness. It has also been repeatedly banned by Congress.[76]

- All these problems are compounded when the data is full of errors—or when the public is not permitted to know what data sources are being used, lacks any practical way of correcting that data and is unable to scrutinize the methods used to create the risk scores.

Reports of "suspicious activity"

It appears that most of what fusion centers currently do is "respond to incoming requests, suspicious activity reports and/or finished intelligence products."[77] In many cases fusion centers amount to little more than centralized call-in centers for the reporting of suspicious activity. This conclusion is consistent with the results of the ACLU's

survey and with media reports, where fusion center personnel report repeatedly answering calls about "people taking pictures" and "people behaving suspiciously."[78]

Centralized call-in centers for the reporting of threats to public safety would not pose significant threats to privacy and civil liberties, so long as information is only collected when there is a reasonable indication of criminality and no information is disseminated except where necessary to achieve a law enforcement purpose. However:

- Current policies require that all terrorist threat information be reported to the FBI Joint Terrorism Task Forces. Since the FBI maintains a "no terrorism lead goes unaddressed" policy, even threat information that a fusion center analyst finds bogus will result in some investigative activity, raising concern that spurious allegations will have real consequences for those falsely accused.[79]

- In too many cases the subjects of these reports are "Arabs" or "Middle Eastern men," which is often why their innocuous behavior is reported as suspicious in the first place. Few of the "literally thousands of such leads" documented around the country have amounted to anything.[80]

- Asked by the *Washington Post* for an example of a successful use of a fusion center, the best one official could apparently come up with was the arrest and detention of a Muslim man spotted videotaping the Chesapeake Bay Bridge. But the *Post* goes on to note that the person in question, a U.S. citizen, was quickly released and never charged with any crime.[81]

- While such calls are often not the fault of fusion centers, outreach and training initiatives that encourage people to "report all suspicious activity" may be creating a culture of fear that encourages such overzealous reporting.[82]

Kentucky's Fusion Center.

V. EXCESSIVE SECRECY

Excessive secrecy not only undercuts the very purpose of fusion centers—the sharing of information with those who need it—but, as always, increases the danger that incompetence and malfeasance will flourish. It also raises sharp questions about how individuals who find they have been hurt by a center's data fusion and "threat identification" practices can seek redress.

Excessive secrecy on the part of the federal government also appears to be thwarting the fundamental aim of fusion centers, which is the prevention of terrorism through the coordination of state, local and federal information.

Fusion centers were born out of state and local frustration with the federal government's failure to share information through the FBI's Joint Terrorism Task Forces and elsewhere. Yet they are once again confronting the failure of the federal government to properly declassify and share intelligence information with their state and local law enforcement partners. As the CRS reported, "Numerous fusion center officials claim that although their center receives a substantial amount of information from federal agencies, they never seem to get the 'right information' or receive it in an efficient manner."[83] These law enforcement officers complained of routinely having to request relevant threat information from the federal government—raising justifiable concerns about potential threats they don't know enough to ask about.

Seattle Police Chief R. Gil Kerlikowske, for example, told Congress that the "federally centered vision of intelligence management" was the primary impediment to integrated intelligence fusion.[84] Kerlikowske complained that security clearances were difficult for local law enforcement to get in a timely manner, and that even for those cleared, "the sharing of vast categories of information is prohibited unless brokered by the FBI."[85]

Overclassification of national security intelligence has been a problem for the intelligence community for as long as a classification system has existed:

- As early as 1956 a committee formed by the Department of Defense to study classification processes and procedures determined that "vague classification standards and the failure to punish overclassification had caused overclassification to reach 'serious proportions.'"[86]

- In 1997 the Moynihan Commission found that the classification system "is too often used to deny the public an understanding of the policymaking process rather than for the necessary protection of intelligence activities," and recommended an overhaul of the classification system.

- Many experts have pointed to the counterproductive effects of overclassification. RAND terrorism expert Brian Jenkins, for example, argues that the classification system is a cold war legacy, and that the government should get away from the hub-and-spoke model of sending information to Washington to be stamped, and instead disseminate information widely.[87] It appears fusion center officials couldn't agree more.

