MARK J. REICHEL, Bar #155034
Attorney At Law
655 University Ave., Suite 215
Sacramento, California 95825
Telephone: (916) 974-7033
mreichel@donaldhellerlaw.com

Attorney for Defendant
ERIC MCDAVID

IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. ERIC MCDAVID, et al. Defendants.	NO. CR-S-06-0035-MCE **NOTICE OF MOTION AND MOTION FOR DISCOVERY ORDER REQUIRING PRODUCTION OF ALL SURVEILLANCE DATA AND MATERIAL OF THIS DEFENDANT OBTAINED THROUGH ALL GOVERNMENT DOMESTIC SPYING, HARVESTING AND MINING PROGRAMS; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT THEREOF**

DATE: February 2, 2007
TIME: 2:00 p.m.
JUDGE: HON. KIMBERLY J. MUELLER

TO: MCGREGOR SCOTT, United States Attorney, and R. STEVEN LAPHAM, Assistant United States Attorney:

Please take notice that on the above date and time, or soon thereafter as counsel may be heard, defendant, through counsel, will move the Court to order discovery as set forth in this motion and the attached memorandum of points and authorities.

This motion is based on the instant motion, the attached

memorandum in support of the motion, and any evidence or argument presented before or at the hearing on the motion.

Dated: December 19, 2006.

Respectfully submitted,

/s/
MARK J. REICHEL
Attorney for Defendant

MOTION

I. INTRODUCTION

In the 1970s, Congressional hearings revealed that government agencies including the NSA had been for years conducting warrantless electronic eavesdropping, maintaining watchlists of purely domestic political dissidents, and using official secrecy policies to preserve their ability to monitor and investigate Americans outside the established boundaries of the Constitution and the laws of the nation. At that time, such well-intentioned men as J. Edgar Hoover feared the threat of Communism and "racial extremists" bent on "destroying our present form of government." Today, equally well-intentioned government officials fear the threat of "eco-terrorists" and animal rights "extremists" and "anarchists" at home. It is perhaps not surprising then that history is repeating itself, and that leaks to the media have led to a series of dramatic disclosures that the NSA is engaging once again in a program of warrantless data-gathering on a massive scale that encompasses not only foreign signals intelligence, but also data and information related to the purely domestic telephone calls and internet activities of Americans at home.[1]

This round of warrantless surveillance of Americans on U.S. soil began shortly after September 11, 2001, and was subsequently authorized by the President by written directive

[1] In well publicized cases, it is now known that P.E.T.A., Mothers For Peace, and other revolutionary cells are the victims of this spying. So is The ACLU and the National Association of Criminal Defense Lawyers, two organizations of which the author of this motion ***very proudly*** belongs.

in 2002. The government has conceded that its surveillance and interception program extends to electronic communications by telephone, internet, or other means in which one party is in the United States and one party is not. It also admits to intercepting communications when both parties were in the United States. And while the full scope of the government's electronic surveillance and interception programs have yet to be disclosed, there are strong indications that it goes well beyond what the government has thus far confirmed to the public.

There are at least two very logical reasons to believe that the government's surveillance programs extend to persons the government claims are connected to or know about activities claimed by the Earth Liberation Front (ELF) or the Animal Liberation Front (ALF). First, the government has repeatedly identified the ELF and ALF as "extremist" and "terrorist" movements, and it has asserted that the ELF and ALF "have become the most active criminal extremist elements in the United States." Animal Rights: Activism vs. Criminality: Hearing before the Senate Judiciary Committee, 108th Cong. 2nd Sess. 3 (May 18, 2004) (testimony of John E. Lewis, Deputy Asst. Director, Counterterrorism Division, FBI). The government consistently characterizes acts of sabotage and arson claimed by the ELF and the ALF as "terrorism." Second, the government has repeatedly noted international ties in its analyses of the ELF and ALF. In Congressional testimony, the FBI has described the origins of the groups in Great Britain. The government repeatedly

asserts that individual defendants who are ELF or ALF related receive financial support from outside the United States and that they would find safe haven with cohorts in other countries were they to flee.

In this case, the criminal complaint on file states just that.

