ACLU
AMERICAN CIVIL LIBERTIES UNION of MASSACHUSETTS

WHEN WE ARE ALL SUSPECTS

A Backgrounder on Government Surveillance in Massachusetts

I. OVERVIEW: SUNLIGHT ON SURVEILLANCE

Americans increasingly are aware that the massive US intelligence system that had failed to prevent the 9/11 attacks remains prone to what President Obama terms a "systemic failure."[1] The 2009 Christmas Day plot to bomb an airplane bound for Detroit was not, the President said, "a failure to collect intelligence. It was a failure to integrate and understand the intelligence that we already had." [2]

The false assumption that the nation can be kept safe by applying "advanced technology" to massive databases, sharing the information with a wide range of partners, and "integrating all instruments of national power to ensure unity of effort" (to quote from the National Counter-Terrorism Center's mission statement) has fostered the emergence of a national security surveillance state. This complex involves federal, state, and local law-enforcement agencies, as well as private entities and foreign governments. Today, some 800,000 local and state operatives are dispersed throughout American cities and towns, filing reports on even the most common everyday behaviors and feeding this information into state, local and regional "fusion centers" under the auspices of a National Strategy for Information Sharing or ISE.[3] This initiative facilitates near real-time sharing of information from a variety of databases among law enforcement officials and others. A new "homeland security" industry is flourishing, with lucrative gains going to Lockheed Martin, Raytheon, Boeing, Northrop Grumman and other major defense contractors, despite their reportedly inadequate performance. [4]

The loss to civil liberties and potential for abuse is far-reaching. With virtually no public discussion about the growing domestic surveillance apparatus and its methodology, we are in danger of losing such core values as the presumption of innocence and the right to privacy. Where intelligence used to mean gathering information for discreet criminal investigations, the definition of intelligence has been re-written to include the broad collection of information about everyday activities in hopes of detecting (and preventing) future behavior. Algorithms detect "pre-crime" in a world in which we are all potential suspects.[5]

This report focuses on the contours and implications of the new domestic intelligence paradigm for the Commonwealth of Massachusetts. Massachusetts, which played such a primary role in attaining the "blessings of liberty" enshrined in the Constitution and Bill of Rights, must again exercise leadership to ensure that liberty and security can co-exist in the 21st century. As the hubs and practices of the new surveillance network get established across the state, we urgently need sunlight to expose what is taking shape in the shadows, a public debate about the kind of society we want to be and remedial legislative action.

II. LESSONS OF 9/11 AND THE CHRISTMAS DAY PLOT: WHY MORE DATA DOESN'T MAKE US SAFE

President's Obama's warning after the 2009 Christmas Day Plot that more intelligence data doesn't necessarily keep us safe echoes statements from the multiple reports into the intelligence failure that led to the 9/11 terrorist attacks. Then too, the problem was not lack of information. Rather, intelligence agencies were drowning in information. According to one source, the highly secretive Echelon spy network run by the National Security Agency processed 3 million electronic communications a minute. [6] Then, as now, the US intelligence community failed to translate and analyze intelligence intercepts in a timely fashion and do what was needed to "connect the dots." The result was the litany of bureaucratic blunders, missed opportunities, turf wars, poor training, ineptitude, and systemic weakness detailed in the 900-page report from the House and Senate Intelligence Committees. [7]

In its review of how a 23-year-old Nigerian national Umar Farouk Abdulmutallab managed to evade the post 9/11 US intelligence network and board a plane carrying an explosive device, the White House reported that the security failure was not caused by the entrenched resistance to sharing information that preceded the 9/11 attacks. [8] Rather it was a failure of "intelligence analysis" for which the CIA and the National Counterterrorism Center were chiefly responsible. [9]

Five years after an extraordinary new layer of bureaucracy was established and heavily funded to promote effective intelligence sharing, integration, evaluation and dissemination, the National Counterterrorism Center (NCTC) has been found seriously wanting. Encompassing a dozen "partner agencies" from within the federal government as well as numerous "foreign partners," it maintains the National Counterterrorism Center's Terrorist Identities Datamart Environment (TIDE) system.

Well before Abdulmutallab took his seat on a plane, the TIDE system was seen to be suffering from what one Member of Congress called "serious, longstanding technical problems," and the attempt to fix it was a $300 million failure. [10] That is where Abdulmutallab's name and biographical data were deposited after his father in November 2009 told the US Embassy in Abuja as well as CIA officials about his son's possible ties to extremists in Yemen. There that information remained, along with a rising tide of information about some 550,000 other identities. Despite the fact that Abdulmutallab had been listed on a UK watch list in May 2009, and despite intelligence about a plot involving a "Nigerian" trained in Yemen, his name was never moved from the TIDE system to the master watch list in the Terrorist Screening Center, maintained by the FBI, a NCTC partner organization.

If TIDE is huge, the FBI's Terrorist Screening Database is a behemoth, containing the identities of 400,000 people and well over a million names, including aliases. [11] The FBI decides on a daily basis who should be included on the master watch list, added to the 4,000 strong "No Fly" list or put on the list of about 14,000 people targeted for additional airport screening. [12] The rate at which names are entered onto the master watch list has been steadily growing. The FBI reported to the Senate Judiciary Committee in the fall of 2009 that 1,600 people are being nominated for inclusion every day [13] - more than double the numbers entered in September 2007.

Two weeks before Abdulmutallab's flight, Timothy Healy, the Director of the Terrorist Screening

Center, told the Senate Committee on Homeland Security that "our interagency watchlisting and screening efforts have matured into a true information sharing success," and that the numbers on the watch lists will continue to increase "as new screening partners join our national and international enterprise." [14] According to Healy, those partners now include 17 foreign governments and all 72 state and local fusion centers within the United States.

As the names of "suspects" rapidly multiply, so do the counterterrorism wiretaps that the FBI has failed to review and share with its partner agencies. The Justice Department's Inspector General reported to Congress that 47,000 hours of tapes had not been processed - the equivalent of a recording lasting five and one-half years (representing a quarter of the recordings made since 2003). FBI Deputy Director John Pistole responded that the backlog was not in fact overwhelming, since the FBI had the assistance of "advanced technology" to identify specific tapes to review. [15]

As for the backlog of 7.2 million electronic files waiting for review, the FBI has maintained this too was not a big problem since "its analysts increasingly used sophisticated computer searches of databases to find high priority files rather than opening each individual file by hand." [16] It was not clear whether the agency expects computers also to do the work of translators. Having failed to meet its hiring goals for linguists in all but two of 14 targeted languages, the FBI now has fewer translators on staff today than it did a few years ago, according to the Justice Department's Inspector General.

III. THE RISE, FALL AND RISE AGAIN OF TOTAL INFORMATION AWARENESS

"[O]ur goal is total information awareness ..."
John Poindexter, Speech to Defense Technology Conference, 2002. [17]

The past decade has witnessed a radical shift in the work of both national and local intelligence and law enforcement communities in reaction to the failures of 9/11. Rather than insist on holding individuals and institutions accountable, the 9/11 Commission, a bipartisan group set up by Congress, recommended the establishment of the National Counter-Terrorism Center under a National Intelligence Director to promote a fundamental change in how intelligence agencies carried out their business. "Stovepipes" that separated agencies and information had to be dismantled as a "unity of effort" was built across government: "The system of 'need to know' should be replaced by a system of 'need to share'." [18]

Before the 9/11 Commission report appeared in 2004, building that "unity of effort" had already been begun with the merging of 22 government offices into the massive Department of Homeland Security (DHS) and the actions of a research arm of the Department of Defense known as the Defense Advanced Research Projects Agency (DARPA). Late in 2002, *The New York Times* revealed that DARPA's Office of Information Awareness under the leadership of Admiral John Poindexter, former National Security Advisor to President Reagan, was planning to "break down the stovepipes" separating commercial and government databases, so that all electronic data could be searched by powerful computers in the hunt for hidden patterns indicating terrorist activity. [19] Under "Total Information Awareness" (TIA), intelligence and law enforcement officials would have "instant access to information from Internet mail and calling records to credit card and banking transactions and

travel documents, without a search warrant." [20] The name reflected the growing belief that in order to prevent another attack, the government needed to know *everything* taking place in the United States and globally – everything about ordinary commercial transactions and personal information, in addition to traditional intelligence related to national security and criminal activity.

Once TIA was publicly unmasked, it faced intense opposition. A wide spectrum of groups feared this would be the end of the "right to be let alone," which Justice Louis Brandeis referred to as the "most comprehensive of rights and the right most valued by all civilized men." [21] Specifically, groups balked at the notion that TIA would access "every American's past addresses, personal medical records, bank dealings, travel itineraries, mental health histories, credit card purchases and other so-called 'transactional' data." [22] The Cato Institute warned that this "power to generate a comprehensive data profile on any U.S. citizen" invoked "the specter of the East German secret police and communist Cuba's block watch system." [23]

As the former CIA employee and Republican Congressman from Georgia Bob Barr and the ACLU's Legislative Director Laura Murphy wrote jointly in 2003:

> "Rarely, if ever, do groups as far apart on the ideological spectrum as the American Civil Liberties Union and Eagle Forum come down on the same side of an issue. But apparently, when it comes to preserving those core American ideals, there is rare common ground to be found." [24]

In response to this strong popular opposition, Congress appeared to reverse course, striking TIA from the Department of Defense Appropriations Act for fiscal year 2004. But the end of the TIA project in name did not mean the end of the "total information awareness" approach. Rather, legislators secretly wrote a classified annex to the appropriations bill that preserved funding for TIA's component technologies, as long as they were transferred to other government agencies and were used for military or foreign intelligence purposes against non-U.S. citizens. [25]

According to later reporting by the *National Journal*, research under TIA "was moved from the Pentagon's research-and-development agency to another group, which builds technologies primarily for the National Security Agency ... The names of key projects were changed, apparently to conceal their identities, but their funding remained intact, often under the same contracts." [26] Despite the official demise of TIA, its domestic intelligence-gathering apparatus continued to be expanded and enhanced under different programs and structures.

