Statement of Caroline Fredrickson, Director

American Civil Liberties Union Washington Legislative Office

On

"Homeland Security Intelligence: Its Relevance and Limitations"

Before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment

House Committee on Homeland Security

March 18, 2009

Good morning Chairwoman Harman, Ranking Member McCaul, 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 the intelligence activities of the Department of Homeland Security (DHS). As you know, the ACLU testified before the full Homeland Security Committee in 2007 to express our concerns about the Department's domestic use of spy satellites through its National Applications Office (NAO).[1] We know this Committee shares our unease with this program and we would like to thank Chairman Thompson and Chairwoman Harman for their leadership in challenging the NAO's funding unless and until a proper legal framework can be established to protect the privacy of ordinary Americans.[2] Recent news that DHS is using Predator drones for surveillance on our northern border raises similar concerns,[3] as do warrantless laptop and cell phone searches and other data seizures at the U.S. border. We look forward to working with you to address these matters.

But rather than focus on particular programs I would like to ask more fundamental questions about the role of intelligence in homeland security, and particularly within DHS. As explained below, problems inherent in the way the intelligence community produces 'intelligence' limit its reliability, rendering its value in improving security suspect. In addition, 'homeland security' is a relatively new and exceptionally broad concept that combines protecting against traditional threats from hostile nations, terrorists and other criminal groups with preparing to respond to outbreaks of infectious disease, natural disasters and industrial accidents. While these are all important missions, taking such an unfocused "all crimes, all hazards"[4] approach to intelligence collection poses significant risks to our individual liberties, our democratic principles and, ironically, even our security. 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.[5] Unfortunately, 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. Recent events indicate that in its zeal to fulfill its broad mandate and establish an intelligence capability, DHS is repeating these mistakes. If DHS is to have a meaningful intelligence role that actually enhances security, it must assess the information it produces accurately, identify an intelligence need to be served, and evaluate whether it can fill this need without violating the privacy and civil rights of innocent Americans. Congress should evaluate these programs regularly and withhold funding from any activities that are unnecessary, ineffective or prone to abuse.

I. THE RELEVANCE OF INTELLIGENCE IN HOMELAND SECURITY

The immediate obstacle to determining the relevance of intelligence in homeland security is the lack of a commonly understood definition of 'intelligence.'[6] People often hear the word and assume that this type of information has some magical quality giving it heightened importance and meaning. But by its very nature, intelligence is often uncorroborated, inadequately vetted and fragmentary at best, and unreliable, misleading or just plain wrong at worst. This deficiency is due to the secretive manner in which intelligence agencies gather, analyze, use and report information. By allowing people to report information against their

neighbors or colleagues in secret, the social mores and legal consequences that normally restrain people from making false or misleading accusations are removed. By masking the sources and methods used to obtain this information, 'intelligence' is stripped of the most essential clues for determining its value. Knowing whether an accusation that a politician is misusing campaign funds is coming from a trusted insider, a political opponent or an unemployed cab driver makes all the difference in determining its credibility. By then compartmentalizing this information and limiting its distribution, outside experts are prevented from effectively evaluating or challenging the finished 'intelligence.' And finally, by keeping contradictory pieces of intelligence and dissenting opinions secret, policy makers can too easily ignore information or advice that might weigh against the policies or activities they choose to pursue. None of these processes necessarily make the final product false; they simply reduce the probability that it is reliable. If we called this material 'unsubstantiated allegations,' 'rumor,' 'speculation,' or 'educated guesses' we would understand its value, but when we call it 'intelligence' it takes on a significance it does not necessarily deserve.