- The 9/11 Commission found that classification issues were a factor in the failure to share intelligence that could have disrupted the terrorist attacks.[88] Of the ten missed "operational opportunities" to prevent the September 11th attacks identified by the Commission, not one involved a failure by a law enforcement officer or a weakness in a traditional law enforcement technique.[89] Instead, each missed opportunity was the result of a failure by intelligence officials to share critical information because of the confusing bureaucratic rules governing the dissemination of classified information.

Rather than overhaul their system for classifying national security secrets, the federal government has responded to the problem by increasing the number of security clearances it gives out. Yet this fails to confront the central problem. Fusion centers have an average of 14 staff members with "Secret" level security clearances, yet the problems with sharing classified information persist.[90] As Washington, DC police Chief Cathy Lanier put it, "it does a local police chief little good to receive information—including classified information—about a threat if she cannot use it to help prevent an attack."[91]

Most likely what is taking place is a power struggle in which federal agencies seek to turn fusion centers into "information farms"—feeding their own centralized programs with data from the states and localities, without providing much in return. The localities, meanwhile, want federal data that the agencies do not want to give up. For federal security agencies, information is often the key currency in turf wars and other bureaucratic battles, and from the days of J. Edgar Hoover they have long been loathe to share it freely.

RECOMMENDATIONS

Fusion centers are a diverse, amorphous and still-evolving new institution in American life. As presently constituted, many centers do not appear to raise any privacy or other issues. Others, however, appear to be taking active steps to dodge privacy rules, incorporating military and private-sector personnel, and flirting with a data-mining approach to their mission. And the federal government's vision for the centers, as well as natural tendencies toward "mission creep," suggest that they may evolve further in these unfortunate directions. Not only will this invade innocent Americans' privacy, but it will also hamper security by clogging the fusion centers with too much information and distracting our police forces from their public safety mission with false leads, fruitless fishing expeditions and bureaucratic turf wars.

The ACLU recommendations will help preserve our privacy, without endangering our security.

- Lift the cloak of secrecy surrounding the techniques that agencies at all levels of government are using to exploit information in the "War on Terror". Without any need to disclose particular investigative data, the public has a right to evaluate the techniques that may be applied to it.

- Urge reporters, legislators and citizens to learn more about fusion centers, and use state and local sunshine laws, as well as federal Freedom of Information Act requests, to do so. A list of questions that should be asked of the state and local fusion center representatives is available on the ACLU website at www.aclu.org/fusion.

- Subject fusion centers that involve the participation of federal agencies or receive federal funds to the federal Freedom of Information Act.

- Rather than use an outdated model of intelligence management that is ill-suited to modern threats to public safety, state and local authorities should return to traditional law enforcement techniques based upon reasonable suspicion that have kept America safe and free for over 230 years.

- Encourage Congress to focus more on the impact fusion centers may have on the privacy and civil liberties of ordinary Americans. The 109th Congress held more than five hearings regarding fusion centers and intelligence sharing, and the 110th held at least four more.[92] Witnesses included federal, state and local law enforcement agencies, and private sector fusion center participants—but no representatives from the privacy and civil liberties community.

- Encourage Congress to lead a pointed inquiry and debate over fusion centers before further resources are put into them. It must pursue the question of whether they represent a promising and effective approach to increasing security, whether they pose dangers to privacy and other civil liberties that outweigh any such promise, and what kind of federal regulatory action is warranted. Congress should explore how privacy protections can actually make these centers *more useful* as security tools.

- Congress should examine the use of military personnel in fusion centers and draw clear lines regarding how and when military personnel can engage in law enforcement intelligence collection and analysis.

- Demand that Congress take further steps to end the turn toward mass data surveillance as an acceptable law enforcement technique. It has already barred several questionable programs that move in this direction, but broader action may be required.

- Urge Congress to protect the privacy and civil rights of innocent Americans by requiring minimization procedures that prevent the intentional collection, retention and dissemination of private information when there is no reasonable indication of criminal activity. And Congress needs to build in protections to ensure that no American will be blacklisted without some form of due process.

- Stanch the free flow of data exchanged between the fusion centers and the private sector, through congressional action if necessary.

- The nation's security establishment must dispense with the myth that law enforcement is not an effective method for preventing terrorism.

Finally, state legislatures must act to create checks and balances on these institutions. Specifically,

- They should determine a proper mission for these entities and develop benchmarks for determining whether they are meeting their stated objectives.