Thus, while the government has not specifically identified ELF and ALF, and those with philosophical sympathies to ELF/ALF, as targets of any secret, warrantless monitoring, or surveillance, the unequivocal assertions that the defendant in this case is among the most serious domestic terrorist threats the nation faces, coupled with claims of international connections and support, make any purported member of the ELF or ALF a prime target of a comprehensive program to monitor the communications of "terrorists." And if, as communications insiders claim, the monitoring goes significantly beyond what the government has been free to publicly admit - if it intentionally sweeps in purely domestic communications and purposely harvests data for "mining" and analysis - then there can be no credible claim that the communications activity of the defendants has not been captured, analyzed, and retained.

The government has publicly stated that Mr. McDavid is an ELF member and an ALF member.

Electronic communications information and material, such as call data, e-mail, and internet activities, that is related to these defendants and that has been gathered or mined by the NSA or any other agency is discoverable under

Fed. R. Crim. P. 16(a)(e)(i) and (iii), as well as Brady and Kyles. The government prosecutors have an affirmative duty to obtain this data and turn it over to the defense.

II. BACKGROUND ON THE NSA SURVEILLANCE PROGRAM

It has been scarcely 12 months since the media broke its silence regarding NSA's warrantless surveillance program. As detailed below, media reports were followed by government admissions of some aspects of the program, while other aspects remain shrouded in mystery or simply "unconfirmed." The disclosures have led to several lawsuits, an outpouring of concern among elected officials, and a profusion of scholarly opinions on the legality of the surveillance and eavesdropping.

It appears that, in reality, there is more than one program. The NSA has been authorized by the President to eavesdrop on specific communications between persons in the United States and persons outside the United States, where agency analysts believe it will lead them to terrorists. In addition, the NSA has launched a massive electronic communication data-harvesting operation, which requires the cooperation of major telecommunications facilities. Both programs have led to the interception of purely domestic data; in the case of the latter program, there is no indication in publicly available documents that the system is even designed to screen out purely domestic communications. As also noted below, there are strong indications that there are yet other programs, the scope and details of which have yet to be publicly revealed in any way.

A. Disclosure of the NSA's Warrantless Electronic Surveillance Program

The New York Times first reported on December 16, 2005 that sometime after September 11, 2001, President Bush "secretly authorized the National Security Agency to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without the court-approved warrants ordinarily required for domestic spying." James Risen and Eric Lichtblau, Bush Lets U.S. Spy on Callers Without Courts, The New York Times (Dec. 16, 2005). The program, according to the authors, allowed the NSA to conduct warrantless eavesdropping on people in the United States who were linked, directly or indirectly, to suspected "terrorists" through a chain of phone numbers and e-mail addresses. See id. The authors stated, however, that officials had told them that warrants were still required for eavesdropping on entirely domestic communications. Id.
A day after the story broke, the President confirmed that the NSA was engaged in warrantless surveillance. In his weekly radio address, President Bush stated:

> In the weeks following the terrorist attacks on our nation, I authorized the National Security Agency, consistent with U.S. law and the Constitution, to intercept the international communications of people with known links to al Qaeda and related terrorist organizations. Before we intercept these communications, the government must have information that establishes a clear link to these terrorist networks.

President's Radio Address (December 17, 2005), at http://www.whitehouse.gov/news/releases/2005/12/20051217.html.

As described by administration officials in the days

after the disclosures, the NSA Program involves neither a court nor a Justice Department official in determining which communications to intercept and which persons to monitor. Rather, these decisions are made by an NSA employee, who need not be a lawyer. According to Lieutenant General Michael V. Hayden (USAF), "[t]he judgment is made by the operational work force at the National Security Agency using the information available to them at the time, and the standard that they apply - and it's a two-person standard that must be signed off by a shift supervisor, and carefully recorded as to what the operational imperative to cover any target, but particularly with regard to those inside the United States." Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, at 8 (Dec. 19, 2005)

On May 11, 2006, USA Today reported that the NSA was also secretly harvesting phone call records of "tens of millions of Americans," with the assistance of some of the nation's largest telecommunications carriers, such as AT&T, BellSouth, and Verizon. Leslie Cauley, "NSA Has Massive Database Of Americans' Phone Calls," USA Today (May 11, 2006) This program, like the warrantless eavesdropping program, started shortly after the attacks of September 11, 2006. Id. The NSA requested, and apparently obtained, "call-detail records," which are a complete listing of the calling histories of millions of customers. Id. As the authors noted, the NSA's domestic program is far more expansive than what the White House had acknowledged in December 2005. Id.