Mark Randol of the Congressional Research Service argues that "raw" information does not become intelligence "until its sources have been evaluated, the information is combined or corroborated by other sources, and analytical and due diligence methodologies are applied to ascertain the information's value."[7] But this asks too much of a closed analytical process. Investigations into the intelligence failures regarding the presence of weapons of mass destruction in Iraq prior to the U.S. invasion, for example, find no shortage of attempts to validate the separate pieces of information.[8] This information was subjected to all the processes Randol describes, but in the end the 'finished' intelligence was wrong. As the Senate Intelligence Committee Phase II report concluded, "[i]t is entirely possible for an analyst to perform meticulous and skillful analysis and be completely wrong."[9] In the end, the intelligence community chose to rely on an untrustworthy source named "Curveball" despite ample warnings that he was a fabricator,[10] and policy-makers failed to heed dissenting opinions about whether aluminum tubes Iraq purchased were designed for use in a nuclear centrifuge.[11] These failures in pre-war intelligence were not because of a lack of process, rather because of what the process lacked.

Our legal system provides a contrasting method for determining the reliability of information. Centuries of jurisprudence have distilled rules of evidence and procedure that are specifically designed to provide the analytical due diligence Randol says is necessary for converting information into intelligence, though in the legal system this information is called 'evidence.' Evidence is "something (as testimony, writings, or objects) presented at a judicial or administrative proceeding *for the purpose of establishing the truth or falsity of an alleged matter of fact*" (emphasis added).[12] The rules of evidence are not arbitrary obstacles for lawyers to navigate; they represent time-tested methods for discerning truth. In order to be admitted into evidence documents must be authenticated by the individual or organization that produced them. Witnesses are examined in public and under oath. Information known to be obtained through unreliable means, such as coerced confessions, is not admissible. And once entered, evidence is challenged in an adversarial process, before a neutral arbiter and a jury of ordinary citizens serving as the ultimate fact-finders. Finally, this process is conducted in public, so that the justice system and those who work within it are accountable to the people they serve. A closed

intelligence process simply cannot match this rigorous testing, and the reliability of the information it produces suffers as a result.

The one thing that is certain about 'intelligence,' is that it is only valuable to our security when it is true. Faulty intelligence is worse than no intelligence at all because it compels policy makers to take actions that may not have been necessary or to fail to take actions that were. And errors in intelligence are often compounded because security resources are finite. Increasing the assets directed at one threat invariably means reducing efforts devoted to another. For example, the New York Times reported that FBI officials began noticing a surge of mortgage frauds in 2003 and 2004 but their requests for additional resources to address financial crimes were denied by a Justice Department focused on counterterrorism.[13] Yet Director of National Intelligence Dennis Blair now identifies the global economic crisis as the "primary near-term security concern of the United States."[14] Intelligence programs that focus on the last crisis to the detriment of anticipating the next crisis do not provide real security.

All of the problems of unreliability of intelligence are compounded with a new system of collection, and the negative impacts are many times greater when the ears and eyes are not pointed outward but inward to the U.S. When intelligence subjects are not foreign nations or their military and intelligence operatives, but citizens, lawful permanent residents and visa holders of our country, the checks and balances must be significantly enhanced over the minimal supervision given other parts of the intelligence apparatus. Therefore, Congress must be especially mindful of the limits of intelligence as it evaluates DHS intelligence programs. Congress should demand empirical evidence that these programs actually enhance security before funding them, particularly where they impact the rights and privacy of innocent Americans. So many of the broad information collection programs the intelligence community instituted over the last eight years were premised on the idea that data mining tools could later be developed to find meaning in these vast pools of data collected,[15] but a recent study funded by DHS found that such programs were likely a wasted effort:

> 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.[16]

Congress cannot afford to allow DHS, or any other intelligence agency, to continue investing in unproven technologies that harm privacy but provide no real security benefit.

II. THE LIMITATIONS OF HOMELAND SECURITY INTELLIGENCE

Intelligence has traditionally been divided into two spheres, foreign and domestic, which operate under different legal regimes. 'Foreign intelligence,' which is directed at foreign powers and their agents and is conducted primarily outside the United States, has less restrictive regulations and oversight, while 'domestic intelligence,' directed primarily at U.S. persons and

conducted inside the U.S. is generally more regulated. Randol suggests that the advantage of 'homeland security intelligence' as a discipline distinct from foreign or domestic intelligence is that it allows a holistic approach that is free from constraints of geography, level of government, or mutual mistrust between the public and private sectors.[17]

