Statement of Caroline Fredrickson, Director

American Civil Liberties Union Washington Legislative Office

On

"Protecting National Security and Civil Liberties: Strategies for Terrorism Information Sharing"

Before the Subcommittee on Terrorism and Homeland Security

Senate Committee on the Judiciary

April 21, 2009

Good morning Chairman Cardin, Ranking Member Kyl, and Members of the Subcommittee. Thank you for the opportunity to testify on behalf of the American Civil Liberties Union, its hundreds of thousands of members and fifty-three affiliates nationwide, regarding terrorism-related information sharing among federal, state, local and tribal law enforcement. The ACLU recognizes a legitimate need to share lawfully-collected information regarding terrorism and other criminal activity among law enforcement agencies at the federal, state, local and tribal levels in an effective and efficient manner. Improving information sharing sounds like a fine goal in the abstract, but increasing the government's authority to collect and disseminate personally identifiable information about Americans in the absence of reasonable suspicion and a specified law enforcement purpose poses significant risks to our privacy and civil liberties.[1] In our view, any effort to expand information sharing among law enforcement agencies must be accompanied by independent oversight mechanisms and a rigorous set of standards to ensure the use of proper methods, to preserve the privacy of innocent individuals, and to maintain the accuracy and usefulness of the shared information.

The police power to investigate, when combined with the secrecy necessary to protect legitimate law enforcement operations, provides ample opportunity for error and abuse. The potential for abuse expands as the amount of information collected and the number of entities it is shared with increases. By its very nature, criminal intelligence information is often uncorroborated, inadequately vetted and fragmentary. At its worst, it is unreliable, misleading or just plain wrong. Just one thing is certain about 'intelligence:' it is only valuable to our security when it is true. If the information collected and shared among law enforcement agencies is inaccurate or irrelevant to a legitimate law enforcement function, sharing it will not improve security, and very well may damage it. Our concerns about information sharing lie in the details. We want to know what information is being collected, who is collecting it, what is done with the information once it has been collected, what authorities regulate these activities, and who is ultimately responsible for ensuring compliance with applicable federal, state, and local laws?

Our testimony examines historical abuses of police intelligence collection and information sharing practices, the guidelines and regulations implemented to curb this abuse, and the steady erosion of these regulations after the terrorist attacks of September 11, 2001. In just the past few years the ACLU has uncovered numerous examples of abusive police intelligence operations at all levels of government targeting non-violent individuals and organizations engaged in First Amendment-protected activity. These unjustified and unnecessary investigations don't just violate the rights of the individuals involved. They harm security by misdirecting resources away from real threats and by polluting terrorism databases with erroneous information. They damage our democracy by suppressing free expression and chilling participation in the political process. The ACLU urges this Subcommittee to intensify its oversight of information collection and sharing practices at all levels of government and to restore appropriate standards to regulate law enforcement information collection and sharing, both to reduce the instances of abuse and to focus our security resources against real threats.

I. HISTORY OF ABUSE OF DOMESTIC INTELLIGENCE PROGRAMS

Last year the ACLU of Maryland exposed an extensive Maryland State Police (MSP) spying operation that targeted at least 23 non-violent political advocacy organizations based

solely on the exercise of their members' First Amendment rights.[2] The MSP surveillance activities were aimed at an array of political and religious organizations, including peace advocates like the American Friends Service Committee (a Quaker organization) and Women in Black (a group of women who dress in black and stand in silent vigil against war), immigrants rights groups like CASA of Maryland, human rights groups like Amnesty International, anti-death penalty advocates like the Maryland Citizens Against State Executions, and gay rights groups like Equality Maryland, among others. None of the MSP reports from these operations suggested any factual basis to suspect these groups posed any threat to security. Not surprisingly, no criminal activity was discovered during these investigations, some of which lasted as long as 14 months. Despite this lack of evidence, the MSP labeled many of these activists "terrorists," distributed information gathered in their investigations widely among Maryland law enforcement and intelligence agencies – including a local police representative of the FBI's Joint Terrorism Task Force, a National Security Agency security official, and an unnamed military intelligence officer –and uploaded the activists' personal information into a federal drug enforcement and terrorism database.[3] The Department of Homeland Security (DHS) was also involved, collecting and disseminating e-mails from of one of the peace groups to assist the MSP spying operations.[4] From a pure information sharing perspective, this case worked well. But the sharing of such misleading, erroneous and irrelevant information provided no security benefit to the people of Maryland, and only undermined the credibility of state and federal intelligence systems.

Such misguided police activity may seem shocking, but anyone who has studied law enforcement intelligence operations in the United States could have predicted it. History has shown that whenever a law enforcement agency takes on an intelligence gathering mission separate from its criminal justice mission, abuse follows and civil rights suffer. Untethered from a criminal predicate, police agencies begin to target people they feel don't fit in: political protesters, immigrants, and minorities.

During the Cold War, the FBI ran a domestic intelligence/counterintelligence program called COINTELPRO that quickly evolved from a legitimate effort to protect the national security from hostile foreign threats into an effort to suppress domestic political dissent through an array of illegal activities. The Senate Select Committee that investigated COINTELPRO (the "Church Committee") found that a combination of factors led law enforcers to become law breakers, including their perception that traditional law enforcement methods were ineffective in addressing the security threats they faced and their easy access to damaging personal information as a result of the unrestrained collection of domestic intelligence.[5] According to the Church Committee report, these agents saw themselves not just as law enforcement officers, but as "guardians of the status quo" responsible for "upholding decency and established morality, [and] defending the correctness of U.S. foreign policy…"[6] The Committee said the "unexpressed major premise of… COINTELPRO is that the Bureau has a role in maintaining the existing social order, and that its efforts should be aimed toward combating those who threaten that order."[7] In testimony before the Committee, White House liaison Tom Charles Huston, author of the infamous "Huston Plan," explained the hazards of expanding a law enforcement agency's mission beyond law enforcement:

> The risk was that you would get people who would be susceptible to political considerations as opposed to national security considerations, or would construe political considerations to be national security considerations, to move from the kid with a bomb to the kid with a picket sign, and from the kid with the picket sign to the kid with the bumper sticker of the opposing candidate.[8]

The FBI used the information it gleaned from these improper investigations not for law enforcement purposes, but to "break up marriages, disrupt meetings, ostracize persons from their professions and provoke target groups into rivalries that might result in deaths."[9] The Church Committee noted that the covert nature of these activities left the targets of this abuse with no protection in the law:

> Intelligence activity… is concealed from its victims and is seldom described in statutes or explicit executive orders. The victim may never suspect that his misfortunes are the intended result of activities undertaken by his government, and accordingly may have no opportunity to challenge the actions taken against him.[10]

FBI headquarters opened over 500,000 domestic intelligence files between 1960 and 1974, and created a list of 26,000 individuals who would be "rounded up" in the event of a national emergency.[11]

The abuse of intelligence powers was not limited to federal authorities, however. State and local police forces long maintained political intelligence units (also known as Anti-Subversive Squads, or Red Squads), which illegally spied upon and sabotaged numerous peaceful groups throughout the twentieth century.[12] They often amassed detailed dossiers on political officials and engaged in "disruptive" activities targeting political activists, labor unions, and civil rights advocates, among others. During the 1960's the New York City Police Department's radical squad, known as the Bureau of Special Services (BOSS), opened an average of one thousand political investigations a year, targeting such groups as the ACLU, the National Association for the Advancement of Colored People, and the Congress of Racial Equality.[13] By 1968 BOSS accumulated a master index of over one million individual entries.