Shortly after the revelation of the NSA's call database and data-mining program, Seymour Hersh of The New Yorker wrote about disclosures made to him by intelligence officials. An insider at a major telecommunications carrier explained that the company had "set up a top-secret high-speed circuit between its main computer complex" and a government intelligence computer center. The effect was to provide the government "total access to all the data." Seymour M. Hersh, "Listening In," The New Yorker (May 29, 2006). The NSA was also eavesdropping, without warrants, on callers to investigate them, in some cases without even going to the FISA court, for fear of having to reveal details of the program. See id. See also Lichtblau & Risen, "Eavesdropping Effort Began Soon After Sept. 11 Attacks," The New York Times (December 18, 2005) ("In the early years of the operation, there were few, if any, controls placed on the activity by anyone outside the security agency, officials say. It was not until 2004, when several officials raised concerns about its legality, that the Justice Department conducted its first audit of the operation. Security agency officials had been given the power to select the people they would single out for eavesdropping inside the United States without getting approval for each case from the White House or the Justice Department, the officials said.")

Mark Klein, who was working as a technician at AT&T's San Francisco facility when the NSA's data-harvesting technology was installed, issued a statement that was published by Wired Magazine. He explained that

In 2003 AT&T built "secret rooms" hidden deep in the bowels of its central offices in various cities, housing computer gear for a government spy operation which taps into the company's popular WorldNet service and the entire internet. These installations enable the government to look at every individual message on the internet and analyze exactly what people are doing. Documents showing the hardwire installation in San Francisco suggest that there are similar locations being installed in numerous other cities.

"Whistle-Blower's Evidence, Uncut," Wired (May 22, 2006), at http://www.wired.com/news/technology/0,70944-0.html?tw=wn_index_18. As outlined in detail by Mr. Klein in his statement, as well as in documents filed in the pending case of Hepting v. AT&T, No. C06-672 VRW (N.D. Cal.), AT&T installed "splitters" to divide the signal on high-speed fiber-optic circuits carrying communications traffic on AT&T's "common backbone." Id. See also, Hepting, Order Denying Motion to Dismiss at 23-24 (July 20, 2006). The effect of splitting the signal and rerouting a portion of it to the NSA is that the agency is given access to wholly domestic electronic communications information of hundreds of thousands, if not millions, of Americans. See, e.g., Eric Lichtblau and James Risen, "Domestic Surveillance: The Program; Spy Agency Mined Vast Data Trove, Officials Report," The New York Times (December 24, 2005) (explaining that access to the switches that route electronic communications would be significant, because, in the words of Phil Karn, a computer engineer and technology expert, "'what you're really

talking about is the capability of an enormous vacuum operation to sweep up data.'")

The present administration has formally confirmed the existence of the data-harvesting and mining aspects of the NSA Program. Some pending litigation, such as the Hepting class action noted above, has focused, so far, on whether the government may rely on the state secrets privilege in order to preclude public confirmation, or negation, of aspects of the Program. However, many have interpreted Mr. Gonzales' public citation of Smith v. Maryland, 442 U.S. 735 (1979), in defense of presidential authority to obtain the data without a warrant or court order, as tacit admission that the data-mining will continue. See Walter Pincus, "Gonzales Defends Phone-Data Collection," The Washington Post (May 24, 2006). See also "Hayden Insists NSA Surveillance Is Legal," The Associated Press (May 18, 2006) (explaining that during his confirmation hearing, Gen. Hayden would only talk about the part of the program the President had confirmed; asked if it was the whole program, he responded "I'm not at liberty to talk about that in open session.")

B. Reaction to the Disclosure of the NSA Program of Warrantless Surveillance

In the aftermath of the disclosure of the NSA Program, a group of constitutional scholars, law professors and former government officials delivered an open letter to Congress, challenging the government's asserted legal justification for the NSA Program. They explained:

"Although the program's secrecy prevents us from being privy to all of its details, the Justice Department's defense of

what it concedes was secret and warrantless electronic surveillance of persons within the United States fails to identify any plausible legal authority for such surveillance. Accordingly, the program appears on its face to violate existing law." Letter from Curtis A. Bradley and others to Sen. Bill Frist an others, at 2 (Jan. 9, 2006) (hereafter "Curtis Letter") Other legal commentators and legislators reached the same conclusion. On January 5, 2006, the Congressional Research Service, the non-partisan public policy research arm of Congress, issued a memorandum to members of Congress on the subject. Elizabeth B. Bazan and Jennifer K. Elsea, "Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information, Congressional Research Service" (Jan. 5, 2006) (hereafter "CRS Presidential Authority Memo"). The 44-page document provides a comprehensive legal analysis of the administration's justification for the NSA Program, concluding that it, "as presented in the summary analysis from the Office of Legal Affairs, does not seem to be as well-grounded as the tenor of that letter suggests." CRS Presidential Authority Memo, at 44. The authors stated that [I]t appears unlikely that a court would hold that Congress has expressly or impliedly authorized the NSA electronic surveillance operations here under discussion, and it would likewise appear that, to the extent that those surveillances fall within the definition of "electronic surveillance" within the meaning of FISA or any activity regulated under Title III, Congress intended to cover the entire field with

these statues. Id.

Members of Congress from both parties called for an investigation into the NSA Program, and government's legal justification for it. See, e.g., Statement of Senator Patrick Leahy (D-Vt.), Ranking Member, Senate Judiciary Committee, Hearing On "NSA III: War Time Executive Power and the FISA Court" (March 28, 2006); Brian Knowlton, "Specter Says Surveillance Program Violated the Law," International Herald Tribune (February 5, 2006) (quoting Sen. Arlen Specter stating that the administration's legal justifications for the NSA Program were "strained and unrealistic," and that the NSA Program "is in flat violation of the Foreign Intelligence Surveillance Act")

Then, both the NSA itself and the Department of Justice Office of Professional Responsibility initiated investigations. See Dan Eggen, "Probe Set In NSA Bugging," The Washington Post (January 11, 2006) The OPR investigation was terminated when the Justice Department lawyers were denied the security clearances necessary to review the role of DOJ lawyers in the NSA Program. In mid-July, Attorney General Gonzales testified that the decision to deny the security clearances necessary for the investigation to proceed was made by the President. See Dan Eggen, "Bush Thwarted Probe into NSA Wiretapping," The Washington Post (July 19, 2006).

In addition to Congressional hearings, aborted investigations, and broad-based expressions of concern among former government officials and legal scholars, the NSA

Program has generated litigation, both in the context of ongoing criminal cases and in the civil courts. See, e.g., ACLU v. NSA (E.D. Mich.), filed Jan. 17, 2006; Hepting v. AT&T, (C.D. Cal.), filed Jan. 31, 2006; Electronic Privacy Information Center v. Department of Justice, (D.D.C.), filed Jan. 19, 2006. In August, The Honorable Anna Diggs Taylor ruled in ACLU v. NSA that the NSA Program, at least those portions of it which have been confirmed by the administration, violates the First and Fourth Amendment and statutory law. ACLU v. NSA, Order on Motion for Permanent Injunction, Case No. 06-CV-10204 (E.D.Mich. August 17, 2006)

C. What Data and Material the NSA Program, and Others Like It, Capture and Maintain

The defense seeks discovery of any and all information, data, and material obtained through warrantless surveillance conducted by government agencies, including the NSA. It is important, therefore, to understand what is known about the types of data that have been captured and obtained through the NSA Program.

1.The NSA Program Captures Purely Domestic Communications Data

The NSA Program, whether by accident or design, has intercepted *wholly domestic* calls. As reported late last year on the heels of the initial revelations of the NSA Program's existence, officials admitted that "some purely domestic communications have been captured because of the technical difficulties of determining where a phone call or e-mail message originated." See Scott Shane, "News of

Surveillance Is Awkward for Agency," The New York Times (December 22, 2005); As Seymour Hersh reported in The New Yorker, the NSA began, in some cases, to eavesdrop on callers (often using computers to listen for key words) or to investigate them using traditional police methods. A government consultant told [Hersh] that tens of thousands of Americans had had their calls monitored in one way or the other. "In the old days, you needed probable cause to listen in," the consultant explained. "But you could not listen in to generate probable cause. What they're doing is a violation of the spirit of the law." Seymour Hersh, "Listening In," The New Yorker (May 29, 2006)"[O]fficials familiar with [the NSA Program said it] eavesdrops without warrants on up to 500 people in the United States at any given time. The list changes as some names are added and others dropped, so the number monitored in this country may have reached into the thousands since the program began, several officials said." See "Bush Lets U.S. Spy On Callers Without Courts", supra.