The FBI has amassed some 1.5 billion records in its National Security Branch Analysis Center in Crystal City, Virginia – including travel records, rental company records, credit card records, data broker records, telephone numbers, records of pilots and drivers of hazardous material in order to subject them to DARPA-style data mining. [27] It is also developing STAR ("The System to Assess Risk") which assigns scores to individuals based on information compiled from government and commercial databases. [28] In addition, it is building a massive database in Clarksburg, West Virginia that contains finger prints, palm patterns, facial recognition images and iris scans of millions of terrorist suspects and criminals. [29]

While the FBI has issued hundreds of thousands of National Security Letters to collect personal information from Internet Service Providers, phone companies and financial institutions, the National

Security Agency (NSA) has funded research into the "mass harvesting of the information that people post about themselves on social networks," and how to do "automated intelligence profiling" of this information combined with a wealth of other personal data. [30] According to *The Wall Street Journal*, by 2008 the NSA "now monitors huge volumes of records of domestic emails and Internet searches as well as bank transfers, credit card transactions, travel and telephone records" and searches for "suspicious patterns." It works in partnership with the FBI to cast a wide net of associations through "social-network analysis." [31]

Not all TIA-style projects have come to fruition. MATRIX (the "Multi-State Anti-Terrorism Information Exchange"), a prototype database combining state law enforcement and private information attracted too much opposition for states to buy into it. The Pentagon's "threat-tracking" Talon database was shut down after it was revealed that it was retaining information about peaceful anti-war protests. The Department of Homeland Security's ADVISE ("Analysis, Dissemination, Visualization, Insight and Semantic Enhancement") planned to troll a vast amount of data "to identify suspicious people, places, and other elements based on their links and behavioral patterns." It was reportedly abandoned after its pilot project was found to have been violating privacy guidelines. [32]

But the search for "suspicious patterns" through the aggregation of data and use of data mining techniques appears here to stay, in spite of the findings of the exhaustive 352-page report produced in October 2008 by the National Research Council. Based on several years of research, the report concludes that the attempts to find terrorists through data mining "is neither feasible as an objective nor desirable as a goal of technology development efforts" and that it will result in "ordinary, law-abiding citizens and businesses" being wrongly treated as suspects. [33]

That assessment has not stopped the Department of Homeland Security and other federal agencies from pushing ahead with plans to ensure "unity of effort" by enlisting state and local law-enforcement agencies in the collection, analysis and dissemination of information. They are seen as the "'eyes and ears' of the extended national security community." [34] As a result, both intelligence-gathering and policing are evolving in radically new directions with few rules in place and little discussion of the implications for "we the people."

IV LITTLE BROTHER IS WATCHING: THE DECENTRALIZATION OF SURVEILLANCE AND THE RISE OF FUSION CENTERS

> *"I envision a truly seamless community of intelligence professionals stretching out across the nation inclusive of traditional intelligence professionals, of law enforcement intelligence professionals, and of State, local and private sector intelligence professionals."*
> Charles E. Allen to the Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, February 4, 2007. [35]

The federal government has aggressively promoted this new surveillance network by directing restricted resources to the states and large urban areas to build the tools for ever-broader collection of information about ordinary Americans. In 2007, Congress codified this new approach by mandating the creation of an Information Sharing Environment ("ISE") to "combine policies, procedures, and technologies that link people, systems, and information among all appropriate federal, state, local and tribal entities and the private sector." [36]

The hubs for this multi-source information collection are the regional and state "fusion centers." Since 2003, with the assistance of Department of Homeland Security funding, these new data-collection institutions have been developed all over the country for the express purpose of "fusing" and analyzing information from law enforcement, other government entities, and private companies, ostensibly to combat terrorism. Now numbering 72, fusion centers are intended to be "the cornerstone of information sharing with state and local governments." [37] Operating on the state and local level, these institutions have been established to feed a rapidly developing national intelligence network, each one serving as a node within the larger information-sharing web.

Fusion centers represent a significant departure from traditional law enforcement objectives and methods. There are few legal limits on what they can and cannot do. They erase jurisdictional boundaries and blur lines of authority and accountability. They expand what information may be collected and with whom it may be shared. They empower local and state officials, including undercover operatives, to engage in domestic intelligence collection and monitor everyday behavior that has nothing to do with criminal investigations. To feed fusion center databases, state and local police are encouraged to collect and report on non-criminal "suspicious" behavior such as taking photographs, writing notes and espousing "radical" beliefs. They invite non-law enforcement participants, including private sector companies and the U.S. military, into local and state intelligence operations. [38] And they have become a repository for "tips" about "suspicious" behavior phoned in by members of the public.

Former Attorney General John Ashcroft's plan to train citizens to report suspicious activity through a program known as Operation TIPS ("Terrorism Information and Prevention System") caused such a public outcry that it was officially cancelled by Congress in November 2002. But now the federal government and local police are reaching out to local community groups in an effort to "engage their communities to prevent crime and terrorism" and to "reaffirm their commitment to working together to improve the utility of fusion centers." [39]

Making intelligence operations more effective by improving the sharing of information material to criminal investigations is a legitimate law enforcement goal. However, increasing law enforcement's capacity and incentive to collect and share information without a connection to suspected criminal activity is neither effective nor wise. History shows that regardless of good intentions, creating the means to secretly gather, store, access and use personal information of millions of Americans without adequate controls is likely to distract law enforcement from its public safety mission and lead to abuses of individual liberties and civil rights.

Spying on Protected Political Activity

The recent dramatic expansion of intelligence collection at the local and state level raises profound civil liberties concerns regarding individual privacy, freedom of speech, freedom of association, and freedom of religion. The quantity of data that law enforcement and federal intelligence agencies are newly able and encouraged to collect, share and store indefinitely opens the door to identity theft, violations of privacy and the very real possibility that innocent people will be considered suspects without having done anything wrong.

With the emphasis on getting more information about everyone and everything that could, however remotely, be connected to "suspicious" activity, it is not surprising that the ACLU has documented instances of improper spying on protected First Amendment speech and rights of association in more than half the states. Examples include:

• A May 7, 2008 report prepared for the Department of Homeland Security entitled "Universal Adversary Dynamic Threat Assessment" that labeled environmental organizations like the Sierra Club, the Humane Society and the Audubon Society as "mainstream organizations with known or possible links to eco-terrorism." [40]

• The fact that animal rights rallies, environmental demonstrations, anti-war protests, student protests against military recruiting on campus, labor union organizing, and demonstrations against police brutality have all found their way into government databases at the California Anti-Terrorism Center, the California Office of Homeland Security and the LA County Terrorist Early Warning Center (LACTEW). [41]

• The infiltration of and monitoring by the Maryland State Police of non-violent peace groups, death penalty groups, Amnesty International and the Chesapeake Climate Action Network. Blatantly incorrect information about peace activists has been entered into the local fusion center and other government databases, bearing labels such as "Terrorism - anti-government," according to documents obtained through an ACLU public records request. [42]

• A document leaked from the Virginia Fusion Center that cited various historically Black colleges and universities as potential "radicalization nodes" for terrorists. The Nation of Islam, New Black Panther Party and Earth First! are among the 33 groups listed as potential terrorist threats. [43]

• A "Prevention Awareness Bulletin" leaked from a Texas fusion center that flagged former Georgia Congresswoman Cynthia McKinney and former U.S. Attorney General Ramsey Clark for surveillance, as well as groups such as the Council on American Islamic Relations, ANSWER and the International Action Center. [44]

• A report on the "modern militia movement" that was leaked from the Missouri Information Analysis Center, the state's fusion center. It stated that militia members are "usually supporters" of presidential candidates Ron Paul, Chuck Baldwin and Bob Barr, and instructed the Missouri police to be on the look out for people displaying bumper stickers and paraphernalia associated with the Constitutional, Campaign for Liberty, and Libertarian parties. [45]

The very federal agencies that have championed the new approach have also raised serious concerns. In 2008, the Department of Homeland Security Privacy Office conducted a review of fusion center programs and identified a number of risks to privacy presented by the fusion center program, including: (1) **Ambiguous Lines of Authority, Rules, and Oversight**; (2) **Participation of the Military and the Private Sector**; (3) **Data Mining**; (4) **Excessive Secrecy**; (5) **Inaccurate or Incomplete Information**; and (6) **Mission Creep**. [46]

Nonetheless, this DHS report offered precious little help from the federal government in addressing these issues. Instead, it placed the burden of safeguarding civil liberties squarely on local

jurisdictions themselves, stating that it "presumes that the States are interested in preserving and competent to protect the rights of their own citizens, and offers no opinion as to their methods." [47]

Has Massachusetts shown itself to be interested in preserving and competent to protect the rights of its residents? It is to the intelligence-gathering network that is taking shape in the Commonwealth that we now turn.

IV. UNTANGLING THE SURVEILLANCE WEB IN MASSACHUSETTS

> *"Are we wiretapping, are we following what's going on, are we seeing who's coming in, who's coming out, are we eavesdropping, carrying out surveillance on those individuals that are coming from places that have sponsored domestic terror?"*
> Governor Mitt Romney, Speech to the Heritage Foundation, September 14, 2005

Mitt Romney served as Governor of Massachusetts during 2003 – 2007, the years when the new intelligence apparatus was being erected around the country. As lead governor on homeland security issues at the National Governors Association and a member of the Department of Homeland Security's Advisory Council, he was an ardent backer of what he called a "new intelligence network" which would be built at the state and local level to sift through crime reports in order to disclose terrorist plots. [48] And he hoped to revive Operation TIPS, which had already been cancelled by Congress: "The eyes and ears which gather intelligence need to be as developed in our country as they were in foreign countries during the cold war …Meter readers, EMS drivers, law enforcement, private sector personnel need to be on the lookout for information which may be useful." [49]

No sooner did Romney become governor than the Massachusetts-FBI Joint Terrorism Task Force (JTTF) was expanded. What started in 1979 as an informal collaboration between the FBI and the New York Police Department to fight bank robberies became a formal arrangement in 1996 when FBI offices began to enter into agreements with local and state police to create JTTFs. Under this form of cross-jurisdictional cooperation, state and local law enforcement officials remain on the local payroll but are deputized by the FBI and given clearance to access information and work under the direction of the FBI agent in charge. Today, every FBI field office in the country has a JTTF and more than 5,000 law enforcement, intelligence, military and civilian members are involved in "field investigations of actual or potential terrorism threats." [50]

The Massachusetts State Police, Boston Police Department, Lowell Police Department, MBTA Police Department and the U.S. Postal Service are all part of a 2003 JTTF agreement with the FBI and work together with members of the military and the federal government. The stated purpose of the Massachusetts JTTF is the "prevention, preemption, deterrence and investigation of terrorism and activities related to terrorism, both actual and potential." [51] In effect, the FBI's JTTF turns local and state police officers into federal domestic intelligence agents who carry out operations and share information with many other agencies and entities.

A year after the Massachusetts JTTF was constituted, Governor Romney brought the fusion center concept to Massachusetts. In 2004, the groundwork was laid for the Commonwealth Fusion Center (CFC) without any public notice or legislative process. A few years later, the Commonwealth Fusion Center was codified by Executive Order – again without any public involvement. [52]

The Commonwealth Fusion Center was joined by a second fusion center in 2005, the Boston Regional Intelligence Center (BRIC). As a major urban area with a vulnerable port and an airport involved in the 9/11 attacks, Boston – and by extension all of Massachusetts – have served as a national model for intelligence cooperation and information-sharing among federal, state, local and private partners.