II. REFORM AND REGULATION: FEDERAL, STATE AND LOCAL GUIDELINES

Revelations of these abusive law enforcement intelligence activities during the Watergate era led to a series of reforms. Congress sought to establish a statutory charter delineating the FBI's investigative authorities, as it had for the Central Intelligence Agency. To forestall such legislation, in 1976 Attorney General Edward Levi issued guidelines to regulate the FBI's activities. These "Attorney General Guidelines" (AGG) authorized the FBI to conduct "full" investigations only "on the basis of specific and articulable facts giving reason to believe that an individual or group is or may be engaged in activities which involve the use of force or violence."[14] The Levi guidelines did include some flexibility to allow the FBI to conduct "preliminary" and "limited" investigations when it had "information or allegations" that were not sufficient to open a full investigation, but these investigations were strictly limited in both time (90 days with the possibility of one 90 day extension) and in the techniques the FBI could employ, and their purpose was "confined to determining whether there is a factual basis for

opening a full investigation." The shortcoming of regulating FBI authority through AGG rather than through statute was that guidelines could be easily amended. Several different sets of guidelines were promulgated and they were altered many times over the ensuing years. In 1983, the "specific and articulable facts" standard was changed to a "reasonable indication" standard, which remained in place until 2002.[15]

The federal government also sought to establish clear guidelines for state and local law enforcement agencies engaged in the collection of criminal intelligence information. In 1979 Title 28, Part 23 of the Code of Federal Regulations was promulgated, requiring state and local law enforcement agencies receiving federal funding to:

> …collect, maintain, and disseminate criminal intelligence information in conformance with policy standards which are prescribed by the Office of Justice Programs and which are written to assure that… systems are not utilized in violation of the privacy and constitutional rights of individuals.[16]

In commentary published during a 1993 revision of the regulation, the Department of Justice Office of Justice Programs (OJP) explained the risks to civil liberties inherent in the collection of criminal intelligence, and the need for regulation of criminal intelligence systems:

> Because criminal intelligence information is both conjectural and subjective in nature, may be widely disseminated through the interagency exchange of information and cannot be accessed by criminal suspects to verify that the information is accurate and complete, the protections and limitations set forth in the regulation are necessary to protect the privacy interests of the subjects and potential suspects of a criminal intelligence system.[17]

Part 23 is designed to ensure that police intelligence operations are properly focused on illegal behavior by requiring that criminal intelligence systems "collect information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity." The Supreme Court had established "reasonable suspicion" as the necessary standard to allow a police officer to stop and frisk an individual for weapons in *Terry v. Ohio* in 1968, so it was a concept police already understood.[18] Over time, "reasonable suspicion" has become universally accepted by law enforcement agencies around the country as the appropriate standard for regulating the intelligence collection activities of law enforcement officers.

The Institute for Intergovernmental Research (IIR), a law enforcement training organization, devotes a website to Part 23 that explains why this decades-old regulation is relevant to today's law enforcement operations:

> The purpose of 28 CFR Part 23 is to ensure the constitutional and privacy rights of individuals. Today's environment of aggressive, proactive information collection and intelligence sharing is very similar to the environment that motivated Congress, in the Justice Systems Improvement Act of 1979, to require the issuance of 28 CFR Part 23 in the first place.[19]

The Association of Law Enforcement Intelligence Units called Part 23 "a valuable guide for all agencies with a criminal intelligence function, regardless of their funding sources."[20]

III. EROSION OF RELIABLE STANDARDS

A. AUTHORIZATION OF SURVEILLANCE WITHOUT SUSPICION

After the terrorist attacks of September 11, 2001, law enforcement agencies at all levels of government abandoned the traditional criminal justice approach in favor of an intelligence model. The federal government initiated a series of broad electronic surveillance and data collection programs based not on reasonable suspicion, but on an unproven theory that threats to our security could be detected and countered through massive data collection coupled with predictive data mining technology. Some of these efforts were authorized by Congress, while others were not.

Through the USA Patriot Act, for example, Congress expanded the FBI's authority to use National Security Letters (NSLs) to obtain telephone, credit and financial information so that these secret demands for information could be used against not just suspected terrorists or agents of foreign powers, but against anyone "relevant" to an FBI investigation.[21] Not surprisingly, a 2007 audit by the Department of Justice Inspector General confirmed widespread FBI mismanagement, misuse and abuse of this unchecked authority.[22] The audit revealed that the FBI managed its use of NSLs so negligently that it literally did not know how many NSLs it had issued. The IG found that FBI agents repeatedly ignored or confused the requirements of the NSL authorizing statutes, and used NSLs to collect private information against individuals two or three times removed from the subjects of FBI investigations. Twenty-two percent of the audited files contained unreported legal violations.[23] Most troubling, FBI supervisors used hundreds of illegal "exigent letters" to obtain telephone records without NSLs by falsely claiming emergencies.[24]

In 2008, the IG released a second audit report covering the FBI's use of NSLs in 2006 and evaluating the reforms implemented by the DOJ and the FBI after the first audit was released.[25] The new report identified many of the same problems discovered in the earlier audit. The 2008 NSL report showed that the FBI issued 49,425 NSLs in 2006 (a 4.7 percent increase over 2005), and confirmed the FBI was increasingly using NSLs to gather information on U.S. persons (57 percent in 2006, up from 53 percent in 2005).[26] The 2008 IG audit also revealed that high-ranking FBI officials improperly issued eleven "blanket NSLs" in 2006 seeking data on 3,860 telephone numbers.[27] None of these "blanket NSLs" complied with FBI policy and eight imposed unlawful non-disclosure requirements on recipients.[28] Moreover, these "blanket NSLs" were allegedly written to "cover information already acquired through exigent letters and other informal responses," which seemed to indicate intentional misconduct.[29]