The danger with this approach is that the constraints are often specifically designed, or at least operate in practice, to protect the privacy and civil rights of U.S. persons. Blending the two disciplines necessarily leads to a dilution of privacy protections for U.S. persons as less restrictive methods of gathering foreign intelligence are increasingly used against U.S. persons. For instance, more than half of the roughly 50,000 National Security Letters the FBI issues each year, which were originally designed for use only against agents of foreign powers, now target U.S. persons.[18] Moreover, the compelling mission to protect the homeland would likely drive routine overrides of minimization procedures restricting the dissemination of U.S. person information collected under a foreign intelligence rubric,[19] particularly as intelligence agents take the 'better safe than sorry' approach that led to excessive number of nominations to the terrorist watch lists.[20]

More significantly, while DHS will undoubtedly require access to foreign intelligence collected by the other intelligence agencies to fulfill its mission, its focus on protecting the 'homeland' will drive a primarily domestic intelligence program. The DHS intelligence mission statement, "to provide homeland security intelligence and information to the Secretary, other federal officials, and our state, local, tribal and private sector partners," suggests a domestic focus.[21] And the DHS intelligence components, the U.S. Citizenship and Immigration Services, U.S. Coast Guard, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement and the Transportation Security Administration, will disproportionately gather U.S. person information in the course of fulfilling their mission responsibilities.

By their nature, all domestic intelligence operations pose a threat to civil liberties and democratic processes. Whenever the government is involved in gathering information about Americans without a reasonable suspicion of criminal activity, there is substantial risk of chilling lawful dissent and association. As the Supreme Court observed in *United States v. United States District Court* (*Keith*), "[h]istory abundantly documents the tendency of Government – however benevolent and benign its motives – to view with suspicion those who most fervently dispute its policies."[22]

• EVIDENCE OF ABUSE

Several recent incidents seem to indicate DHS is ignoring this history in its zeal to establish an intelligence role, and improperly monitoring peaceful advocacy groups and religious and racial minorities. Charles Allen, DHS Undersecretary for Intelligence and Analysis, said one of the analytic elements his office assesses is the threat of radicalization and extremism. The ACLU is concerned that these terms are ill-defined and seem to suggest a connection between terrorism and advocacy against government policies. Undersecretary Allen stated categorically in recent testimony that DHS does not monitor known extremists and their activities, but documents obtained by the ACLU suggest otherwise.[23]

The ACLU of Maryland recently uncovered a Maryland State Police (MSP) intelligence operation that targeted 23 non-violent political advocacy organizations based solely on the exercise of their First Amendment rights.[24] MSP spying activities were aimed at 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. Many of the members of these organizations were referenced as terrorists in a federal database.

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,[25] particularly because DHS representatives had previously denied that DHS had any information regarding the MSP investigations targeting these protesters.[26] 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."[27]

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."[28] 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.

This bulletin is not the only indication of abuse in DHS intelligence operations. Another 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."[29] 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 limited DHS resources to generate such intelligence products – and yet these events continue to occur.

Last month 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.[30] The bulletin, which reportedly is sent to over 100 different agencies, would be laughable except that it comes with the imprimatur of a federally-backed intelligence operation, and it directs law enforcement officers to monitor the activities of these groups in their areas. The ACLU has long warned that these state, local and regional intelligence fusion centers lacked proper oversight and accountability and we hope the discovery of this shockingly inappropriate report leads to much needed examination and reform. In December 2008 the DHS Privacy Office issued a Privacy Impact Assessment of fusion centers that echoed the ACLU's concerns regarding the threat these rapidly expanding intelligence centers pose to the privacy of innocent Americans.[31]

• DILUTION OF EFFECTIVE REGULATION

It isn't surprising that an intelligence operation with an overbroad 'all hazards' mission and lax oversight would trample on individual privacy rights. The police power to investigate combined with the secrecy necessary to protect legitimate law enforcement operations provide ample opportunity for error and abuse, which is why in the 1970s the federal government sought to establish clear guidelines for state and local law enforcement agencies engaged in the collection of criminal intelligence information. Title 28, Part 23 of the Code of Federal Regulations was promulgated pursuant to 42 U.S.C. §3789(g)(c) which requires 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 the funding and operation of these systems further the purpose of this chapter and to assure that some systems are not utilized in violation of the privacy and constitutional rights of individuals."[32]