Although the surveillance and information-sharing mechanisms being developed and employed in Massachusetts remain largely secret, the ACLU of Massachusetts has been able to uncover some facts that shed light on what is happening – and raise many more questions.

First, the ACLU of Massachusetts has made and continues to make requests for information under the Massachusetts public records laws and the federal Freedom of Information Act (FOIA). The information we received uncovered inconsistencies and areas that are open for abuse.

Second, attorneys from the ACLU of Massachusetts met with officials from the Commonwealth Fusion Center and toured the facility. While the government officials were forthcoming with information and answered many of our questions, more remain. The following is a synopsis of what we have learned through our FOIA work and through publicly available information.

The Commonwealth Fusion Center

Because of the lack of publicly available information about the CFC, the ACLU of Massachusetts wrote to the Secretary of the state Executive Office of Public Safety ("EOPS") in December 2007 requesting information under the Massachusetts public records laws. We received an informative reply. However, because of its inherently secret nature, many questions remain about the structure and functioning of the CFC.

Here is what we do know about the CFC, which is currently based in Maynard, Massachusetts. The Fusion Center was first mentioned in the State Homeland Security Strategy issued by the Executive Office of Public Safety in February 2004, which reported that "the operational and organizational 'hub' of the commonwealth's homeland security efforts will be a 14/7 information fusion center maintained by the Massachusetts State Police Criminal Intelligence Section" which would work closely with the new Joint Terrorism Task Force, the US Attorney's Office and other key state, regional and local entities to collect and share intelligence.

The CFC was subsequently set up as a multi-agency data collection center under the supervision of the Massachusetts State Police. Federal, state, local and private officials of various agencies and companies were soon embedded within it, providing the CFC with access to their databases and having access to the information stored and analyzed in the CFC hub. These agencies include the FBI, Bureau of Alcohol, Tobacco, Firearms and Explosives, the Massachusetts National Guard, the Department of Correction, the Department of Homeland Security Office of Intelligence Analysis,

the Geographic Information Systems and the U.S. Army Civil Support Team. [53] In addition, a police officer from CSX Railroad, a private entity, was also embedded in the CFC. [54]

The Fusion Center has entered into data-sharing agreements with local police departments in Massachusetts, state police in other states and with a number of state agencies. Through the national Information Sharing Environment, the Fusion Center is linked to other federal and state agencies, and the data it collects can easily be shared. The information apparently is shared both ways: in addition to federal agents having access to local information, local personnel have been granted clearance by DHS and FBI to access classified information.[55]

What is the focus of all this intelligence gathering? The original mandate of the CFC was to "detect, protect against, prevent, respond to, and recover from terrorist attacks and other critical incidents," and to "allow for the seamless exchange of homeland security information, terrorism information, and law enforcement information related to terrorism." [56] But from the beginning, it had a broader vision of its mission, undertaking to employ an "all hazards," "all threats," and "all crimes" approach to homeland security and to collect information that was unrelated to terrorism.[57]

Crucially, the line between traditional crime fighting and terrorism detection was blurred, ostensibly because terrorists increasingly relied on crime to finance their activities. But there were other reasons. According to a report by the Congressional Research Service, "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" *[58]*

Created as terrorism-fighting tools, soon most fusion centers in the country changed the focus of their data collection to an "all crimes" and "all hazards" mission that is substantially broader than the laws that created them envisioned. [59] This broader approach enabled them to apply for a wider range of grants to fund the work. [60] By the end of 2007, a survey of 36 fusion centers found that only 15 percent of them said their focus was solely counterterrorism.[61]

The CFC, like other fusion centers around the country that later expanded their mission, can collect information that goes well beyond criminal intelligence. This includes information obtained from "medical examiners (unattended death), public health entities, emergency rooms (information similar to the Drug Abuse Warning Network program), environmental regulatory inspectors, transportation entities, housing inspectors, health inspectors, building code inspectors, etc." [62]

According to the Massachusetts Executive Office of Public Safety, which is responsible up the chain of command for the CFC:

"The CFC actually has several core functions. These include its role as the repository of traditional criminal information so that localities and regions can work together to share criminal information about specific investigations, arrests, warrants and trends. It also includes issues involving critical infrastructure assessments (i.e. managing a statewide database, known as ACAMS, which assesses vulnerabilities), serves as a missing children information clearinghouse, and promotes uniform crime reporting and gun tracing." [63]

In Massachusetts, Fusion Center officials have told us that the CFC does not have its own operatives, but that it instead relies on information gathered by participating entities. [64] However, the CFC guidelines anticipate that the CFC will not just rely on information sent to them by local law enforcement, but that CFC personnel will themselves perform surveillance duties – which can be done undercover.

The CFC guidelines make specific provision for CFC undercover operatives. For example, the guidelines suggest that CFC undercover operatives may engage in checking leads and conducting preliminary inquiries in response to any allegation or information received or collected by the Fusion Center, even when there is no reasonable suspicion of unlawful activity. CFC undercover operatives are authorized to "attend meetings that are open to the public for purpose of observing and documenting events" and are not required to identify themselves or leave a gathering if it is requested that police officers leave or identify themselves." [65] The guidelines further state that "the mere presence of legal counsel at a meeting does not require an undercover to miss or leave the meeting."

Even though the CFC purports to "voluntarily" [66] comply with 28 CFR 23, a federal regulation that mandates that any project receiving federal money "shall collect and maintain criminal intelligence 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," the CFC's own procedures contradict this.

CFC Standard Operating Procedure allows officers to conduct "preliminary inquiries" and check leads before establishing reasonable suspicion that a target is involved in criminal activity. During preliminary inquiries, "all lawful investigative techniques may be used." [67] As a result, such preliminary inquiries can even involve undercover operatives or known informants.[68]

While continuing to rely on the flow of counter-terrorism funding from the federal government and the public's support of broad powers in the anti-terrorism field, the CFC and fusion centers across the country now collect data that has little or no relation to terrorism, and in many cases, no relation to actual crimes.

In the process, something new has been born, again with the help of federal grants: a concept of policing that is no longer primarily reactive and focused on solving crimes that have been committed, or collecting concrete evidence that a crime may be about to be committed. In "intelligence-led policing," officers on the beat are seen as "an excellent resource for gathering information on all kinds of potential threats and vulnerabilities." [69] "Predictive policing" involves strategies and tactics "that improve the situational awareness of law enforcement concerning individuals and locations before criminal activity occurs….These methods may include contemporary approaches to dynamic systems modeling and forecasting such as algorithmic methods, machine or statistical learning, or ensemble methods. Prediction can focus on a number of variables including places, individuals, groups, or incidents." [70]

The hunt for "pre crime" is taken up by local police who no longer are entirely "local." When local police are assigned to JTTFs they become federal officers and are no longer under the supervision of and accountable to their local departments and communities. When they participate with fusion centers in the collection and sharing of information, they are integrated into a national domestic surveillance network for law enforcement and intelligence agencies where lines of authority between local, state and federal agencies are blurred and there is no meaningful local control. The City of Boston has been a lead player in the construction of this new police paradigm.

The Boston Regional Intelligence Center and the Rise of "Suspicious Activity Reporting"

In 2005, the Boston Police Department unveiled its own intelligence-sharing center, known as the Boston Regional Intelligence Center (BRIC). According to the Boston Police, BRIC "was conceived as a way to further integrate the intelligence capabilities of Boston, local, state, and federal law enforcement partners and represents a strategic overhaul to the department's traditional intelligence operation."[71]

Like the Fusion Center, BRIC entered into data-sharing agreements with local police departments in Massachusetts, state police in other states and with a number of state agencies.[72] And like the Fusion Center, BRIC has embedded in it representatives from other law enforcement agencies, including the Massachusetts State Police, the MBTA Transit Police, the Massachusetts Department of Correction, the Suffolk County Sheriff's Office, the Brookline and Cambridge Police Departments and a representative from the private sector who serves as a liaison between law enforcement and the business community.[73] BRIC also shares information with the Fusion Center and the Joint Terrorism Task Force.

In 2009, the City of Boston received nearly $2 million in federal stimulus funding from the American Recovery and Reinvestment Act for two grants presented to the Boston Police Department (BPD) and the Boston Public Health Commission (BPHC).[74] The grant to the BPD will be used for 10 new positions inside the BRIC, including three Real-Time Crime Center Intelligence analyst positions and two Social Network Analysis Intelligence positions. In addition, Boston was one of seven cities to receive a Predictive Policing Demonstration and Evaluation Program award of $200,000 in FY 2009.

Suspicious Activity Reports (SARS)

Boston, along with Los Angeles, Chicago and Miami-Dade, is also participating in a pilot program known as the "Nationwide SAR Initiative." As rolled out by the Los Angeles Police Department (LAPD) in 2007, the program requires officers to report "suspicious behaviors" in addition to their other duties – creating a stream of "intelligence" about a range of everyday activities that will be fed into the local fusion center. [75] The LAPD program defines as "suspicious behaviors" a range of activities such as using binoculars, taking measurements, taking pictures or video footage, taking notes, and espousing "extremist views."[76]

The Office of the Director of National Intelligence touted the LAPD as a "national model," and the Departments of Justice and Homeland Security recently teamed with the Major City Chiefs Association to expand the "Suspicious Activity Reporting" to three other cities, including Boston.[77] According to *The Wall Street Journal,* the next stage is getting the public involved "in an education program, called iWATCH, which will instruct citizens on specific behaviors to report to authorities." [78] Within three years, the federal government plans to expand it to 72 cities and town nationwide. [79]

In an effort to document and make available as much information as possible regarding activities that are merely potential indicators of crime, Suspicious Activity Reporting requires that incidents involving a range of everyday activities – such a taking pictures of buildings – are written up in reports that are fed into the nationwide Information Sharing Environment through fusion centers, the

JTTFs or a massive FBI database called eGuardian. Through the Information Sharing Environment, participants from myriad agencies around the country would have access to the reports.

The original purpose for filing Suspicious Activity Reports was to help prevent acts of terrorism, and the federal agencies purport to use this expansive information-gathering method only in connection to terrorism. However, under the government's definition, a Suspicious Activity Report is "official documentation of observed behavior that may be indicative of intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit intention." [80] Note that the activity could be related to *any* illicit intention, and that the activity may or may not be linked to a crime at all. This standard is well below that of "reasonable suspicion" set out in 28 CFR Part 23, which governs much gathering of criminal intelligence.

According to the government's own rules, SARs "are not intended to be used to track or record ongoing enforcement, intelligence, or investigatory operations although they can provide information to these activities."[81] Instead, SARs are a way to document and share information about potential crimes *before* they happen. As such, these data-gathering centers can compile files on people that are full of information on activities that may be innocent, and in some cases, constitutionally protected.