But NSLs weren't the only surveillance authority abused. In December of 2005 the *New York Times* revealed that shortly after the 9/11 attacks the National Security Agency (NSA) began conducting warrantless domestic eavesdropping in violation of the Foreign Intelligence Surveillance Act.[30] Subsequent articles in *USAToday* alleged that major telecommunications companies "working under contract to the NSA" also provided the government domestic call

data from millions of Americans for "social network analysis."[31] Congress expanded the government's authority to eavesdrop on international communications without particularized suspicion, but a recent article in the *New York Times* revealed the NSA exceeded even those broad limits.[32]

Yet the information collected with these NSA warrantless wiretapping programs was reported to be of little value to FBI agents investigating terrorism.[33] Data produced by the Executive Office for United States Attorneys and analyzed by the Transactional Records Access Clearinghouse (TRAC) shows that from 2002 to 2008, as these surveillance programs increased, prosecutions of FBI international terrorism cases steadily dropped.[34] Perhaps more critical to evaluating the effectiveness of post-9/11 surveillance programs, however, is DOJ's increasing tendency to refuse to prosecute FBI international terrorism investigations. In 2006, the DOJ declined to prosecute a shocking 87% of the international terrorism cases the FBI referred for prosecution. Considering that only a tiny fraction of the many thousands of terrorism investigations the FBI opens each year are even referred for prosecution, it has become clear that the vast majority of the FBI's terrorism-related investigative activity is completely for naught – yet the FBI keeps all of the personally identifiable information it collects through these dubious investigations forever.[35]

Like so many of the broad information collection programs the intelligence community instituted over the last eight years,[36] these unfocused, ineffective collection programs appear to have been premised on the idea that data mining tools could later be developed to find meaning in these vast pools of collected information. A recent National Research Council study funded by the Department of Homeland Security calls this premise into serious question, however, and may explain why these programs do not seem to have produced demonstrable results. The study concluded:

> Automated identification of terrorists through data mining (or any other known methodology) is neither feasible as an objective nor desirable as a goal of technology development efforts. One reason is that collecting and examining information to inhibit terrorists inevitably conflicts with efforts to protect individual privacy. And when privacy is breached, the damage is real. The degree to which privacy is compromised is fundamentally related to the sciences of database technology and statistics as well as to policy and process.[37]

B. AMENDING THE ATTORNEY GENERAL GUIDELINES

The AGG underwent four separate changes under the Bush administration alone.[38] Attorney General John Ashcroft first amended the guidelines in 2002 to expand the investigative techniques the FBI could use during preliminary inquiries, and to increase the time limits to 180 days with the possibility of two or more 90 day extensions. [39] Under the Ashcroft guidelines only mail openings and non-consensual electronic surveillance were prohibited during preliminary inquiries, meaning the FBI could conduct intrusive investigations of people for an entire year without facts and circumstances establishing a "reasonable indication" that the subjects were engaged in criminal activity. The Ashcroft guidelines also allowed FBI agents to "visit any place and attend any event that is open to the public, on the same terms and conditions

as members of the public generally." The FBI later claimed this authority did not require the FBI agents attending public meetings to identify themselves as government officials. Abuse quickly followed. In 2005 the IG audited the FBI's compliance with AG Guidelines and found significant deficiencies: 53 % of the audited preliminary inquiries that extended beyond the initial 180-day authorization period did not contain necessary documentation authorizing the extension, and 77% of those that extended past the first 90-day extension period lacked the required authorizations. The IG audit was unable to determine whether or how frequently agents attended public events, however, because the FBI failed to keep records of such activity.

One illustration of the excess of the Ashcroft guidelines is that all of the investigative activity known to have taken place during the MSP spying operations targeting peaceful advocacy organizations would arguably have been authorized in preliminary inquiries conducted under the Ashcroft guidelines. There is no evidence the MSP opened mail or engaged in non-consensual electronic monitoring during their investigations, which were the only prohibited investigative techniques in preliminary inquiries. The only constraint in the Ashcroft guidelines that could have prevented a spying operation like the one the MSP conducted was the requirement of "information or an allegation which indicates the possibility of criminal activity." This slight factual prerequisite was the only limitation protecting innocent Americans from a year or more of intense FBI scrutiny.

Unfortunately, the FBI was not content with such excessive power and in December 2008, Attorney General Michael Mukasey instituted new guidelines that authorized the FBI to conduct intrusive "assessments" without requiring any factual predicate to justify an investigation. The Mukasey guidelines allow the FBI to utilize a number of intrusive investigative techniques during assessments, including physical surveillance, retrieving data from commercial databases, recruiting and tasking informants to attend meetings under false pretenses, and engaging in "pretext" interviews in which FBI agents misrepresent their identities in order to elicit information. These "assessments" can even be conducted against an individual simply to determine if he or she would be a suitable FBI informant. Nothing in the new Guidelines protects entirely innocent Americans from being thoroughly investigated by the FBI. The new Guidelines explicitly authorize the surveillance and infiltration of peaceful advocacy groups in advance of demonstrations, and they do not clearly prohibit using race, religion, or national origin as factors in initiating assessments.

C. TURNING STATE AND LOCAL POLICE INTO INTELLIGENCE AGENTS

State and local law enforcement also moved away from traditional law enforcement during this period and embraced a concept called intelligence-led policing (ILP). ILP focuses on the gathering and analysis of "intelligence" in the pursuit of proactive strategies "geared toward crime control *and quality of life issues* (emphasis added)."[40] One law enforcement official described ILP as policing that is "robust enough" to resist "terrorism as well as crime *and disorder* (emphasis added)."[41] If this language is eerily reminiscent of the rhetoric FBI agents used to defend COINTELPRO, it should not be surprising. Just last month at a hearing on Homeland Security Intelligence in the House of Representatives, Commerce, Georgia Chief of Police John Gaissert testified: "The street cop isn't looking for the normal. He's looking for the

abnormal."[42] The tendency for law enforcement to see the outsider as a potential threat has not diminished with the passage of time.