- They should require regular reporting by the centers to determine what type of information they are collecting, how it is being used and with whom they are sharing it.

- They should regularly assess whether the fusion centers are acting in accordance with state law.

- If Congress will not act, state legislatures should bar fusion centers in their states from exchanging information with private-sector companies that are unaccountable to the public, or closely regulate such exchange.

End Notes

[1] Jay Stanley and Barry Steinhardt, Even Bigger, Even Weaker: The Emerging Surveillance Society: Where Are We Now? American Civil Liberties Union, (Sept. 2007), *available at* http://www.aclu.org/pdfs/privacy/bigger_weaker.pdf.

[2] Todd Masse, Siobhan O'Neil and John Rollins, Congressional Research Service, CRS Report for Congress: Fusion Centers: Issues and Options for Congress (July 6, 2007) [hereinafter CRS Fusion Center Report].

[3] CRS Fusion Center Report, *supra* note 2, at 18.

[4] *See generally, Mayor wants Portland out of anti-terrorism task force*, kgw.com and Associated Press, April 22, 2005, http://www.kgw.com/news-local/stories/kgw_042205_news_joint_terrorism_task_force_.201f434fe.html.

[5] Democratic Staff of the H.R. Comm. on Homeland Security, 110th Cong., LEAP: A Law Enforcement Assistance and Partnership Strategy, prepared at the request of Congressman Bennie G. Thompson, Ranking Member 5 (2006), http://hsc-democrats.house.gov/SiteDocuments/20060927193035-23713.pdf [Hereinafter LEAP Report].

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

[7] CRS Fusion Center Report, *supra* note 2, at 22 n.60.

[8] CRS Fusion Center Report, *supra*, note 2, at 21.

[9] CRS Fusion Center Report, supra note 2, at 18-19.

[10] Bureau of Justice Assistance, Office of Justice Programs, U.S. Dep't. of Justice, Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era, at iii, (Aug. 2006) [hereinafter Guidelines].

[11] Guidelines, *supra* note 10, at 2.

[12] CRS Fusion Center Report, *supra* note 2, at 1.

[13] 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).

[14] *Id.* at 11.

[15] *Id.* at 12.

[16] *The Way Forward with Fusion Centers: Challenges and Strategies for Change: Hearing Before the Subcomm. on Intelligence, Information Sharing and Terrorism Risk Assessment of the H. Comm. on Homeland Security*, 110th Cong. (Sept. 27, 2007) (quoting testimony of Jack Tomarchio, Principle Deputy Assistant Secretary for Intelligence and Analysis, Department of Homeland Security).

[17] Adena Schutzberg, *MetaCarta Users Tap Unstructured Data for New Geographic Uses*, Directions Magazine, May 30, 2007, http://www.directionsmag.com/article.php?article_id=2478&trv=1.

[18] CRS Fusion Center Report, *supra* note 2, at 1.

[19] CRS Fusion Center Report, *supra* note 2, at summary.

[20] *The Way Forward with Fusion Centers: Challenges and Strategies for Change: Hearing Before the Subcomm. on Intelligence, Information Sharing and Terrorism Risk Assessment of the H. Comm. on Homeland Security*, 110th Cong. (Sept. 27, 2007) (quoting testimony of Michael Mines, Deputy Assistant Director, Directorate of Intelligence, Federal Bureau of Investigation).

[21] CRS Fusion Center Report, *supra* note 2, at 41.

[22] CRS Fusion Center Report, *supra* note 2, at 36.

[23] CRS Fusion Center Report, *supra* note 2, at 7.

[24] CRS Fusion Center Report, *supra* note 2, at 9.

[25] *See* National Conference of State Legislatures, http://www.ncsl.org/programs/pubs/privacy-overview.htm (last visited Oct. 16, 2007).

[26] Schutzberg, *supra* note 17.

[27] *Visual Analytics to Support Information Sharing for the Maryland Coordination and Analytical Center (MCAC)*, PRNewswire, Nov. 14, 2003, http://sev.prnewswire.com/computer-electronics/20051114/DCM06114112005-1.html; *See also* Visual Analytics Technical Information, http://www.visualanalytics.com/products/dig/details/index.cfm (last visited Oct. 16, 2007).

[28] 28 C.F.R., §23.20(a) (2006).