Domestic law enforcement is not the only sector that can draft and file SARs. In addition to government agencies, "private sector organizations responsible for Critical Infrastructure/Key Resources (CI/KR) and foreign partners are also potential sources for terrorism-related SARs."[82]

An Expanding Web of Surveillance Databases

When SARS are filed, they end up in a data mountain that is growing ever larger in size and reach. Agencies that enter into information-sharing agreements have access to a variety of different databases, both government-run and private. The accessing entities have no control over or knowledge about the kind and quality of information that is entered into the databases, yet they may rely on the information they retrieve in order to begin or continue an investigation.

For example, the "MassGangs" database in the Commonwealth Fusion Center collects a vast range of personal and associational information on "gangs," defined broadly as "[a]n identifiable organization, association or group of two or more persons, whether formal or informal, whose members or associates engage, either individually or collectively, in criminal activity." [83] Based on this broad definition, a "gang member" could include any person who merely associates informally with another person who is engaged in criminal activity. Yet MassGangs is designed to collect personal data on anyone who fits this broad definition and to share this personal information with the Fusion Center, including names, characteristics, primary activities, pictures, electronic documents, associations, scars or marks, physical details, addresses, employers, vehicles, and motor vehicle information.[84]

Massachusetts is developing several other databases that will make information-sharing easier. In 2008, the Commonwealth unveiled SWISS, the Statewide Information Sharing System – a "criminal incident data collection and warehousing system that for the first time enables law enforcement entities from across the state to seamlessly share criminal incident data."[85] SWISS allows multiple agencies to contribute police reports in real-time to a state repository and then access and search these

reports remotely through a desktop or mobile computer.[86] Such a database will create a permanent record not only of arrests, but of *all* incidents – from fighting neighbors to a barking dog, because it is based on all "calls to service." In addition, the database will include each time a police officer stops someone on the street and makes a search. [87]

Gathered information will also be put into another database known as "COPLINK,"[88] a project in development jointly by the Fusion Center and the Massachusetts Criminal History Systems Board, which, according to the government, is a "powerful analytical tool that provides officers, investigators, analysts, and police executives with new methods to generate leads, perform crime analysis, map data and trends, and support decision-making." [89]

Technology-Driven Surveillance

Information that was once contained only in paper records situated in dispersed and remote locations is increasingly available in digital form that can be shared instantly. Intelligence agencies have the ability to gather, analyze, store indefinitely and share vast quantities of data, including personally identifiable information, which is available in thousands of public and private databases at lightning speed.

Modern technology has far outpaced our laws' ability to protect civil liberties. The information that can be learned about a person today bears little resemblance to the dossiers and files that government could compile about citizens at the time privacy and civil liberties protections were drafted. Today, the government can learn about anybody's physical location, buying preferences, health, political views and more through a myriad of available technologies that are constantly increasing and improving.

Some examples:

FACIAL RECOGNITION SOFTWARE

Raytheon, based in Waltham, Massachusetts, is a top provider of surveillance technology to law enforcement. It has developed "customized facial recognition solutions," that allow computers to recognize human faces in real time.[90]

BIOMETRICS

The FBI biometric database now contains over 56 million records and the Department of Homeland Security holds over one hundred million records. [91]

GPS LOCATION THROUGH CELLULAR PHONES

The government can gain access to any cell phone's location through cell phone providers. An automated system can send out a ping to a phone, which comes back with the phone's latitude and longitude. A recent report revealed that Sprint Nextel "pinged" its customers more than eight million times between September 2008 and 2009 on behalf of law enforcement.[92]

RADIO FREQUENCY IDENTIFICATION (RFID):

These tiny chips send out radio signals that can be read wirelessly from several yards away and without the knowledge of the holder. U.S. passports now contain these chips, as do the MBTA's Charlie cards, some cellular phones and countless other commercial products.

SURVEILLANCE CAMERAS

Modern cameras have the capability of facial recognition, detailed zoom, night vision capabilities, "X-Ray" vision, and tracking in 3-D. The network of DHS-funded surveillance cameras that has been installed in the nine cities and towns of the Greater Boston "Urban Area Security Initiative" could eventually be fitted with facial recognition software, eye scans, radio frequency identification tags and other forms of software and connected to large law enforcement databases. [93]

Imagine a database, accessible via a web browser from handheld mobiles and laptops in police cruisers, that contains billions of data entries on millions of people including but not limited to bank and telephone records, email correspondence, web habits, images and travel patterns. In early 2003, the Massachusetts State Police (MSP) put out a request for proposals for an Information Management System (IMS) that would do just that.[94]

The software sought by MSP would: "Automate the collection, collation and processing of intelligence data; Automate the dissemination of intelligence information to law enforcement personnel both internal and external to the State Police; Manage intelligence data collected from disparate sources (paper reports, electronic reports/documents, existing databases, email, fax); Provide the technology tools necessary to analyze collected intelligence data; [and] Provide a reporting package that allows the collected data to be utilized to produce meaningful intelligence reports."

In May 2005, the Massachusetts State Police awarded Raytheon a $2.2 million contract to build, install, troubleshoot and maintain the Information Management System. [95]

V. TOTAL SURVEILLANCE SOCIETY: A PRICE WORTH PAYING?

> *It's a pretty simple concept: we bring together people from every U.S. agency that collects and processes intelligence; we put them in one room and hook them into their own and into our FBI intelligence databases; and all of a sudden we have the universe of terrorist intelligence on the table."*
> Ken Love, Acting Chief of the National Joint Terrorism Task Force [96]

What appeared simple to Mr. Love back in 2004 seems much more complicated today – and more troubling. Much remains unknown about the emerging national intelligence system, including the Commonwealth Fusion Center, BRIC, and the implementation of aggressive new law enforcement strategies in Massachusetts. What we *do* know, however, is cause for serious concern for a variety of reasons.

First, these new strategies are less effective than traditional intelligence efforts and wasteful of precious resources.

Second, Fusion Center policies and the Suspicious Activity Reporting program, respectively, permit and encourage investigation of totally lawful First Amendment activities – including creative expression, political expression, political and religious association, and communal worship – without

reasonable suspicion of criminal wrongdoing.

Third, the Fusion Center's lack of verification of the accuracy of the information collected and disseminated, together with gaps in state and federal law, threaten to produce incurably flawed files and undermine privacy rights.

Finally, these new intelligence data centers remain frighteningly opaque and unaccountable.

Total Surveillance Doesn't Keep us Safe

According to Mike German, a former FBI agent who infiltrated terrorist groups and now works as an ACLU Policy Counsel, "Investigating people who aren't breaking the law is a waste of law enforcement time and finite security resources, as well as an unnecessary violation of privacy." [97]

More information is not necessarily better information. Intelligence agencies have been drowning in a tsunami of data, much of it flawed when it was entered into databases, and much of it irretrievable because of the bigger flaws in technology systems that are supposed to make it "simple" to deliver actionable intelligence. According to the Government Accountability Office, "413 government IT projects totaling more than $25 billion in FY2008 alone were 'poorly planned, poorly performing, or both.'" [98] The number grew by a further 238 projects and $13 billion in FY2009. [99]

Instead of focusing law enforcement resources and attention on identifying and investigating threats, billions of dollars have been put into gathering as much information as possible about as many people, situations and facts as possible, in the hopes of using automated systems to create links that will prevent terrorist attacks and catch criminals. Valuable time is wasted in the attempt to broaden access to secure computer systems that may not be compatible, to make sure that those who have access have proper clearances and background checks, and to figure out ways to restrict unauthorized access without impeding the flow of data and to store data securely. One keystroke can mean that a name will not be retrieved, as reportedly happened when the State Department attempted to see if the 2009 Christmas Day bomber, Umar Farouk Abdulmutallab, possessed a valid US visa.

However, when the number and type of intelligence sources is so vast that we are all potential suspects, it becomes impossible to validate or give appropriate weight to different pieces of information that are being fed into the system. With reports in different forms and with different sets of data from local police officers, banks, surveillance cameras, public transportation systems, health systems and more, data sifting replaces traditional sleuthing and it becomes difficult to separate the wheat of useful information from the chaff of endless data. A focus on data mining and gathering an ever-increasing *quantity* of data runs the risk of distracting law enforcement from tried-and-true investigative techniques that focus on indications of specific criminal wrongdoing and yield *high quality* intelligence.

Feeding the Surveillance Monster; Undermining Community Policing

As the National Research Council found after years of studying the subject, data mining is not an effective way to prevent terrorism. Yet the architecture has been built and needs funding and feeding. Pressure on local officials to obtain federal homeland security grant money is leading

the state down the wrong path, away from effective intelligence and public safety. As a result, Massachusetts and other states have adopted anti-terrorism plans that have little or no relationship to actual threats or hazards. To qualify for its full allotment of federal money, for example, Massachusetts had to come up with a plan to protect the state from improvised explosive devices, although there was no intelligence to indicate that such devices were or were about to be a domestic threat within the Commonwealth. [100]

The MBTA is one agency that appears to have prioritized intelligence gathering over such commonsense public safety matters as keeping its infrastructure in good repair.[101] In 2005, it reported that it had established an intelligence unit monitoring transit-related terrorism world wide. [102] This unit, which was partnered with the JTTF, Boston Police, State Police, ICE, DHS, DEA, the MTA Interagency Counterterrorism Task Force in New York City and the Commonwealth Fusion Center, maintained 14 stand alone databases and entered information about suspicious activity and crime and forwarded it to its partners. It also compiled a weekly bulletin, "Reporting on Terrorism-Related Activity," which it distributed nationally.

When the net is cast so wide, everything and anything begins to look and sound like "terrorism-related activity," forcing police officers to waste their time checking out dead end tips Invariably, innocent people are caught in the net. Peter Watchorn, an internationally-known harpsichordist, and a fellow musician were pulled off the MBTA on March 13, 2008, when they were on their way to the airport. Eight state troopers subjected them to a search and interrogation for 30 minutes because they were, as one trooper allegedly put it, "having conversations we were not supposed to be having" which triggered an anonymous tip. On the basis of this tip - which Mr. Watchorn assumes was a hoax - the MBTA police decided they represented a "credible threat," brought the subway line to a halt, searched it with sniffer dogs, and forced them to miss their plane. [103]

Furthermore, so-called "intelligence-led" and "predictive" policing without quality-control safeguards undermines community trust, on which crime-prevention and crime-solving efforts rely. Law enforcement officials must create the conditions of trust under which everyday citizens will feel free to call the police and report suspicious activities. Increased surveillance cannot take the place of effective community-based policing, in which residents trust the uniformed men and women who protect them.