This new theory of criminal intelligence argues that collecting even outwardly innocuous behaviors will somehow enhance security. In 2006, former DHS Secretary Michael Chertoff said,

> Intelligence is about thousands and thousands of routine, everyday observations and activities. Surveillance, interactions – each of which may be taken in isolation as not a particularly meaningful piece of information, but when fused together, give us a sense of the patterns and flow that really is at the core of what intelligence is all about.[43]

In case the implications for civil liberties were not obvious enough, the Chief of the Lexana, Kansas Police Department described how she uses ILP programs to improve community awareness:

> Here in Lexana we have incorporated this element into our Crime Resistant Community Policing Program. We conduct regular trainings with the maintenance and rental staffs of apartment complexes, motels, and storage facilities. We show them how to spot and identify things *like printed terrorist materials and propaganda* and unique weapons of mass destruction like suicide bomb vests and briefcases (emphasis added).[44]

ILP did more than just train motel maids in Kansas to identify terrorist propaganda; it introduced a new institution into American life: the intelligence fusion center. Fusion centers are a direct institutional outgrowth of ILP, which promotes information collection and sharing as a strategy for preventative law enforcement, emphasizing the use of data mining technology in order to find patterns of potential criminal or terrorist behavior in a community. Intelligence fusion centers grew in popularity among state and local law enforcement officers as they sought to establish a role in defending homeland security by developing their own intelligence capabilities. These centers evolved largely independently of one another, beginning in about 2003, and were originally tailored to meet local and regional needs.

This growth took place in the absence of any legal framework for regulating fusion centers' activities. This lack of regulation quickly led to "mission creep," in which fusion centers originally justified as anti-terrorism initiatives rapidly drifted toward an "all-crimes, all-hazards" policy "flexible enough for use in all emergencies."[45] The leadership at some fusion centers has admitted that they switched to an "all-hazards" approach so they could apply for a broader range of grants, and because there was far too little terrorism-related information to analyze:

> [I]t 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.[46]

An intelligence capability without a well-defined mission is an unnecessary risk to liberty.

As fusion centers proliferated, national efforts at bolstering, defining and standardizing these institutions on the part of governors and the federal government began to intensify.[47] The federal government began providing facilities, manpower and financial resources to fuel the growth of these state and local intelligence centers. In 2006, the Departments of Justice and Homeland Security produced a report, "Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era," (the FC Guidelines) which outlined the federal government's vision for the centers, and sought to encourage and systematize their growth. "Intelligence sharing among states and jurisdictions will become seamless and efficient when each fusion center uses a common set of guidelines," the agencies proclaimed.[48] The FC Guidelines defined a fusion center as a "collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity."[49] These goals are laudable and appropriate for any law enforcement intelligence operation, as we all want the police to protect us from criminals and terrorists. But the voluntary federal guidelines then go on to encourage fusion centers to broaden their sources of data "beyond criminal intelligence, to include federal intelligence as well as public and private sector data."[50]

The FC Guidelines envision fusion centers doing more than simply sharing legitimately acquired law enforcement information across different levels of government. They encourage fusion centers to compile data "from nontraditional sources, such as public safety entities and private sector organizations" and combine it with federal intelligence produced by the federal intelligence community "to anticipate, identify, prevent, and/or monitor criminal and terrorist activity."[51] At a fusion center, threat assessments and information related to public safety, law enforcement, public health, social services and public works could be 'fused' with federal data containing personally identifiable information whenever a "threat, criminal predicate, or public safety need is identified."[52] The FC Guidelines also encourage fusion centers to invite a wide range of public safety, public works, social services, and private sector entities to participate, and some fusion centers include National Guardsmen as well as active duty military personnel.

D. FAILURE TO ENFORCE EXISTING REGULATIONS

Such broad information collection and dissemination would obviously exceed the limitations imposed by 28 C.F.R. Part 23. Yet the federal government actively encourages the violation of the regulation. The FCG encourage fusion centers to broaden their sources of data "beyond criminal intelligence, to include federal intelligence as well as public and private sector data."[53] Rather than being constrained by the law regarding what they can collect, Delaware State Police Captain Bill Harris, head of the Delaware Information Analysis Center (DIAC), appeared to feel constrained only by resources: "I don't want to say it's unlimited, but the ceiling is very high… When we have the money, we'll start going to those other agencies and say, 'Are you willing to share that database and what would it cost.'"[54] The federal official in charge of the High Intensity Drug Trafficking Area Task Force that controlled the database in which the MSP placed erroneous information about the peaceful activists they spied on later said it was up

to the participating state and local agencies to monitor their own compliance with the federal regulation.[55]

In January 2008 the Office of Director of National Intelligence (ODNI) Information Sharing Environment (ISE) Program Manager published functional standards for state and local law enforcement officers to report 'suspicious' activities to fusion centers and the ISE.[56] The behaviors described as inherently suspicious included such innocuous activities as photography, acquisition of expertise, and eliciting information. We are already seeing the results of such a program as police increasingly stop, question and even detain innocent Americans engaging in First Amendment-protected activity to collect their personal information for later use by the intelligence community.[57] This type of information collection does not improve security; it merely clogs criminal intelligence and information sharing systems with irrelevant and useless data. The ACLU and other privacy and civil liberties advocates are working with the ISE Program Manager, and with several state and local law enforcement agencies such as the Los Angeles Police Department, to modify these programs to avoid abrogation of First Amendment rights and federal regulations. While these efforts show some progress in strengthening privacy guidelines for these programs, even the best internal controls have rarely proved sufficient to eliminate abuse in secret intelligence operations.

And unfortunately, rather than cooperate with one another, the various federal intelligence agencies still seem to compete. Though the Intelligence Reform and Terrorism Prevention Act of 2004 established the ODNI ISE as the primary mechanism for the sharing of terrorism information, homeland security information, and law enforcement information among federal departments and agencies, state, local, and tribal governments, and private sector entities, the FBI recently introduced its own network for sharing suspicious activity reports from state and local law enforcement, eGuardian.[58] As it stands now there are several avenues for state and local governments to engage with the federal government to share law enforcement information: the DHS Office of Intelligence and Analysis, the FBI Joint Terrorism Task Forces, the ODNI ISE, and the fusion centers. Likewise there are several different portals to receive information: Law Enforcement Online (LEO), the National Data Exchange (N-Dex), the National Law Enforcement Telecommunication System (NLETS), the FBI's Guardian and now eGuardian systems, and the Homeland Secure Information Network (HSIN) to name just a few. The problem from a civil rights perspective is that the existence of competing intelligence programs creates the incentive for each agency to collect and report more information than the others to prove its value, to the detriment of the privacy and liberties of ordinary Americans. Indeed, the FBI appears to want to bend the rules in order to collect more information than the other systems. FBI documents distributed at the 2009 National Fusion Center Conference misstate federal regulations by asserting "[i]nformation that is deemed inconclusive will be maintained in eGuardian for a maximum of five years in accordance with 28 Code of Federal Regulations (CFR) Part 23." Of course the regulation does not allow for the collection or retention of "inconclusive" information for any period of time. This Subcommittee should examine all these information sharing programs closely, assess whether they demonstrably improve security, and ensure that they operate in a manner that complies with the law and protects individual rights before authorizing federal resources to support them.