The regulation was part of a series of law enforcement reforms initiated to curb widespread abuses of police investigative authorities for political purposes, particularly by local police intelligence units or "red squads," which often amassed detailed dossiers on political officials and engaged in "disruptive" activities targeting political activists, labor unions, and civil rights advocates, among others. 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."[33]

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 "reasonable suspicion" standard is clear, well-defined, time-tested and universally accepted by law enforcement agencies around the country as the appropriate standard for regulating the intelligence collection activities of law enforcement officers.

Unfortunately, there is a new theory of domestic intelligence that 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.[34]

It is clear from this statement that Secretary Chertoff was relying on the extravagant promises of the now-debunked data mining technologies to make sense of the thousand routine observations that would be recorded each day. But suspicious activity reporting programs are moving forward nonetheless.

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.[35] 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.[36] 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 the Part 23 reasonable suspicion standard. 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 intelligence programs. This Subcommittee should examine these programs closely, assess whether they demonstrably improve security and ensure that they operate in a manner that protects individual rights before authorizing DHS resources to support them.

III. THE ROLE OF THE DEPARTMENT OF HOMELAND SECURITY IN INTELLIGENCE

The Homeland Security Act of 2002 tasked DHS with the responsibility to manage programs for sharing law enforcement and intelligence information between the federal government and state, local and tribal authorities.[37] Unfortunately, other federal law enforcement and intelligence agencies, such as the FBI, already had well-established relationships and information-sharing arrangements with state and local law enforcement and resisted DHS efforts to manage these programs. In 2004, Congress established the ODNI Information Sharing Environment to address this ongoing resistance to information sharing, but this only further complicated the question of DHS's intelligence role.[38]

As it stands now there are several mechanisms 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 e-Guardian systems and the Homeland Secure Information Network (HSIN) to name just a few. With several different federal agencies responsible for intelligence collection and analysis and several different mechanisms for sharing intelligence with state and local authorities, DHS intelligence operations risk being redundant or even superfluous.

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 to the privacy and liberties of ordinary Americans. Intelligence offices are too often judged by the number of reports they disseminate rather than the value of the information in those reports, which is part of what drives the over-collection and over-reporting of innocuous information. In 2008, Undersecretary Allen boasted that I&A increased production of Homeland Intelligence Reports "from 2,000 to nearly 3,100" over the previous year but this statistic only represents an improvement if the information reported is correct, relevant and unique.[39] Intelligence reports like those produced by the North Central Texas Fusion Center provide nothing to enhance homeland security, and may actually undermine it by diverting attention from real threats.

DHS intelligence programs should not compete with other federal programs. DHS should assess what state, local and other federal agencies need from DHS intelligence programs that they are not currently receiving from other sources. It is possible that there is no gap in intelligence, which would render DHS intelligence wholly unnecessary. If there is a gap, then

DHS should evaluate the information produced by each of its intelligence components during the normal course of business to determine whether it can tailor this information to suit the specific intelligence needs identified. If DHS intelligence activities produce no demonstrably useful information, Congress should de-fund them. Where new types or sources of information need to be developed to fill intelligence gaps, DHS should carefully evaluate whether collection of this information is appropriate under the law, whether DHS is the agency best suited to collect this information, and whether the dissemination of such information can be accomplished without violating the privacy or civil rights of U.S. persons. Where DHS finds it can produce a necessary intelligence product, such programs should be narrowly tailored to fulfill that specific need and constantly reviewed to ensure conformance with all laws and policies. Finally, Congress should evaluate these programs regularly, and in public to the greatest extent possible. In the famous words of Supreme Court Justice Louis Brandeis, sunshine is the best disinfectant.