With local law enforcement agencies increasingly no longer accountable to local communities because they have been federalized through their work with the JTTFs and Fusion Centers and have other agendas, it is difficult to see how these relationships of trust can be preserved.

In Massachusetts, many communities lack trust in law enforcement because of a history of misconduct, and the failure of police to respond in a timely manner when they are most needed. Trust has been further eroded because they are now seen as working hand in hand with federal agencies, including Immigration and Customs Enforcement (ICE) and the FBI, whose revised 2008 guidelines permit it to use religion or ethnicity as a factor in deciding what people to interview and to infiltrate organizations and religious groups when opening "assessments." The Muslim, Arab and South Asian communities feel particularly vulnerable and are frequently reluctant to engage with law enforcement.

What is called "intelligence-led policing" is eroding the relationships of trust that have

traditionally defined effective "community policing." "Intelligence-led policing" came to the United States from Great Britain, where, among other things, it "de-emphasized responses to service calls by prioritizing calls" and referring less serious ones to other agencies so that police could focus on broad criminal trends. [104] But are the police more likely to win community trust if they spend their time chasing down vague "tips" and attempting to keep abreast of massive amounts of data, instead of responding to calls for assistance that may not seem "priorities" but help them forge close community ties? Relationships of trust are unlikely to flourish as long as local police have a separate federal agenda with no accountability to or oversight from the community.

Excessive Surveillance and the Threat to Freedom

When the government targets an ever-increasing list of activities for surveillance, it is inevitable that protected speech and conduct will be caught up in that web. With profound implications for the ability of all persons in the United States to exercise their constitutionally-protected rights, this kind of targeting has had a disproportionate impact on Arab, Muslim and South Asian communities, as well as peace activists, environmental advocates, celebrities, and anyone who opposes current government policy.

For example, it has been reported to the ACLU of Massachusetts that there has been a decline in attendance at local mosques because of the confirmed FBI surveillance of these places of worship, and deployment of informants. When the overly-broad collection of information leads innocent individuals to feel that they are not safe to worship freely, such policies have gone too far.

Other community members have reported that they no longer speak in Arabic or other foreign languages on the telephone for fear that the government could be listening and could misinterpret something said in that language. Still others report not wearing religious forms of dress and symbols or possessing Arabic texts in public, and especially at airports, for fear of being singled out for questioning and having trouble clearing security.

When the breadth of possible investigations is so large, protected activities can easily be made to seem "suspicious." In its policy specifically addressing the collection of information about expressive activity, the CFC asserts that it does not gather information based *solely* on First Amendment activity.

However, it is unclear when and to whom this policy actually applies, as the exceptions make the policy largely meaningless. The guidelines state that they "specifically do not apply to investigations focused on solving crimes that have already been committed. These guidelines also do not apply to investigations under the control of the Joint Terrorism Task Force or other federal, state or local task forces that members of the CFC may be assigned to."[105]

The policy goes on to declare that "for the purpose of detecting or preventing unlawful activities, as well as to assess the need for police planning related to lawful activities, CFC members are authorized to visit any place, attend any event, and visit any website that is open to the public, on the same terms and conditions as members of the public generally."[106]

But CFC and other law enforcement agents are not simply members of the public. Their presence at places of worship and their active surveillance have an impact on the ability of ordinary people to

exercise their constitutional rights.

Because the Fusion Center and BRIC operate largely in secret and without independent oversight, it is difficult to determine the extent to which the civil liberties of Massachusetts residents may have been violated as a result of the creation of this local and state domestic surveillance system.

But since 9/11, there have been numerous reports in the Commonwealth of police invading people's privacy, and stopping, questioning and even arresting individuals based on nothing more than perfectly lawful activities, such as taking photographs, participating in political rallies, and speaking critically of the FBI.[107]

According to a scathing audit recently released by the Massachusetts state Auditor A. Joseph DeNucci, police from communities across the state have repeatedly tapped into the state's criminal records system to improperly access information on celebrities and high-profile citizens, such as actor Matt Damon, singer James Taylor and football star Tom Brady. The year-long review depicted a system accessed by users "without any apparent work-related justification."[108] It is unclear how many other private citizens might also have had their privacy violated by these improper searches.

In December 2002, a police officer at the University of Massachusetts campus at Amherst was recruited by the FBI to spend several days a week working exclusively for its Anti-Terrorism Task Force. The arrangement came to light after FBI agents, acting on the basis of information provided by the campus officer, questioned a faculty member and an organizer for a campus union. The faculty member is of Iraqi descent and the union organizer is from Sri Lanka.[109]

A plainclothes Harvard University detective was caught photographing people at a peaceful protest for "intelligence gathering" purposes. Harvard University Police Department ("HUPD") officers are sworn special State Police officers and often work "in conjunction with other agencies, including the Massachusetts State Police, Boston Police, Cambridge Police, Somerville Police, and many federal agencies." A university spokesman refused to say what the HUPD does with the photographs it takes for "intelligence gathering" purposes, so it is unknown whether this information was shared.[110]

A "Protective Intelligence Bulletin" issued by the DHS Intelligence Branch of the Threat Management Division of the Federal Protective Service improperly collected and disseminated information regarding political demonstrations and inappropriately labeled peaceful advocacy groups and other activists as "extremists." Included in this report was an event organized in Boston on March 18, 2006 on the topic, "Stop the violence, stop the war at home and abroad."[111]

Inadequate Privacy Protections Threaten Fundamental Freedoms

BRIC and the Fusion Center have steadily expanded the number of public and private sources from which they collect information. The CFC began with access to the considerable data available through state and national criminal justice information systems. It has since secured direct access to scores of federal and state government databases and has contracted with major commercial data aggregators and investigative services.[112]

This aggressive collection of personal data by the state, made newly possible with the development of 21st century information technology, represents an unprecedented government intrusion into the minutiae of the lives of ordinary Massachusetts residents. As such, it also represents an enormous threat to personal privacy. Apart from most medical history information, there is now virtually nothing that a Fusion Center investigator could not deduce about an individual's living arrangements, employment history, financial condition, personal relationships, and in some cases, personal views.[113]

This troubling invasion of privacy is magnified further by a total lack of quality controls – standards for accuracy and reliability – to ensure that the information gathered is correct and appropriately classified, or that it even pertains to the identified individual. Without adequate safeguards, it is all too easy for wrong information to be disseminated nationwide, and all but impossible to rein it in later.

The Commonwealth Fusion Center's treatment of data accuracy and privacy provides particular cause for concern. The Fusion Center Privacy Policy is a study in contradiction and double-speak which does more to shield its operations from public scrutiny than it does to protect individual privacy.[114] Indeed, the policy disclaims any responsibility for the accuracy of data it may collect, instead passing the buck to the agencies where the information originated, stating: "Participating agencies remain ... responsible for the quality and accuracy of the data accessed by the CFC." [115] And, when an error is reported, it pushes responsibility even further away: "Participating agencies will refer citizens to the original collector of the data as the appropriate entity to address any concern about data accuracy and quality." [116]

Compounding the problem, because the Fusion Center contracts with private data aggregators to gather personal and commercial information about Massachusetts residents, the "original collector" may not be a government agency at all, and therefore would not be subject to state open government laws that exist to ensure the integrity of personal information held by the government about individuals. Yet the information does make its way into a government database and is used by law enforcement officials.

In the end, the Privacy Policy of the Commonwealth Fusion Center creates no enforceable rights.[117] It depends for its effectiveness on a combination of internal self-regulation and unwarranted trust in the integrity of other entities' data quality controls.

Current Privacy Law Lags Behind the Surveillance System

Unfortunately, state law may not adequately provide protections where the Fusion Center Privacy Policy fails. Massachusetts' Fair Information Practices Act (FIPA)[118] "was intended to correct abuses in the way in which personal data about individuals, collected by State agencies, was maintained and disseminated." [119] The law provides that personal information held by state agencies about an identifiable individual may not be disclosed to other agencies or individuals without express legal authorization. It also provides individuals with access to the information about them maintained by the government and an opportunity to contest its accuracy. [120]

Yet the utility of FIPA as a check on the Fusion Center remains open to question. The "personal

data" subject to the provisions of FIPA does not include "intelligence information," which is defined in G.L. c. 6, § 167 as data "compiled by a criminal justice agency for purposes of criminal investigation, including reports of informants, investigators or other persons, or from any type of surveillance associated with an identifiable individual." With the unprecedented expansion of the intelligence activities of the State Police, this exemption is likely to be used to thwart efforts to ensure the accuracy of the information that is being collected or to prevent its widespread dissemination.

In 1968, Congress created a federal regulation, 28 C.F.R. Part 23, to ensure the privacy of individuals in the context of multi-jurisdictional criminal investigations. Reasoning that "because the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates," Congress mandated that any criminal intelligence system receiving federal funding adhere to the regulation's "reasonable suspicion" standard for the gathering of data.

However, this regulation has no enforcement mechanism. Meanwhile, the fusion centers that should be subject to it are collecting more information than the regulation allows. Because the focus of these centers is on preventing crimes that may occur in the future, and not solving crimes that have happened in the past, much information is gathered, analyzed and shared long before officials have determined that there is reasonable suspicion of criminal activity. As a result, the Fourth Amendment standard for searches and seizures has been rendered all but meaningless.

The Commonwealth Fusion Center's Standard Operating Procedure (SOP), for example, gives its officers the ability to conduct preliminary and then full investigations into people and organizations before establishing reasonable suspicion. According to the SOP, the standard for opening a full investigation is "satisfied where there is not yet a current substantive or preparatory unlawful act, but facts and circumstances reasonably indicate that such unlawful conduct will occur in the future." [121]

Apparent protections at the federal level are similarly illusory. Department of Justice regulations applicable to state intelligence activities that receive federal funds ostensibly limit the collection and dissemination of personal information.[122] The viability of the federal guidelines, however, depends entirely on monitoring by the same federal agencies that are pressing the states to expand their intelligence-gathering activities. State officials have pledged to adhere to the requirements of these federal regulations and to be guided by national best practices for intelligence and information-sharing. However, without federal enforcement or other methods of accountability, the Fusion Center is regulated exclusively by good intentions.

Who Watches the Watchers?

The only ostensible check on the rules by which the Fusion Center operates is an appointed body without any real powers. In August of 2008, Kevin Burke, Massachusetts Secretary of Public Safety and Security, established a "Privacy Working Group" (PWG) to advise him on "programmatic, technological, and policy issues within [the Executive Office of Public Safety and Security] as they relate to information security, individual privacy, data integrity, and other privacy related matters."[123] Presumably, because EOPSS has authority over the Fusion Center, the PWG's purview includes the Fusion Center. However, the PWG provides no independent oversight or enforcement of privacy standards, and offers no public accountability vis-à-vis the Fusion Center or BRIC. [124]

Because the PWG lacks independence it cannot be an effective oversight mechanism. PWG members are appointed by the Secretary of Public Safety and Security, and the PWG carries on current and future operations at his discretion. Moreover, the PWG's mission is to respond to specific assignments from the Secretary, not to set its own agenda for investigation, analysis and policy recommendation.