[29] 28 C.F.R., §23.20(e) (2006).

[30] CRS Fusion Center Report, *supra* note 2, at 49.

[31] John Moore, *Policing Terror*, Federal Computer Week, Nov. 13, 2006, http://www.fcw.com/print/12_41/news/96760-1.html.

[32] Jay Stanley, The Surveillance-Industrial Complex, American Civil Liberties Union, (Aug. 2004), *available at* http://www.aclu.org/FilesPDFs/surveillance_report.pdf.

[33] Guidelines, *supra* note 10, at 17.

[34] CRS Fusion Center Report, *supra* note 2, at 4.

[35] *Building a Partnership Strategy: Improving Information Sharing with State & Local Law Enforcement and the Private Sector: Hearing Before the Subcomm. on Intelligence, Information Sharing and Terrorism Risk Assessment of the H. Comm. on Homeland Security*, 110th Cong. (May 25, 2007) (statement of Richard E. Hovel, Aviation Security Advisor, The Boeing Company), *available at* http://homeland.house.gov/SiteDocuments/20070525162

154-66669.pdf.

[36] *Private Sector Information Sharing: What Is It, Who Does It, and What's Working at DHS?: Hearing Before the Subcomm. on Intelligence, Information Sharing and Terrorism Risk Assessment of the H. Comm. on Homeland Security*, 110th Cong. (July 26, 2007) (statement of Richard E. Hovel, Senior Aviation & Homeland Security Advisor, The Boeing Company), *available a t* http://hsc.house.gov/SiteDocuments/20070726123058-82504.pdf.

[37] Jake Bernstein, *The Governor's Database*, The Texas Observer, April 20, 2007, http://www.texasobserver.org/article.php?aid=2472.

[38] *Id.*

[39] America's Career Info CareerOneStop, Washington State Profile: Largest Employers, http://www.acinet.org/acinet/oview6.asp?soccode=&stfips=53&from=State&id=&nodeid=12 (last visited Oct. 16, 2007).

[40] Leslie Cauley, *NSA has massive database of Americans' calls*, USA Today, May 11, 2006, at A1, *available at* http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

[41] Dep't. of Justice, Office of Inspector General, A Review of the Federal Bureau of Investigation's Use of National Security Letters 87 (March 2007), http://www.usdoj.gov/oig/special/s0703b/final.pdf.

[42] *Id.*

[43] Posting of Justin Rood to ABC News Blotter, http://blogs.abcnews.com/theblotter/2007/07/fbi-would-skirt.html (July 10, 2007 1:12 PM) (Post is titled: FBI Would Skirt Law with Proposed Phone Records Program).

[44] First Amended Complaint, *Binyam Mohamed et al., v. Jeppesen Dataplan, Inc.*, Civil Action No. 5:07-cv-02798(JW), filed Aug. 1, 2007, http://www.aclu.org/pdfs/safefree/mohamed_v_jeppesen_1stamendedcomplaint.pdf.

[45] *See*, Michael Barbaro and Tom Zeller, Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. Times, Aug. 9, 2006, *available at* http://www.nytimes.com/2006/08/09/technology/09aol.html?ex=1312776000&en=996f61c946da4d34&ei=5088&partner=rssnyt&emc=.

[46] 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, (1976).

[47] *See* Stanley, *supra* note 32.

[48] LEAP Report, *supra* note 5, at 6 (quoting Chief Ellen Hanson of the City of Lexana, Kansas Police Department).

[49] Mary Beth Sheridan and Spencer S. Hsu, *Localities Operate Intelligence Centers To Pool Terror Data,* Wash. Post, Dec. 31, 2006, at A03, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/12/30/AR2006123000238.html.

[50] 18 U.S.C.A. §1385 (West 2005).

[51] National Guardsmen are not governed by the Posse Comitatus Act when they are not called to federal service and therefore remain employees of the state. Still, the level of their participation in law enforcement activities is limited by law. In discussing the limits on National Guard participation in fusion centers, Major Robert Pankiw, coordinator of the Delaware National Guard program, reportedly explained that "the practice does not violate the federal Posse Comitatus Act because the Guard analysts have no arrest powers, focus only on drug crime and are under state, not federal, control." *See*, Mike Chalmers and Lee Williams, *Intelligence Facility Casts a Wide Net*, The News Journal, May 7, 2007, http://www.delawareonline.com/apps/pbcs.dll/article?AID=/20070507/NEWS/705070333. MCAC officials, however, stated that their National Guard participants were not totally restricted to drug intelligence analysis, although that was their primary focus.