IV. EVIDENCE OF ABUSE

The erosion of reasonable limits on police powers has set the stage for a return of the abusive practices of the past. In recent years the ACLU has uncovered substantial evidence that domestic intelligence powers are being misused at all levels of government to target non-violent political activists. In addition to the abusive MSP investigations discovered by the ACLU of Maryland, the ACLU of Colorado uncovered illegal surveillance of peaceful protestors and environmental activists by the Denver Police and the FBI,[59] and the ACLU of Northern California produced a report of widespread illegal spying activities by federal, state and local officials.[60] ACLU Freedom of Information Act litigation revealed JTTF investigations targeting peace activists in Pennsylvania and Georgia, and Department of Defense intelligence operations targeting anti-military protestors from around the country.[61]

The revelation that DHS was involved in collecting and disseminating the e-mails of one of the peace groups subjected to the MSP spying operation is alarming,[62] particularly because DHS representatives had previously denied that DHS had any information regarding the MSP investigations targeting these protesters.[63] In a letter to U.S. Senators Benjamin Cardin, Barbara Mikulski and Russ Feingold, DHS said it had done an "exhaustive" search of its databases and could find no information relating to the MSP surveillance operations. Yet MSP documents provided to the ACLU indicate that DHS Atlanta provided MSP with information regarding its investigation of the DC Anti-war Network (DAWN). An entry in the MSP files dated June 21, 2005 says:

> "The US Department of Homeland Security, Atlanta, recently forwarded two emails from [REDACTED] an affiliate of the DC DAWN Network and the [REDACTED]. Activists from DAWN, [REDACTED] and other groups working under the banner of [REDACTED] are going to stage several small (12-15) weekly demonstrations at the Silver Spring Armed Forces Recruitment Center (AFRC). If there is enough support these will become weekly vigils."[64]

Not only was DHS apparently aware of the MSP investigation, it was actually monitoring the communications of DAWN affiliates and forwarding them to MSP. We want to know how and why DHS obtained these e-mails (which contained no reference to any illegal activity), why DHS disseminated them to the MSP, and why DHS could not find records documenting this activity in the DHS databases.

Contrary to what DHS told the senators, a DHS spokesman quoted in the Washington Post said that law enforcement agencies exchange information regarding planned demonstrations "every day."[65] Indeed, a March 2006 "Protective Intelligence Bulletin" issued by the Federal Protective Service (FPS) lists several advocacy groups that were targets of the MSP operations, including Code Pink, Iraq Pledge of Resistance and DAWN, and contains a "civil activists and extremists action calendar" that details dozens of demonstrations planned around the country, mostly peace rallies. FPS apparently gleans this information from the Internet. However, it is still not clear under what authority DHS officials monitor the Internet to document and report on the activities of "civil activists," since there is no indication anywhere in the document to suggest illegal activity might occur at any of these demonstrations. What is clear is that MSP and DHS spying operations targeting peaceful activists serve no legitimate law enforcement, intelligence

or homeland security purpose. The operations threatened free expression and association rights, and they were a waste of time.

The MSP case wasn't the only evidence of abuse in DHS programs. An assessment published by DHS this month warned that right-wing extremists might recruit and radicalize "disgruntled military veterans,"[66] and an intelligence report produced for DHS by a private contractor smears environmental organizations like the Sierra Club, the Humane Society and the Audubon Society as "mainstream organizations with known or possible links to eco-terrorism."[67] Slandering upstanding and respectable organizations does not just violate the rights of these groups and those who associate with them; it undermines the credibility of all intelligence produced by and for DHS. There is simply no value in using our limited security resources to generate such intelligence products – and yet these events continue to occur.

The ACLU has also produced two reports detailing problems at intelligence fusion centers.[68] Since these reports were published a Texas fusion center supported by DHS released an intelligence bulletin that described a purported conspiracy between Muslim civil rights organizations, lobbying groups, the anti-war movement, a former U.S. Congresswoman, the U.S. Treasury Department and hip hop bands to spread Sharia law in the U.S.[69] The same month, but on the other side of the political spectrum, a Missouri Fusion Center released a report on "the modern militia movement" that claimed militia members are "usually supporters" of presidential candidates Ron Paul and Bob Barr.[70] In March 2008 the Virginia Fusion Center issued a terrorism threat assessment that described the state's universities and colleges as "nodes for radicalization" and characterized the "diversity" surrounding a Virginia military base and the state's "historically black" colleges as possible threats. These bulletins, which are widely distributed, would be laughable except that they come with the imprimatur of a federally-backed intelligence operation, and they encourage law enforcement officers to monitor the activities of political activists and racial and religious minorities.

What is clear is that these abusive intelligence reports do nothing to improve security. Sharing misleading information about the ideologies and activities of non-violent groups only undermines public support for law enforcement. FBI tactics targeting Arab and Muslim-Americans have so alienated the community that advocacy organizations that once teamed with the FBI threatened to end their cooperation with outreach efforts.[71]

V. RECOMMENDATIONS

1. Congress must intensify its oversight of all government information collection and sharing practices that implicate the rights of Americans. The collection and sharing of personally identifiable information about Americans pose serious risks to liberty and democracy, and the evidence of abuse is overwhelming. Past intelligence programs like the CIA's Operation Chaos, the NSA's Shamrock, the FBI's COINTELPRO, and the red squads of local police departments are infamous not just because they violated the rights of innocent Americans and undermined democratic processes, but also because they were completely ineffective in enhancing national security in any meaningful way.[72] It turns out, not surprisingly, that spying on innocent people is not useful to uncovering true threats to security. Unfortunately these lessons were ignored and we are increasingly seeing a return to abusive intelligence operations that target protest groups

and religious and racial minorities. Congress should examine and evaluate all information collection and sharing practices and bring an end to any government activities that are illegal, ineffective or prone to abuse. Three Patriot Act-related surveillance provisions expire at the end of this year, which gives Congress the opportunity to conduct a comprehensive review of all expanded post-9/11 intelligence authorities.[73]

2. Congress should not implement or fund new intelligence programs without empirical evidence that they effectively improve security. We should not sacrifice our liberty for the illusion of security. Fusion centers, in particular, should be audited to determine whether they can effectively serve a legitimate law enforcement function without violating the rights of innocent Americans. Any new effort to expand information sharing among law enforcement agencies must be accompanied by independent oversight mechanisms and a rigorous set of standards to ensure the use of proper methods, to preserve the privacy of innocent individuals, and to maintain the accuracy and usefulness of the shared information. Congress should review the National Research Council findings regarding the ineffectiveness of data mining as a counterterrorism tool, and should ban information collection programs that rely on data mining technology.