Given these dynamics, it is unlikely that the PWG will conduct a rigorous analysis of the Fusion Center's operations as they relate to privacy and civil liberties. Moreover, even the most robust recommendations from the PWG regarding privacy and liberty protections would be merely hortatory, lacking the force of law necessary to ensure appropriate implementation and enforcement.

Garbage In/Garbage Out: Absence of Quality Controls Imperils Data Integrity

An intelligence system that fails to put a premium on the accuracy and reliability of its information is likely not only to undermine its own goals, but to harm innocent people in the process. When the system picks up whispers from unreliable sources and broadcasts them in a national intelligence echo chamber, the resulting reverberations appear to give additional credibility to inaccurate information. Even when the dissemination of such inaccurate information adversely impacts its subject – as when the late Senator Ted Kennedy's name appeared on the federal "no fly" list – it has become decentralized and next to impossible to fix.

The government itself does not have a good track record of ensuring the accuracy of its data. When it comes to terrorism, the government cannot even get the numbers correct. In 2007, the Department of Justice's Office of Inspector General conducted a study of the accuracy in the department's reporting of terrorism-related statistics. These statistics include the number of individuals charged as a result of terrorism investigations, the number of terrorism convictions and the number terrorism-related threats. The Inspector General found that the FBI inaccurately reported 8 out of 10 statistics and that the US Attorney's Office incorrectly reported all the 11 out of 11 statistics randomly surveyed.[125]

How long is bad information stored? The FBI's e-Guardian system, which takes in suspicious activity reports from multiple agencies, claims that it purges reports that have been deemed to have no probable link to terrorism. However, reports that are deemed "inconclusive" – in other words, reports that may or may not have a link to terrorism – are kept in eGuardian for up to five years.

Excessive Secrecy Hinders Public Accountability

Perhaps the most problematic aspect of the new intelligence data centers in Massachusetts is their lack of transparency and accountability. These institutions were created without any public process, so residents of the Commonwealth know next to nothing about them. Moreover, their operations remain resolutely opaque, for two critical reasons. First, their organizational structure entangles federal, state, and local law enforcement, creating ambiguous lines of authority and accountability. Second, their policies serve to impede, rather than encourage, transparency.

Ambiguity over who is in charge of and responsible for Fusion Center operations can lead to a practice of "policy shopping," in which officials pick and choose from overlapping sets of laws so that they can collect and use personal information as freely as possible, while avoiding privacy laws, open-records statutes and civil liability.

Though the Fusion Center operates under a chain of command that "ends with the Colonel of State Police, who is under the authority of the Secretary of Public Safety and Security and ultimately the Governor,"[126] it also takes "strategic guidance" from the federal Department of Homeland Security. Similarly, though it is primarily staffed by Massachusetts State Police officers who report to the State Police Department, others, assigned to the FBI Joint Terrorism Task Force (JTTF), are under the direct command of the Fusion Center. [127]

In addition to the FBI, the Fusion Center also includes representatives from other federal agencies, including the Bureau of Alcohol, Tobacco, Firearms and Explosives, the National Guard, the Department of Homeland Security, and the US Army. [128] It is not clear whether each of these representatives reports to the Fusion Center central command, to their respective agency heads, or both.

The various agencies that have a representative embedded in the Fusion Center each have a separate Memorandum of Understanding with the CFC, including a separate agreement about how that person will be supervised. For example, most agencies agree that the embedded person will be "directed by the decisions of the Commanding Officer of the CFC for all matters occurring in the normal course of business of the CFC," but that administrative, personnel, salary and benefits issues are under the control of their supervisor at the agency. [129]

But this agreement does not apply to all embedded personnel. The Massachusetts National Guard's MOU has set up a structure where the embedded person is responsible up the chain of command and can only receive "guidance" from the CFC Commanding Officer. [130] This sets up a situation in which the CFC Commander has different levels of control over the persons working there.

This complicated web of affiliations and allegiances makes it difficult to know who is in charge of the various staff members, providing guidance, direction and discipline when necessary. Without clear lines of authority, it is impossible to ensure proper staff accountability for maintaining the privacy and civil liberties of Massachusetts residents. These concerns are particularly acute in view of the active involvement of representatives from the military and a private, commercial railroad company (CSX Corporation) in Fusion Center operations.

As for the question of transparency, good open government practices typically include reasonable access by individuals to information the government holds about them, as well as public oversight and reporting on government activities. To that end, we have laws that promote openness and accountability, including public records laws, independent auditing, and external review processes. Unfortunately, the Fusion Center's records and operations enjoy unwarranted freedom from public scrutiny, either because they can hide behind overbroad exemptions in otherwise applicable laws, or because the Fusion Center's policies deliberately sidestep the law. The operations of the Fusion Center are being placed outside the Massachusetts laws restricting government secrecy.

In the case of the state's Fair Information Practices Act, a gaping exemption for all "intelligence information" means that residents who are concerned about what information Massachusetts intelligence data centers hold about them have no way of finding out. Unlike its counterpart in the federal Freedom of Information Act, this exemption from FIPA is not tailored to achieve reasonable, specific goals, such as protecting ongoing criminal investigations or law enforcement proceedings, preventing unwarranted invasions of personal privacy, or protecting identifiable people from harms that might result from disclosure. Instead, it contains no exceptions and makes it impossible for an individual to learn about and correct inaccuracies in any "intelligence" the government has gathered about him or her.

The Fusion Center has taken a similar approach to the public's right to know about its operations, generally. Massachusetts' public records law broadly defines a public record to include all records or data "made or received by any officer or employee of any agency, executive office [or] department . . . of the commonwealth."[131] Such records must be disclosed on request unless exempted by one of several specific statutory exceptions. However, privileging secrecy over good government, the Fusion Center disavows responsibility under the state public records law.

Even though data accessed by the Fusion Center is clearly "made or received" by it, the Fusion Center has indicated it will not respond to requests from members of the public for information obtained from other sources, directing them instead to "the agency or entity that is the source of the data in question."[132] Consistent with this policy, the Fusion Center has incorporated into its agreements with third party agencies a specific provision that shared information obtained from any other agency will not be disclosed in response to a public records request. These agreements almost certainly violate state law,[133] but they will, with equal certainty, be used to obstruct the release of information necessary to ensure effective public scrutiny of the Fusion Center's activities.

Without any independent oversight mechanism or public reporting, the general public remains in the dark. Fusion centers are left to police themselves, even though they have every incentive – as well as the stated intention – to sidestep laws they find inconvenient. Good law enforcement makes its operations transparent, even while maintaining confidentiality about ongoing investigations and protecting witnesses and confidential sources from harm. Massachusetts should expect this much from intelligence data centers operating within its borders.

VI. RECOMMENDATIONS

Massachusetts, the cradle of liberty, has never been passive when it comes to overzealous government intrusion. We demand our say in the institutions that directly impact our lives.

In light of the secretive development of the new domestic surveillance apparatus in the Commonwealth and the federal government's unwillingness to establish simple safeguards for our fundamental freedoms, we must shine a light on this shadowy government activity, examine it carefully, and consider its efficacy and impact. We must decide for ourselves if these aggressive "intelligence" programs are right for Massachusetts, and make sure that any domestic surveillance operations in the Commonwealth conform to long-standing principles of liberty, instead of undermining them.

A COST/BENEFIT ANALYSIS SHOULD BE UNDERTAKEN.

The Massachusetts executive branch and legislature should ask difficult questions about whether the fusion centers in the state and related law enforcement data programs accomplish worthwhile objectives. Do fusion centers make a demonstrable positive impact on law enforcement efficacy? If so, at what cost to the civil liberties and privacy of Massachusetts residents? Do the purported benefits outweigh the damage to community relationships that will inevitably occur when residents perceive – correctly – that their local police, whether directly or indirectly, now play a considerably larger role in federal law and immigration enforcement?

In addition, the state should conduct a fiscal analysis. The Commonwealth Fusion Center and BRIC are expensive to operate. Although the Department of Homeland Security spent more than $250 million to provide "start up" funding for state fusion centers[134] and continues to make sustaining grants available to the states, it is unclear if the federal government will continue to fund these massive projects indefinitely. According to a recent GAO report, "the federal government has not clearly articulated the long-term role it expects to play in sustaining fusion centers." If we anticipate that the financial burden for fusion centers will shift to the states, is that a cost that is worth Massachusetts shouldering?

THE STATE LEGISATURE SHOULD REGULATE "INTELLIGENCE" OPERATIONS.

The new domestic surveillance apparatus in Massachusetts was built without legislative input, but it should certainly not continue that way. The fiscal implications of fusion centers and related law enforcement data programs, the consequences for public safety, and the impact on civil liberties demand legislative participation. The Massachusetts legislature must not abdicate its responsibility to regulate such important state institutions and ensure that they operate in keeping with established constitutional and good government norms in the Commonwealth. Senate Bill 931, *An Act Regarding the Commonwealth Fusion Center and Other Intelligence Data Centers*, filed in the 2009-2010 legislative session, is one vehicle for such regulation, and would accomplish many of the following goals.

1. Prohibit Investigation of First Amendment Activity

Massachusetts should ensure that state law robustly protects residents' first amendment rights by explicitly prohibiting law enforcement agencies from collecting information about individuals' political and religious views, associations, or activities, unless that information directly relates to an investigation that is based on reasonable suspicion of criminal conduct. Unless we insist upon this

familiar standard for investigations, the fundamental rights upon which our Commonwealth was founded – the right to assemble with like-minded people, the right to protest government activity, the right to worship freely according to one's own conscience – will be dangerously chilled and undermined.

2. Establish Independent Oversight, Auditing and Public Reporting

Effective oversight of executive branch programs like the Commonwealth Fusion Center must be independent, apply independently-developed standards, and have the authority to enforce those standards or provide analysis and recommendations to another entity with such authority. The legislature should create an oversight mechanism for intelligence data center operations throughout the state, either in the form of a new office empowered to audit and investigate the activities of the Fusion Center, BRIC, and like entities, or by statutorily authorizing an existing independent watchdog office, such as the Office of the Inspector General, to conduct such investigations.

Such an office must also make public reports of its findings to the legislature or appropriate legislative committees. Only by publicizing findings and giving the legislature a monitoring role can meaningful oversight take place. Investigative authority must be coupled with public reporting to hold otherwise unaccountable institutions to agreed-upon standards.