[52] Law Enforcement Information Exchange, http://www.ncis.navy.mil/linx/index.html (last visited Oct. 16, 2007).

[53] *Building a Partnership Strategy: Improving Information Sharing with State & Local Law Enforcement and the Private Sector: Hearing Before the Subcomm. on Intelligence, Information Sharing and Terrorism Risk Assessment of the H. Comm. on Homeland Security*, 110th Cong. (May 25, 2007) (statement of Major General Timothy Lowenberg, the Adjutant General –Washington National Guard and Director, Washington Military Department), *available at,* http://homeland.house.gov/SiteDocuments/20070525162917-27103.pdf.

[54] Guidelines, *supra* note 10, at 13.

[55] For example, the FBI's Terrorist Screening Center's (TSC) watchlist contains over 700,000 records and increases by an average of 20,000 records per month. A recent Department of Justice Inspector General audit determined that 38 percent of the TSC records tested "continued to contain errors or inconsistencies that were not identified through the TSC's quality assurance efforts," thereby increasing "the chances of innocent persons being stopped or detained during an encounter because of being misidentified as a watchlist identity." Moreover, the list was also incomplete, as the IG determined that several known or suspected terrorists were not watchlisted appropriately. *See,* Dep't. of Justice, Office of Inspector General, Audit Division, Follow-up Audit of the Terrorist Screening Center, (Sept. 2007), at iii, http://www.usdoj.gov/oig/reports/FBI/a0741/final.pdf. Highlighting the fact that such bloated watchlists do nothing to improve security, even this inappropriately long list has apparently produced few arrests. *See*, Ellen Nakashima, *Terror Watchlist Yields few Arrests*, Wash. Post, Aug. 25, 2007, at A1, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/08/24/AR2007082402256.html?nav=rss_.

[56] Guidelines, *supra* note 10, at 2.

[57] Guidelines, *supra* note 10, at 13.

[58] Guidelines, *supra* note 10, at 13.

[59] Mike Chalmers and Lee Williams, *Intelligence Facility Casts a Wide Net*, The News Journal, May 7, 2007, http://www.delawareonline.com/apps/pbcs.dll/article?AID=/20070507/NEWS/705070333.

[60] *Id.*

[61] Guidelines, *supra* note 10, at F2 (definition of Crime-Pattern Analysis).

[62] Steve Lohr, *Data Expert is Cautious About Misuse of Information*, N.Y. Times, Mar. 25, 2003, at C6, *available at* http://query.nytimes.com/gst/fullpage.html?sec=technology&res=9E07E6D71530F936A15750C0A9659C8B63.

[63] Letter from Association for Computing Machinery Public Policy Committee to Sens. John Warner and Carl Levin (January 23, 2003) (on file with author), *available at* http://www.acm.org/usacm/Letters/tia_final.html.

[64] Jeff Jonas and Jim Harper, *Effective Counterterrorism and the Limited Role of Predictive Data Mining,* CATO Institute Policy Analysis, Dec. 11, 2006, at 1, http://www.cato.org/pubs/pas/pa584.pdf.

[65] *Id.* at 8.

[66] *See,* Dep't. of Justice, Office of Inspector General, Audit Division, Follow-up Audit of the Terrorist Screening Center, (Sept. 2007), at iii, http://www.usdoj.gov/oig/reports/FBI/a0741/final.pdf.

[67] This problem has been pointed out by several experts, including computer scientist Benjamin Kuipers of the University of Texas at Austinand Bruce Schneier. *See* E-mail from Benjamin Kuipers, Professor, Computer Sciences Department, University of Texas at Austin (Dec. 14, 2002), http://osdir.com/ml/culture.people.interesting-people/2002-12/msg00061.html**;** Bruce Schneier *National Crime Information Center (NCIC) Database Accuracy* Crypto-Gram Newsletter, http://www.counterpane.com/crypto-gram-0304.html.