3. Congress should codify relevant portions of 28 C.F.R. Part 23 to establish a reasonable suspicion standard for all criminal intelligence information collection programs and to limit dissemination absent a legitimate law enforcement need. Reforms instituted after the exposure of abusive law enforcement intelligence programs were designed not only to protect the rights of innocent Americans, but also to help our law enforcement and intelligence agencies become more effective by focusing their resources on people they reasonably suspected of wrongdoing. Dissemination of criminal intelligence information to non-law enforcement entities should be prohibited unless necessary to avoid imminent danger to life or property. Congress should also provide a remedy for individuals who are harmed by intelligence activities conducted in violation of the regulatory standards.

4. Congress should ban racial profiling in all government intelligence and law enforcement programs and enact a legislative charter delineating the FBI's investigative authority. The statute should require a factual predicate establishing a reasonable suspicion that a person or organization is or will engage in illegal activity before the FBI may employ investigative techniques that implicate the privacy and civil rights of U.S. persons.

VI. CONCLUSION

While effective and efficient information sharing among law enforcement agencies is an important goal, we must remember that U.S. intelligence activities have too often targeted political dissent as a threat to security, which has led to misguided investigations that violated rights, chilled free expression and wasted the time and resources of our security agencies. Establishing new information collection and sharing authorities for the federal, state and local law enforcement poses significant risks to our individual liberties, our democratic principles and, ironically, even our security, particularly when fulfilling a broad and unfocused "all crimes, all hazards"[74] mandate. Frederick the Great warned that those who seek to defend everything defend nothing. Especially at a point in history when the troubled economy is regarded as the

most significant threat to national security, we must ensure that all of our security resources are used wisely and focused on real threats.[75] Congress should examine and evaluate all government intelligence and information sharing programs regularly and withhold funding from any activities that are unnecessary, ineffective or prone to abuse.

It would be an enormous mistake to ignore the lessons of past failure and abuse on a subject as critical as spying on the American people. We don't have to choose between security and liberty. In order to be effective, intelligence activities need to be narrowly focused on real threats, tightly regulated and closely monitored. We look forward to working with this Subcommittee to examine the abuse of these law enforcement authorities to spy on peaceful advocacy organizations. As the Supreme Court warned, "The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power."[76]

---

[1] The Government Accountability Office defined the term "personally identifiable information" as "any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, biometric records, and any other personal information that is linked or linkable to an individual." *See* GOVERNMENT ACCOUNTABILITY OFFICE, GAO 08-343, REPORT TO CONGRESSIONAL REQUESTERS: INFORMATION SECURITY: PROTECTING PERSONALLY IDENTIFIABLE INFORMATION, 5, n. 9, (Jan. 2008), *available at* http://www.gao.gov/new.items/d08343.pdf.

[2] *See,* ACLU of Maryland "Stop Spying" info page, http://www.aclu-md.org/Index%20content/NoSpying/NoSpying.html (last visited Apr. 15, 2009).

[3] MSP submitted the information to the Washington-Baltimore High Intensity Drug Trafficking Area Task Force (HIDTA) database. HIDTA is a federal program that provides funding and support to participating law enforcement agencies to support regional counter-drug and counter-terrorism efforts. *See*, 21 U.S.C. §1706 (2006).

[4] Lisa Rein, *Federal Agency Aided Md. Spying*, WASH. POST, Feb. 17, 2009, at B01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2009/02/16/AR2009021601131.html.

[5] SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, U.S. SENATE, 94TH CONG., FINAL REPORT ON SUPPLEMENTAL DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS (BOOK III), S. Rep. No. 94-755, at 10 (1976).

[6] *Id.*, at 7.

[7] *Id.,* at 7.

[8] *Id.*, at 27.

[9] SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, U.S. SENATE, 94TH CONG., FINAL REPORT ON SUPPLEMENTAL DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS (BOOK II), S. Rep. No. 94-755, at 5, (1976).

[10] *Id*., at 2-3.

[11] *Id*., at 6-7.

[12] *See*, FRANK DONNER, PROTECTORS OF PRIVILEGE: RED SQUADS AND POLICE REPRESSION IN URBAN AMERICA (1990).

[13] *See*, Arthur N. Eisenberg, New York Civil Liberties Union, Testimony Before The New York Advisory Committee To The U.S. Commission On Civil Rights: Police Surveillance of Political Activity -- The History and Current State of the *Handschu* Decree (May 21, 2003), *available at* http://www.nyclu.org/node/731.

[14] FBI Statutory Charter: Hearings Before the Senate Committee on the Judiciary, 95th Cong. Pt. 1, at 22, (Apr. 20 and 25, 1978).

[15] FBI Domestic Security Guidelines: Oversight Hearings Before the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary, 98th Cong. 67-85 (1983).