3. Ensure Transparency for Individuals and The Public

To further ensure accountability, new intelligence programs must also respect the public's right to know about their operations. Indeed, the Department of Homeland Security has endorsed the application of fair information principles – including transparency – to fusion centers' collection and management of data containing personally identifiable information.[135] Both the policies of the new intelligence programs and the general laws should clearly state that public records laws apply to these institutions, so people can have access to information about their government.

Furthermore, the exemption for all "intelligence information" under the state Fair Information Practices Act should be amended so that it is not overbroad. In general, individuals should be able to learn what information the government maintains about them, and any exemptions should be narrowly tailored to reflect specific objectives, such as protecting people from harm and maintaining appropriate secrecy about ongoing investigations.

4. Develop Standards for Data Integrity, Security, and Privacy

Intelligence operations are only as effective as their information is accurate and reliable. To this end, the legislature should establish commonsense standards regarding data collection, validation, and accuracy. In addition, it must safeguard residents' privacy by developing standards for data use, retention, and dissemination to ensure that intelligence data centers operate in keeping with established principles regarding individual rights under Massachusetts law.

By taking these steps, the Massachusetts legislature can create a model for the nation to follow, and help ensure that the national surveillance security complex being erected in the Commonwealth and across the country does not become the apparatus of a police state. Our fundamental freedoms hang in the balance.

ENDNOTES

[1] Peter Baker & Carl Hulse, *U.S. Had Early Signals of a Terror Plot, Obama Says*, N.Y. Times, Dec. 30, 2009.
[2] Jeff Zeleny & Helene Cooper, *Obama says Plot Could Have Been Disrupted*, N.Y. Times, Jan. 6, 2010.
[3] Mike German & Jay Stanley, *Fusion Center Update*, July 2008, ACLU report available at http://www.aclu.org/pdfs/privacy/fusion_update_20080729.pdf
[4] Rep. Brad Miller (D-NC), chairman of the Subcommittee on Investigations and Oversight of the Committee on Science and Technology, wrote a letter on August 21, 2008 to the Inspector General of the Office of the Director of National Intelligence in which he states that "a significant portion of the estimated $300 million dollars spent on Railhead has been inappropriately used to renovate a building of one of the prime contractors, The Boeing Company" and cites a Government Accountability Office report on federal investment in information technology programs: "413 government IT projects totaling more than $25 billion in FY2008 alone were 'poorly planned, poorly performing, or both.'"
http://democrats.science.house.gov/Media/File/AdminLetters/bm_InspectorGeneralMaquire_terrorwatchlist_8.21.08.pdf
[5] The 2002 film Minority Report features a specialized 'Department of Pre Crime,' where psychic 'precogs' discern which 'criminals' to pursue before they commit crimes.
[6] Alan Perrott, *Echelon: Spying Chain's Cover Blown*, The Independent (UK), July 14, 2001.
[7] *Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001 by the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence*, July 25, 2003. The report was dated December 2002 and finally released in redacted form after months of wrangling within the Bush Administration about which parts could be declassified.
[8] *Summary of the White House Review of the December 25, 2009 Attempted Terrorist Attack,* The White House, Jan. 7, 2010.
[9] The Intelligence Reform and Terrorism Act of 2004 created the National Counterterrorism Center to integrate and analyze threat information from a wide variety of government agencies and networks. See its website http://www.nctc.gov/
[10] Rep. Brad Miller in his August 21, 2008 letter (*supra* note 4) detailed TIDE's technical problems: its failure to properly process tens of thousands of "potentially vital CIA messages," fundamental design flaws that make the data in the system difficult or even impossible to search, its tendency to crash, the fact "that there is no fool proof way to ensure that only good data gets into the TIDE database and unqualified data stays out," the fact that the attempt to fix it by developing the fatally flawed $300 million dollar 'Railhead' system has only made the problems worse.
[11] In a *Follow Up Audit of the Terrorist Screening Center* (September 2007) the U.S. Department of Justice's Inspector General for the Audit Division reported that the FBI's terrorism database had over 700,000 names by April 2007 and was growing at a rate of 20,000 records per month.
[12] These are the numbers cited in Kevin Whitelaw, *Watching for Terrorists: Many Names, Many Lists*, National Public Radio, Jan. 7, 2010. On the list of those mandated for screening is eight-year-old Mikey Hicks, who has faced hassles getting on planes since he was a baby. He was profiled in the N.Y. Times (*Meet Mikey, 8: U.S. Has Him On Watch List*, Jan. 14, 2010). Over 80,000 people have asked to be taken off the list. The number of those slated for extra screening at airports ballooned when the Obama Administration in early 2010 mandated additional scrutiny for passengers from 14 countries. Within four months this policy was rescinded and a new policy introduced that focused a 'tailored' use of intelligence data (*Security Checks on Flights to U.S. to be Revamped: Focus on Sifting Data*, N.Y. Times, April 2, 2010).
[13] Walter Pincus, *1,600 Daily are Considered for the FBI's List*, Wash. Post, Nov. 1, 2009.
[14] *Statement of Timothy Healy, Director, Terrorist Screening Center, before the Senate Homeland Security and Governmental Affairs Committee*, Dec. 9, 2009.
[15] Associated Press, *F.B.I. Hit for Backlog in Evidence Review*, Boston Globe, Oct. 27, 2009.
[16] Charlie Savage, *F.B.I. Slow to Translate Intelligence, Report Says*, N.Y. Times, Oct. 27, 2009.

[17] *Remarks as prepared for delivery by Dr. John Poindexter, Director, Information Awareness Office of DARPA*, at DARPA Tech 2002 Conference, Anaheim, Calif., Aug. 2, 2002, available at http://www.fas.org/irp/agency/dod/poindexter.html

[18] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, Executive Summary, 24 (July 2004).

[19] John Markoff, *Threats and Responses: Intelligence: Pentagon Plans a Computer System That Would Peek at Personal Data of Americans*, N.Y. Times, Nov. 9, 2002.

[20] *Id*.

[21] Justice Louis D. Brandeis, *Olmstead v. United States*, 277 U.S. 438, 478 (1928).

[22] Bob Barr & Laura Murphy, *Ideological Foes Agree: Privacy in Danger*, Atlanta Journal Constitution, May 16, 2003.

[23] Gene Healy, *Beware of Total Information Awareness*, Cato Institute, Jan. 20, 2003.

[24] Barr & Murphy, *supra* note 22.

[25] Mark Williams, *The Total Information Awareness Project Lives On*, Technology Review, April 26, 2006.

[26] Shane Harris, *TIA. Lives On*, National Journal, Feb. 23, 2006.

[27] Ryan Singel, *Newly Declassified Files Detail Massive FBI Data-Mining Project*, Wired Magazine, Sept. 23, 2008.

[28] Anita Ramasastry, *The FBI STAR Terrorist Risk Assessment Program Should Raise Renewed Concerns about Private Sector Data Mining*, Find Law, July 24, 2007.

[29] Ellen Nakashima, *FBI Prepares Vast Database of Biometrics: $1 Billion Project to Include Images of Irises and Faces*, Wash. Post, Dec. 22, 2007.

[30] Paul Marks, *Pentagon Sets its Sights on Social Networking Websites*, New Scientist, June 9, 2006.

[31] Siobhan Gorman, *NSA.'s Domestic Spying Grows as Agency Sweeps Up Data*, Wall St. Journal, March 10, 2008.

[32] Ann Broache, *Report: DHS Kills Data-mining Project*, Cnet News, Sept. 8, 2007.

[33] Committee on Technology and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals et al, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment*, National Research Council, Oct. 2008.

[34] John Rollins, *Fusion Centers: Issues and Options for Congress, Congressional Research Service Report for Congress*, 7 Jan. 18, 2008.

[35] A former C.I.A. Director of Intelligence Collection, Charles Allen served as the Department of Homeland Security's Undersecretary for Intelligence and Analysis and Chief Intelligence Officer from 2005 – 2009.

[36] *Statement of Eileen R. Larence, Director, Homeland Security and Justice Issues*, GAO-07-1214T, 1-2.

[37] *Id*. Of the 72 current fusion centers, 50 are state-designated centers and 20 major urban area centers.

[38] Information on the Nationwide SAR Initiative can be found at http://www.ise.gov/pages/sar-initiative.aspx. See also Thomas Cincotta, *Platform for Prejudice: How the Nationwide Suspicious Activity Reporting Initiative Invites Racial Profiling, Erodes Civil Liberties, and Undermines Security*, Political Research Associates (2010); *Final Report: Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Evaluation Environment*, Bureau of Justice Assistance, Jan. 2010.

[39] *Building Communities of Trust Project, The Bureau of Justice Assistance – in Partnership with the Program Manager for the Information Sharing Environment*, White Paper distributed at a meeting in Boston, Oct. 7, 2009.

[40] http://www.aclu.org/privacy/gen/39226prs20090401.html

[41] See Mike German & Jay Stanley, *What's Wrong with Fusion Centers?* American Civil Liberties Union, Dec. 2007, http://www.aclu.org/pdfs/privacy/fusioncenter_20071212.pdf; http://www.aclu.org/pdfs/privacy/fusion_update_20080729.pdf

[42] *Fusion Center Update*, *supra* note 3, at 7-8.

[43] http://www.aclu.org/safefree/general/39501prs20090430.html and http://www.aclu.org/privacy/gen/39333prs20090406.html

[44] North Central Texas Fusion System Prevention Awareness Bulletin, Feb. 19, 2009, available at http://www.baumbach.org/fusion/PAB_19Feb09.doc.

[45] T.J. Greaney, *Fusion Center Data Draws Fire over Assertions*, Columbia Daily Tribune, March 14, 2009.