IV. CONCLUSION

Intelligence operations directed at Americans pose serious risks to liberty and democracy. First and foremost, we should not sacrifice our liberty for the illusion of security. Congress should not implement or fund new intelligence programs without empirical evidence that they effectively improve security. 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.[40] It turns out, not surprisingly, that spying on innocent people is not useful to uncovering true threats to security. Reforms instituted after the exposure of these abusive intelligence programs were designed not only to protect the rights of innocent Americans, but to help our law enforcement and intelligence agencies become more effective by focusing their resources on people they reasonably suspected of wrongdoing. Unfortunately these lessons of the past have too often been ignored, and we are increasingly seeing a return to abusive intelligence operations targeting protest groups and religious and racial minorities.

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 DHS's involvement in monitoring peaceful advocacy organizations. As the *Keith* Court warned, "The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power."[41]

---

[1] *Turning Spy Satellites on the Homeland: the Privacy and Civil Liberties Implications of the National Applications Office: Hearing before the H. Comm. on Homeland Security*, 110th Cong. (Sept. 6, 2007) (statement of Barry Steinhardt, Director, Technology and Liberty Program, American Civil Liberties Union), *available at* http://www.aclu.org/images/asset_upload_file278_31829.pdf.

[2] *See* Letter from Rep. Bennie G. Thompson, Chairman, Committee on Homeland Security, U.S. House of Representatives, Rep. Jane Harman, Chair, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Committee on Homeland Security, U.S. House of Representatives, and Rep. Christopher P. Carney, Chairman, Subcommittee on Management, Investigations, and Oversight, Committee on Homeland Security, U.S. House of Representatives, to Michael Chertoff, Department of Homeland Security and Charles Allen, Office of

Intelligence and Analysis, Department of Homeland Security (Apr. 7, 2008) (on file with authors), *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB229/44c.pdf.

[3] *Drone to Patrol Border Between Manitoba and North Dakota,* THE CANADIAN PRESS, Feb. 16, 2009, http://cnews.canoe.ca/CNEWS/World/2009/02/16/8412951-cp.html.

[4] 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.

[5] *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.

[6] *See*, MARK A. RANDOL, CONGRESSIONAL RESEARCH SERVICE, CRS REPORT FOR CONGRESS: HOMELAND SECURITY INTELLIGENCE: PERCEPTIONS, STATUTORY DEFINITIONS AND APPROACHES 2 (Jan. 14, 2009), *available at* http://fas.org/sgp/crs/intel/RL33616.pdf ("At the broadest level, there is a plethora of definitions for intelligence.").

[7] MARK A. RANDOL, CONGRESSIONAL RESEARCH SERVICE, CRS REPORT FOR CONGRESS: HOMELAND SECURITY INTELLIGENCE: PERCEPTIONS, STATUTORY DEFINITIONS AND APPROACHES 2 (Jan. 14, 2009), *available at* http://fas.org/sgp/crs/intel/RL33616.pdf.

[8] *See*, S. REP. NO. 108-301(2004), *available at* http://www.gpoaccess.gov/serialset/creports/iraq.html; S. REP. NO. 109-331 (2006), *available at* http://intelligence.senate.gov/phaseiiaccuracy.pdf (Phase II Report).

[9] S. REP. NO. 109-331, at 6 (2006), *available at* http://intelligence.senate.gov/phaseiiaccuracy.pdf (Phase II Report).

[10] Bob Drogan and Greg Miller, *Curveball Debacle Reignites CIA Feud*, L.A. TIMES, Apr. 2, 2005, *available at* http://articles.latimes.com/2005/apr/02/nation/na-intel2.

[11] David Barstow, William J. Broad, and Jeff Gerth, *How the White House Embraced Disputed Arms Intelligence,* N.Y. TIMES, Oct. 3, 2004, *available at:* http://www.nytimes.com/2004/10/03/international/middleeast/03tube.html

[12] Miriam-Webster's Dictionary of Law 171-72 (1996).

[13] Eric Lichtblau, David Johnston, and Ron Nixon, *FBI Struggles to Handle Financial Fraud Cases*, N.Y. TIMES, Oct. 18, 2008, *available at* http://www.nytimes.com/2008/10/19/washington/19fbi.html?pagewanted=1&_r=1&dbk.