[68] Dana Priest, *Retired Official Defends the CIA's Performance*, Wash. Post, Nov. 5, 2004, at A23, *available at* http://www.washingtonpost.com/wp-dyn/articles/A26485-2004Nov4.html.

[69] CRS Fusion Center Report, *supra* note 2, at 30.

[70] 5 U.S.C.A. §552a (West 2005).

[71] Jay Stanley and Barry Steinhardt, Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society, American Civil Liberties Union (Dec. 2002).

[72] Guidelines, *supra,* note 10, at 2.

[73] 28 C.F.R. Part 23.

[74] Jim Dempsey and Lara Flint provide a useful overview. *See* Jim Dempsey and Lara Flint, Privacy's Gap: The Largely Non-Existent Legal Framework for Government Mining of Commercial Data, Center for Democracy and Technology, (May 28, 2003), http://www.cdt.org/security/usapatriot/030528cdt.pdf.

[75] Guidelines, *supra* note 10, at D2. Other examples include the CAPPS II and Automated Targeting System airline passenger profiling programs. *See* American Civil Liberties Union, Feature on CAPPS II, www.aclu.org/capps (last visited Oct. 16, 2007); American Civil Liberties Union, Automated Targeting System, www.aclu.org/ats (last visited Oct. 16, 2007).

[76] Section 514(e) of the Department of Homeland Security 2007 Appropriations Act states,"[n]one of the funds provided in this or previous appropriations Acts may be utilized to develop or test algorithms assigning risk to passengers whose names are not on Government watchlists." Department of Homeland Security 2007 Appropriations Act, H.R. 5441, 110th Cong., §514(e) (2007).

[77] CRS Fusion Center Report, *supra* note 2, at 25.

[78] Shane Harris, *Shadow Hunters*, Nat'l J., April 27, 2007, *available at* http://nationaljournal.com/about/njweekly/stories/2007/0427nj1.htm.

[79] *See*, *National Commission on Terrorist Attacks upon the United States: Tenth Public Hearing* (April 14, 2004) (Statement of Robert S. Mueller, III, Director, FBI Before the National Commission on Terrorist Attacks upon the United States), *available at* http://www.fbi.gov/congress/congress04/mueller041404.htm.

[80] Harris, *supra* note 78.

[81] Mary Beth Sheridan and Spencer Hsu, *Localities Operate Intelligence Centers to Pool Terror Data*, Wash. Post, December 31, 2006, at A03, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/12/30/AR2006123000238.html.

[82] Stanley, *supra* note 32.

[83] CRS Fusion Center Report, *supra* note 2, at 28.

[84] *Building a Partnership Strategy: Improving Information Sharing with State & Local Law Enforcement and the Private Sector: Hearing Before the Subcomm. on Intelligence, Information Sharing and Terrorism Risk Assessment of the H. Comm. on Homeland Security*, 110th Cong. (May 25, 2007) (statement of R. Gil Kerlikowske, Chief of Police, Seattle Police Department), *available at* http://homeland.house.gov/SiteDocuments/20070525162207-44751.pdf.

[85] *Id.*

[86] *Report of the Commission on Protecting and Reducing Government Secrecy, Sen. Daniel Patrick Moynihan, Chairman,* S. Doc. No. 105-2, at Appendix G (1997), *available at* http://www.fas.org/sgp/library/moynihan/appg.html.

[87] *Five and Ten Year Homeland Security Goals: Hearing Before the Subcomm. on Homeland Security of the H. Comm. on Appropriations,* 110th Cong. (2007) (Statement of Brian Michael Jenkins, Senior Adviser, Rand Corporation).

[88] National Commission on Terrorist Attacks, The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States 417 (2004), *available at* http://www.9-

11commission.gov/report/911Report_Ch13.pdf.

89 *Id.* at 355.

90 CRS Fusion Center Report, *supra* note 2, at 26.

91 *Over-classification and Pseudo-classification: The Impact on Information Sharing: Hearing Before the Subcomm. on Intelligence, Information Sharing and Terrorism Risk Assessment of the H. Comm. on Homeland Security*, 110th Cong. (March 22, 2007) (statement of Cathy L. Lanier, Acting Police Chief, Metropolitan Police Department, Washington, DC), *available at,* http://fas.org/sgp/congress/2007/032207lanier.pdf.

92 CRS Fusion Center Report, supra note 2, at 53.