[46] *Privacy Impact Assessment for the Department of Homeland Security State, Local, and Regional Fusion Center Initiative*, Dec. 11, 2008, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ia_slrfci.pdf

[47] *Id*.
[48] Bryan Bender, *Massachusetts Governor Hopes to Enlist Citizens in Antiterrorism Effort*, Knight Ridder/Tribune Business News, Sept. 2003.
[49] Pam Belluck, *States and Cities Must Hunt Terror Plots, Mass. Governor Says*, N.Y. Times, Dec. 21, 2004.
[50] *DOJ Evaluation and Inspections Report 1 – 2005-007*, June 2005. In 2005 the budget for JTTF activities was $375 million.
[51] *Boston Joint Terrorism Task Memorandum of Agreement*, signed January 17, 2003 [on file with the ACLU of Massachusetts].
[52] While general authority for the criminal information and intelligence collection functions of the Massachusetts State Police was provided by the Massachusetts legislature in the 1991 reorganization of the state police forces, the transformative expansion of the Commonwealth's investigative and intelligence activities and their integration into a national intelligence network was accomplished through a series of executive decisions during the Romney Administration.
[53] *Letter from Juliette N. Kayyem, Undersecretary for Homeland Security*, Executive Office of Public Safety, March 10, 2008.
[54] *Id*.
[55] *Statement of Eillen R. Larence*, *supra* note 36, at 9.
[56] *Romney Executive Order No. 476*, 7.
[57] *Id*., 8.
[58] Todd Masse, Siobhan O'Neil & John Rollins, *CRS Report for Congress: Fusion Centers: Issues and Options for Congress*, Congressional Research Service, July 6, 2007, note 2, 21.
[59] *Privacy Impact Assessment, supra* note 46.
[60] *Letter from Juliette N. Kayyem*, *supra* note 53.
[61] Ben Bain, *Strategy Refines Fusion Center's Role*, Federal Computer Week, Nov. 5, 2007.
[62] Homeland Security Advisory Council 2005, 4.
[63] *Letter from Juliette N. Kayyem*, *supra* note 53.
[64] *Interview with CFC Officials*, Maynard, MA, April 7, 2009.
[65] *Standard Operating Procedure (SOP)*, Commonwealth Fusion Center, Number CFC-04, effective date March 5, 2008. *Guidelines for Investigations Involving First Amendment Activity*, 4.
[66] *Letter from Juliette N. Kayyem*, *supra* note 53.
[67] FOIA Doc: CFC *SOP*, *supra* note 65.
[68] *Id*.
[69] *Intelligence-Led Policing: The New Intelligence Architecture, New Realities: Law Enforcement in the Post 9/11 Era*, Bureau of Justice Assistance, Sept. 2005 NCJ 210681.
[70] *Solicitation: Predictive Policing Demonstration and Evaluation Program*, CFDA No. 16.560, U.S. Department of Justice, SL#000877.
[71] *Annual Repor*t, Boston Police Department, 2005.
[72] *Id.*
[73] *Id*.
[74] *Press Release*, Boston Police Department, Sept. 11, 2009, http://www.cityofboston.gov/news/default.aspx?id=4350
[75] Siobhan Gorman, *LAPD Terror-Tip Plan May Serve As Model*, Wall St. Journal, April 15, 2008; Josh Meyer, *LAPD Leads the Way in Local Counter-Terrorism*, Los Angeles Times, April 18, 2008.
[76] Office of the Chief of Police, *Special Order No. 11, Reporting Incidents Potentially Related to Foreign or Domestic Terrorism*, Los Angeles Police Department, March 5, 2008 [on file with the ACLU].
[77] Global Information Sharing Initiative, Major City Chiefs Association & Department of Homeland Security, *Findings and Recommendations of the Suspicious Activity Report Support and Implementation Projec*t, Department of Justice, June 2008, http://online.wsj.com/public/resources/documents/mccarecommendation-06132008.pdf.
[78] Siobhan Gorman, *In Cities, the Fight against Terrorism Walks the Beat*, Wall St. Journal, Nov. 25, 2008.
[79] The SAR Initiative will be coordinated by the nation's 72 fusion centers. See *supra* note 38.
[80] *Information Sharing Environment (ISE) - Suspicious Activity Reporting (SAR), Functional Standard,* Section 5, g.

[81] *Id.* at v. 1.5, ISE-FS-200.
[82] *ISE-SAR Factsheet* http://www.ise.gov/docs/sar/Fact_Sheet_NSI_-_December_23_2008_Final.pdf
[83] *MassGangs: Project Overview*, Draft of Dec. 14, 2007 [on file with the ACLU of Massachusetts].
[84] *Id.*
[85] *The State of Homeland Security in the Commonwealth: Trends and Process*, Commonwealth of Massachusetts Oct. 2008, available at http://www.mass.gov/Eeops/docs/eops/hsd_oct_2_doc_final.pdf
[86] *Id.*
[87] Meeting with Commonwealth Fusion Center officials, April 7, 2009.
[88] *Id.*
[89] *Id.*
[90] *Biometrics Solutions: Secure Identity Management Systems*, Raytheon brochure, www.raytheon.com/capabilities/.../rtn_iis_biometrics_datasheet.pdf. *Raytheon Selected as Network Systems Integrator for Army Expeditionary Warrior Experiment*, Raytheon press release, Oct. 23, 2009. Elizabeth Woyke, *Raytheon Sends Android To Battlefield*, Forbes, Oct. 19, 2009. *Raytheon Develops World's Largest Infrared Light-Wave Detector*, Raytheon press release, Aug. 17, 2009.
[91] DHS Exhibit 300 Public Release BY 10/NPPD - US Visit - Automated Biometric Identification System, *The world's largest biometrics database is being built in West Virginia*, Homeland Security Newswire, Nov. 6, 2009.
[92] Kim Zetter, *Feds 'Pinged' Sprint GPS Data 8 Million Times over a Year,* Wired.com, Dec. 1, 2009.
[93] The DHS-funded surveillance cameras have been vigorously opposed in Cambridge and Somerville, and both the Cambridge City Council and the Somerville Town Meeting have demanded that they be dismantled.
[94] Massachusetts State Police Request for Information *re:* Data base software [on file with ACLU of Massachusetts].
[95] *Id.*
[96] *Protecting America from Terrorist Attack: Meet the National Joint Terrorism Task Force*, F.B.I., July 2, 2005, www.fbi.gov/page2/july04/njttf070204.htm
[97] Michael German, *Testimony in Support of Senate Bill 931 Before the Joint Committee on Public Safety and Homeland Security, Massachusetts Legislature*, Oct. 21, 2009 [on file with ACLU of Massachusetts].
[98] *Information Technology: OMB and Agencies Need to Improve Planning, Management, and Oversight of Projects Totaling Billions of Dollars, Testimony by David A. Powner, Director, Information Technology and Management Issues*, Government Accountability Office, GAO-08-105IT, July 31, 2008.
[99] Rep. Miller, *supra* note 4.
[100] Eric Schmitt & David Johnston, *States Chafing at U.S. Focus on Terrorism*, N.Y. Times, May 26, 2008.
[101] The MBTA has categorized 51 unfunded infrastructure projects as representing danger to "life and limb." Noah Bierman, *A System under Strain*, Boston Globe, Dec. 6, 2009.
[102] Anti-Terrorism Advisory Council Meeting, Moakley Courthouse, Boston, May 18, 2005.
[103] Peter Watchorn, *A Cautionary Tale, March 13, 2008, evidence submitted to the Joint Committee on Public Safety and Homeland Security*, Oct. 21, 2009 [on file with the ACLU of Massachusetts].
[104] I*ntelligence-Led Policing: The New Intelligence Architecture, New Realities: Law Enforcement in the Post 9/11 Era*, Bureau of Justice Assistance, 9 (Sept. 2005), NCJ 210681.
[105] FOIA Doc: *CFC-SOP, supra* note 65 (on First Amendment).
[106] *Id.*
[107] *Fusion Center Update*, *supra* note 3, at 6-7. See also *Mass Impact: The Domestic War Against Terrorism in Massachusetts – Are We On The Right Track?*, ACLU of Massachusetts, May 2004.
[108] Andrea Estes & Peter Schworm, *Police Prying into Stars' Data*, Boston Globe, May 6, 2009.
[109] http://www.aclu.org/safefree/general/17079prs20021212.html
[110] *Fusion Center Update, supra* note 3.
[111] http://www.aclu.org/privacy/gen/39226prs20090401.html
[112] Among the systems used by the Fusion Center is the Autotrack search engine now operated by West which provides access to billions of records about individuals.
[113] Robert O'Harrow, Jr., *Centers Tap into Personal Databases*, Wash. Post, April 2, 2008.

[114] FOIA Doc: *CFC-SOP*, *supra* note 65, CFC-05, July 1, 2006 (*CFC Privacy Policy*). Under the heading of "Collection Limitation," for example, the policy states that it is the responsibility of the source agency rather than the Fusion Center to observe limits on collection of information. Participating agencies are similarly responsible for the quality and accuracy of data accessed by the Fusion Center.
[115] *Id*. ("Data Quality"), 2.
[116] *Id*. ("Openness"), 3.
[117] The Privacy Working Group (PWG) of the Executive Office of Public Safety and Security was established by the Secretary of Public Safety and Security on August 7, 2008 to advise the Secretary on "information security, individual privacy, data integrity and other privacy related matters." The meetings of the PWG are not open to the public, and any recommendations it may have made concerning privacy have not been incorporated in the *CFC Privacy Policy*.
[118] G.L. c. 66A, §§ 1 *et seq*.
[119] *Swartz v. Department of Banking & Insurance,* 376 Mass. 593, 597 (1978), citing Special Legislative Commission on Privacy—First Interim Report, 1975 House Doc. No. 5417.
[120] G.L. c. 66A, §§ 1-2. "Personal data" does not include information contained in a public record, as defined by G.L. c. 4, § 7 cl. 26, or information relating to specific criminal investigations or prosecutions.
[121] FOIA Doc: *CFC-SOP, supra* note 65.
[122] 28 CFR Part 23.
[123] *Memorandum from Kevin M. Burke, Secretary,* Executive Office of Public Safety and Security, Aug. 7, 2008.
[124] *Memorandum from the Privacy Working Group Members*, Executive Office of Public Safety, 2008.
[125] Department of Justice Office of Inspector General, *The Department of Justice's Internal Controls Over Terrorism Reporting Audit Report 07-20*, February 2007, http://www.justice.gov/oig/reports/plus/a0720/final.pdf
[126] *Letter from Juliette N. Kayyem*, *supra* note 53.
[127] *Id*.
[128] *Id*.
[129] FOIA Docs: MOUS with MBTA and others.
[130] FOIA Doc: MOU between CFC and Massachusetts National Guard.
[131] G.L. c. 4, § 7 cl. 26.
[132] FOIA Doc: *CFC Privacy Policy*, *supra* note 114, at 3.
[133] See EPIC reports describing challenge to a similar agreement by Virginia's fusion center, http://epic.org/privacy/virginia_fusion/
[134] CRS Report for Congress, *Intelligence and Information-Sharing Elements of S.4 and H.R. 1*, June 26, 2007. See also Dan Olson, *Fusion centers protect us, but at what cost?* Minnesota Public Radio, Dec. 16, 2008, available at http://minnesota.publicradio.org/display/web/2008/12/16/fusion_centers_privacy/
[135] *Privacy Impact Assessment for the Department of Homeland Security State, Local, and Regional Fusion Center Initiative*, Dec. 11, 2008.

Produced by
The American Civil Liberties Union of Massachusetts
211 Congress Street
Boston, MA 02110
tel (617) 482 3170
fax (617) 451 0009
www.aclum.org