[16] 42 U.S.C.A. §3789(g)(c) (WEST 2007). The provision instructing the Office of Justice Programs to prescribe regulations to assure that criminal intelligence systems are "not utilized in violation of the privacy and constitutional rights of individuals" was added when the Omnibus Crime Control and Safe Streets Act of 1968 was reauthorized and amended by the Justice System Improvement Act of 1979 (*See*, Justice System Improvement Act of 1979, Pub.L. No. 96-157, 1979 U.S.C.C.A.N. (96 Stat.) 1167, 1213, 2471-77, 2539).
[17] *See* Office of Justice Programs, U.S. Department of Justice, *Final Revision to the Office of Justice Programs, Criminal Intelligence Systems Operation Policies, 1993 Revision and Commentary,* 28 C.F.R. Part 23 (1993), at 4, http://www.homeland.ca.gov/pdf/civil_liberties/1993RevisionCommentary_28CFRPart23.pdf.
[18] 392 U.S. 1 (1968).
[19] Institute for Intergovernmental Research, Frequently Asked Questions, http://www.iir.com/28cfr/FAQ.htm.
[20] Letter from Russell M. Porter, General Chairman, Association of Law Enforcement Intelligence Units to Michael Dever, Department of Justice Office of Justice Programs, Comments on proposed amendments to 28 Code of Federal Regulations Part 23, OJP Docket No. 1473, (Sept. 1, 2008), (on file with author).
[21] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (PATRIOT Act) of 2001, Section 505, Pub. L. No. 107-56, 115 Stat. 272 (2001). The four NSL authorizing statutes include the Electronic Communications Privacy Act, 18 U.S.C. § 2709 (2000), the Right to Financial Privacy Act, 12 U.S.C. § 3401 (2000), the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. (2000), and the National Security Act of 1947, 50 U.S.C. § 436(a)(1)(2000).
[22] DEP'T OF JUSTICE, OFFICE OF INSPECTOR GENERAL, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS (Mar. 2007), *available at* http://www.usdoj.gov/oig/special/s0703b/final.pdf [hereinafter 2007 NSL Report].
[23] 2007 NSL Report, *supra* note 22, at 84.
[24] 2007 NSL Report, *supra* note 22, at 86-99.
[25] DEP'T OF JUSTICE, OFFICE OF INSPECTOR GENERAL, A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006 (Mar. 2008), *available at* http://www.usdoj.gov/oig/special/s0803b/final.pdf [hereinafter 2008 NSL Report].
[26] 2008 NSL Report, *supra* note 25, at 9.
[27] 2008 NSL Report, *supra* note 25, at 127, 129 n.116.
[28] 2008 NSL Report, *supra* note 25, at 127.
[29] 2008 NSL Report, *supra* note 25, at 127.
[30] James Risen and Eric Lichtblau, *Bush lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1, *available at* http://www.nytimes.com/2005/12/16/politics/16program.html?ei=5090&en=e32072d786623ac1&ex=1292389200.
[31] Leslie Cauley, *NSA has Massive Database of Americans' Phone Calls*, USATODAY, May 11, 2006, at 1A, *available at* http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm.
[32] Eric Lichtblau & James Risen, *Officials Say U.S. Wiretaps Exceeded Law,* N.Y. Times, Apr. 15, 2009, at A1, *available at http://www.nytimes.com/2009/04/16/us/16nsa.html.*
[33] Lowell Bergman, Eric Lichtblau, Scott Shane and Don Van Natta, Jr., Spy *Agency Data After Sept. 11 Led FBI to Dead Ends*, N.Y. TIMES, Jan. 17, 2006, at A1, *available at* http://www.nytimes.com/2006/01/17/politics/17spy.html?ei=5090&en=f3247cd88fa84898&ex=1295154000&pagewanted=print.
[34] *See*, TRANSACTIONAL RECORDS ACCESS CLEARINGHOUSE, NATIONAL PROFILE AND ENFORCEMENT: TRENDS OVER TIME (2006), http://trac.syr.edu/tracfbi/newfindings/current/ (last visited Apr. 15, 2009); Todd Lochner, *Sound and Fury: Perpetual Prosecution and Department of Justice Antiterrorism Efforts*, 30 LAW & POLICY 168, 179 (2008), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1109250.
[35] *See*, TRANSACTIONAL RECORDS ACCESS CLEARINGHOUSE, NATIONAL PROFILE AND ENFORCEMENT: TRENDS OVER TIME (2006), http://trac.syr.edu/tracfbi/newfindings/current/ (last visited Apr. 15, 2009); Todd Lochner, *Sound and Fury: Perpetual Prosecution and Department of Justice Antiterrorism Efforts*, 30 LAW & POLICY 168, 179 (2008), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1109250.
[36] JEFFREY W. SEIFERT, CONGRESSIONAL RESEARCH SERVICE, CRS REPORT FOR CONGRESS: DATA MINING AND HOMELAND SECURITY: AN OVERVIEW (Jan. 18, 2007), *available at* http://www.fas.org/sgp/crs/intel/RL31798.pdf.
[37] NATIONAL RESEARCH COUNCIL, PROTECTING INDIVIDUAL PRIVACY IN THE STRUGGLE AGAINST TERRORISTS: A FRAMEWORK FOR PROGRAM ASSESSMENTS, COMMITTEE ON TECHNICAL AND PRIVACY DIMENSIONS OF INFORMATION FOR TERRORISM PREVENTION AND OTHER NATIONAL GOALS (Oct. 2007), *available at* http://www.nap.edu/catalog.php?record_id=12452.

[38] For a detailed analysis of the changes to the AGG over time, *See*, DEP'T OF JUSTICE, OFFICE OF INSPECTOR GENERAL, THE FEDERAL BUREAU OF INVESTIGATION'S COMPLIANCE WITH ATTORNEY GENERAL'S INVESTIGATIVE GUIDELINES (2005), *available at* http://www.usdoj.gov/oig/special/0509/final.pdf.
[39] The Attorney General's Guidelines on General Crimes, Racketeering Enterprise, and Terrorism Enterprise Investigations, (May 30, 2002), available at: http://www.ignet.gov/pande/standards/prgexhibitg.pdf
[40] DEMOCRATIC STAFF OF THE H.R. COMM. ON HOMELAND SECURITY, 110TH CONG., LEAP: A LAW ENFORCEMENT ASSISTANCE AND PARTNERSHIP STRATEGY, PREPARED AT THE REQUEST OF CONGRESSMAN BENNIE G. THOMPSON, RANKING MEMBER 5 (2006), http://hsc-democrats.house.gov/SiteDocuments/20060927193035-23713.pdf.
[41] *Id.* at 5 (quoting Michael Downing, Commander, Los Angeles Police Department Counterterrorism/Criminal Intelligence Bureau).
[42] *Homeland Security Intelligence: Its Relevance and Limitations: Hearing Before the Subcomm. on Intelligence, Information Sharing and Terrorism Risk Assessment of the H. Comm. on Homeland Security*, 111th Cong. 8 (March 18, 2009) (Testimony of John Gaissert, Chief of Police, Commerce Police Department, Commerce, Georgia).
[43] Secretary of Homeland Security Michael Chertoff, Remarks at the 2006, Bureau of Justice Assistance, U.S. Department of Justice and SEARCH Symposium on Justice and Public Safety Information Sharing, Mar. 14, 2006, http://www.dhs.gov/xnews/speeches/speech_0273.shtm.
[44] *Id.*, at 6 (quoting Chief Ellen Hanson of the City of Lexana, Kansas Police Department).
[45] TODD MASSE, SIOBHAN O'NEIL AND JOHN ROLLINS, CONGRESSIONAL RESEARCH SERVICE, CRS REPORT FOR CONGRESS: FUSION CENTERS: ISSUES AND OPTIONS FOR CONGRESS at 22 n.60, (July 6, 2007) [hereinafter CRS Fusion Center Report].
[46] CRS Fusion Center Report, *supra*, note 45, at 21.
[47] CRS Fusion Center Report, supra note 45, at 18-19.
[48] BUREAU OF JUSTICE ASSISTANCE, OFFICE OF JUSTICE PROGRAMS, U.S. DEP'T. OF JUSTICE, FUSION CENTER GUIDELINES: DEVELOPING AND SHARING INFORMATION AND INTELLIGENCE IN A NEW ERA, at iii, (Aug. 2006) [hereinafter Guidelines].
[49] Guidelines, *supra* note 48, at 2.
[50] CRS Fusion Center Report, *supra* note 45, at 1.
[51] Guidelines, *supra* note 48, at 13.
[52] Guidelines, *supra* note 48, at 13.
[53] CRS Fusion Center Report, *supra* note 45, at 1.
[54] Mike Chalmers and Lee Williams, *Intelligence Facility Casts a Wide Net*, THE NEWS JOURNAL, May 7, 2007, http://www.delawareonline.com/apps/pbcs.dll/article?AID=/20070507/NEWS/705070333.
[55] Shaun Waterman, *Analysis: Md. Spy Charges Prompt Review, United Press International*, MIDDLE EAST TIMES (July 24, 2008), http://www.metimes.com/Security/2008/07/24/analysis_md_spy_charges_prompt_review/4743/.
[56] Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.0, ISE-FS-200, (Jan. 25, 2008) (on file with authors).
[57] *See*, MIKE GERMAN AND JAY STANLEY, AMERICAN CIVIL LIBERTIES UNION, FUSION CENTER REPORT UPDATE (July 2008), http://www.aclu.org/pdfs/privacy/fusion_update_20080729.pdf.
[58] IRTPA, Pub. L. No. 108-458, 118 Stat. 3638 (2004).
[59] The Denver Police Spy Files, ACLU of Colorado, http://www.aclu-co.org/spyfiles/fbifiles.htm (last visited Apr. 15, 2009).
[60] MARK SCHLOSBERG, STATE OF SURVEILLANCE: GOVERNMENT MONITORING OF POLITICAL ACTIVITY IN NORTHERN AND CENTRAL CALIFORNIA, ACLU OF NORTHERN CALIFORNIA (July 2006), *available at* http://www.aclunc.org/issues/government_surveillance/asset_upload_file714_3255.pdf.
[61] Faces of Surveillance: Targets of Illegal Spying, ACLU Website, http://www.aclu.org/safefree/general/24287res20060227.html (last visited Apr. 15, 2009).
[62] Lisa Rein, *Federal Agency Aided Md. Spying*, WASH. POST, Feb. 17, 2009, at B01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2009/02/16/AR2009021601131.html.
[63] Letter from Jim Howe, Acting Assistant Secretary, U.S. Department of Homeland Security, to Senator Benjamin L. Cardin, (Jan 29, 2009) (on file with author).
[64] Maryland State Police Intelligence File on the D.C. Anti-War Network (DAWN), 13, (2005) (on file with the ACLU). This document was released pursuant to the Maryland's Public Information Act. *See* Public Information Act, Md. Code Ann., State Gov't § 10-630 (West 2008).