[14] *Current and Projected National Security Threats to the United States: Hearing before the S. Select Comm. on Intelligence,* 111th Cong. 2 (Feb. 12, 2009) (statement of Admiral Dennis C. Blair, Director of National Intelligence), http://www.dni.gov/testimonies/20090212_testimony.pdf.

[15] 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.

[16] 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.

[17] MARK A. RANDOL, CONGRESSIONAL RESEARCH SERVICE, CRS REPORT FOR CONGRESS: HOMELAND SECURITY INTELLIGENCE: PERCEPTIONS, STATUTORY DEFINITIONS AND APPROACHES 13 (Jan. 14, 2009), *available at* http://fas.org/sgp/crs/intel/RL33616.pdf.

[18] U.S. DEPARTMENT 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.

[19] *See,* NATIONAL SECURITY AGENCY, REPORT TO CONGRESS: LEGAL STANDARDS FOR THE INTELLIGENCE COMMUNITY IN CONDUCTING ELECTRONIC SURVEILLANCE (Feb. 2000), *available at* http://www.fas.org/irp/nsa/standards.html ("The overarching standard as implemented in both E.O. 12333 and FISA minimization procedures is that to disseminate personally identifiable information concerning a U.S. person, the information must be found necessary to understand a particular piece of foreign intelligence or assess its importance").

[20] DEPARTMENT OF JUSTICE, OFFICE OF INSPECTOR GENERAL REVIEW OF THE TERRORIST SCREENING CENTER viii (June 2005), *available at* http://www.fas.org/irp/agency/doj/oig/tsc.pdf.

[21] Department of Homeland Security, Office of Intelligence and Analysis webpage, http://www.dhs.gov/xabout/structure/gc_1220886590914.shtm (last visited Mar. 11, 2009).

[22] United States v. United States Dist. Court *(Keith),* 407 U.S. 297, 313-314 (1972).

[23] *Homeland Security Intelligence at a Crossroads: The Office of Intelligence and Analysis' Vision for 2008: Hearing before the Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment of the H. Comm. on Homeland Security,* 110th Cong. 4 (Feb. 26, 2008) (Statement of Charles E. Allen, Undersecretary for

Intelligence and Analysis, Department of Homeland Security), *available at* http://homeland.house.gov/SiteDocuments/20080226165154-47048.pdf.

[24] *See,* ACLU of Maryland "Stop Spying" info page, http://www.aclu-md.org/Index%20content/NoSpying/NoSpying.html (last visited Mar. 11, 2009).

[25] Lisa Rein, Federal Agency Aided Md. Spying, Washington Post, Feb. 17, 2009, at: http://www.washingtonpost.com/wp-dyn/content/article/2009/02/16/AR2009021601131.html

[26] 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).

[27] Maryland State Police Intelligence File on the D.C. Anti-War Network (DAWN), p. 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).

[28] 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.

[29] 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.

[30] 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.

[31] U.S. DEPARTMENT OF HOMELAND SECURITY PRIVACY IMPACT ASSESSMENT FOR THE DEPARTMENT OF HOMELAND SECURITY STATE, LOCAL AND REGIONAL FUSION CENTER INITIATIVE (Dec. 11, 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ia_slrfci.pdf.

[32] 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).

[33] *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.

[34] 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.

[35] Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.0, ISE-FS-200, (Jan. 25, 2008) (on file with authors).

[36] *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.

[37] 6 U.S.C.A. §101 et seq (West 2006).

[38] *See*, Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C.A. §401, et seq (West 2006).

[39] *Homeland Security Intelligence at a Crossroads: The Office of Intelligence and Analysis' Vision for 2008: Hearing before the Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment of the H. Comm. on Homeland Security,* 110th Cong. 4 (Feb. 26, 2008) (Statement of Charles E. Allen, Undersecretary for Intelligence and Analysis, Department of Homeland Security), *available at* http://homeland.house.gov/SiteDocuments/20080226165154-47048.pdf.

[40] 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).

[41] United States v. United States Dist. Court *(Keith),* 407 U.S. 297, 314 (1972).