[65] Lisa Rein, *Federal Agency Aided Md. Spying*, WASH. POST, Feb. 17, 2009, at B01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2009/02/16/AR20090216011131.html.
[66] *See,* U.S. Dep't of Homeland Security, Assessment: Rightwing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment (Apr. 7, 2009), *available at* http://wnd.com/images/dhs-rightwing-extremism.pdf.
[67] UNIVERSAL ADVERSARY DYNAMIC THREAT ASSESSMENT, ECO-TERRORISM: ENVIRONMENTAL AND ANIMAL RIGHTS MILITANTS IN THE UNITED STATES, (May 7, 2008), *available at* http://wikileaks.org/leak/dhs-ecoterrorism-in-us-2008.pdf.
[68] MICHAEL GERMAN AND JAY STANLEY, WHAT'S WRONG WITH FUSION CENTERS? AMERICAN CIVIL LIBERTIES UNION (Dec. 2007), http://www.aclu.org/pdfs/privacy/fusioncenter_20071212.pdf; MIKE GERMAN AND JAY STANLEY, AMERICAN CIVIL LIBERTIES UNION, FUSION CENTER REPORT UPDATE (July 2008), http://www.aclu.org/pdfs/privacy/fusion_update_20080729.pdf.
[69] North Central Texas Fusion System Prevention Awareness Bulletin, (Feb. 19, 2009), *available at* http://www.baumbach.org/fusion/PAB_19Feb09.doc. For a discussion of DHS support of the North Central Texas Fusion Center, *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF INSPECTOR GENERAL, DHS'S ROLE IN STATE AND LOCAL FUSION CENTERS IS EVOLVING (Dec. 2008), *available at* http://www.fas.org/irp/agency/dhs/ig-fusion.pdf ; GENERAL ACCOUNTABILITY OFFICE, HOMELAND SECURITY: FEDERAL EFFORTS ARE HELPING TO ALLEVIATE SOME CHALLENGES ENCOUNTERED BY STATE AND LOCAL INFORMATION FUSION CENTERS (Oct. 2007), *available at* http://www.gao.gov/new.items/d0835.pdf.
[70] T.J. Greaney, *'Fusion Center' Data Draws Fire over Assertions*, COLOMBIA DAILY TRIBUNE, (March 14, 2009), *available at* http://www.columbiatribune.com/news/2009/mar/14/fusion-center-data-draws-fire-over-assertions/.
[71] Alexandra Marks, *FBI and American Muslims at Odds*, CHRISTIAN SCIENCE MONITOR, March 25, 2009, *available at* http://www.csmonitor.com/2009/0325/p02s01-ussc.html.
[72] SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, U.S. SENATE, 94TH CONG., FINAL REPORT ON SUPPLEMENTAL DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS (BOOK III), S. Rep. No. 94-755 (1976).
[73] *See*, MIKE GERMAN AND MICHELLE RICHARDSON, RECLAIMING PATRIOTISM: A CALL TO RECONSIDER THE PATRIOT ACT, AMERICAN CIVIL LIBERTIES UNION (MARCH 2009), *available at* http://www.aclu.org/pdfs/safefree/patriot_report_20090310.pdf.
[74] TODD MASSE, SIOBHAN O'NEIL & JOHN ROLLINS, CONGRESSIONAL RESEARCH SERVICE, CRS REPORT FOR CONGRESS: FUSION CENTERS: ISSUES AND OPTIONS FOR CONGRESS 22 (July 6, 2007), *available at* http://www.fas.org/sgp/crs/intel/RL34070.pdf.
[75] *Current and Projected National Security Threats to the United States: Hearing before the S. Select Comm. on Intelligence,* 111th Cong. (Feb. 12, 2009) (statement of Admiral Dennis C. Blair, Director of National Intelligence), http://www.dni.gov/testimonies/20090212_testimony.pdf.
[76] United States v. United States Dist. Court *(Keith),* 407 U.S. 297, 314 (1972).