Data mining. Beyond the parameters of the warrantless interception aspects of the Program, there remains the NSA's resort to data-mining. As to this effort, as described by witnesses in the Hepting litigation and others, there is no indication the administration would even attempt to limit it to communications between U.S. persons and persons overseas. As noted in the USA Today report, this program, intentionally and by design, "reaches into homes and businesses across the nation by amassing information about the calls of ordinary

Americans - most of whom aren't suspected of any crime." Leslie Cauley, "NSA Has Massive Database of Americans' Phone Calls," USA Today (May 11, 2006). As James Bamford, author of The Puzzle Palace, explains it, "[d]espite the low odds of having a request turned down, President Bush established a secret program in which the N.S.A. would bypass the FISA court and begin eavesdropping without warrant on Americans. This decision seems to have been based on a new concept of monitoring by the agency, a way, according to the administration, to effectively handle all the data and new information. At the time, the buzzword in national security circles was data mining: digging deep into piles of information to come up with some pattern or clue to what might happen next. Rather than monitoring a dozen or so people for months at a time, as had been the practice, the decision was made to begin secretly eavesdropping on hundreds, perhaps thousands, of people for just a few days or a week at a time in order to determine who posed potential threats. Those deemed innocent would quickly be eliminated from the watch list, while those thought suspicious would be submitted to the FISA court for a warrant." James Bamford, "Private Lives: The Agency That Could Be Big Brother," The New York Times, (Dec. 25, 2005).

In at least two lawsuits, plaintiffs allege that the NSA and major telecommunications providers set up equipment and procedures to engage in domestic call monitoring. See, e.g., Complaint, McMurry v. Verizon Communications Inc., 06 CV 3650 (S.D.N.Y) (alleging that the NSA asked AT&T to help it set up

a domestic call monitoring site seven months before the September 11, 2001 attacks); Andrew Harris, "Spy Agency Sought U.S. Call Records Before 9/1, Lawyers Say," Bloomberg (June 30, 2006); Hepting v. AT&T, No. 06-0672 VRW (N.D. Cal.). Mark Klein, the AT&T technician and whistle-blower referred to above in this memo who witnessed the building of a secret room for NSA equipment, stated that "[i]t appears the NSA is capable of conducting what amounts to vacuum-cleaner surveillance ***of all the data crossing the Internet, whether that be by people's e-mail, Web surfing or any other data.***" (Emphasis added.) David Kravets, "Whistle-Blower Says AT&T Gave NSA Access to Network," Associated Press (April 14, 2006) See also, The Puzzle Palace, at 318-19 (explaining that because of NSA's "vacuum-cleaner" approach to intelligence collection, which involves gathering the maximum amount of telecommunications data and then filtering it, "if an organization is targeted, all its members' communications to, from or even mentioning the individual are scooped up.").

Mr. Klein also reported that he was told by other AT&T technicians that similar "secret rooms" were constructed in other locations, including San Jose, Los Angeles, San Diego, and Seattle.

2. The NSA Program Captures Privileged Communications

The NSA Program has apparently intercepted privileged attorney-client communications. Indeed, there are indications that the NSA Program's protocols do not call for distinguishing privileged from non-privileged communications. In response to inquiries from Congress, the Justice Department stated that "[a]lthough the [NSA] program does not specifically target the communications of attorneys or physicians, calls involving such persons would not be categorically excluded from interception" as long as they satisfied the other criteria. Letter from William Moschella to F. James Sensenbrenner, Attachment "Responses to Joint Questions from House Judiciary Committee Minority Members," 45, at 15 (March 24, 2006) at http://fas.org/irp/agency/doj/fisa/doj032406.pdf).

Sadly, privileged communications have in fact been intercepted and apparently used. In Al-Haramain Islamic Foundation, Inc., et al. v. Bush, et al., CV 06 274 MO (D. Oregon), the plaintiffs have alleged that in March and April 2004, the NSA Program targeted and captured electronic communications between Al-Haramain, a Saudi charity (in the person of its Director, who was in Saudi Arabia) and two of its lawyers in the United States. See Al-Haramain, Complaint at 19. The Complaint also alleges that NSA provided logs of those intercepted conversations to the U.S. Treasury Department's Office of Foreign Asset Control, which in turn relied upon them in designating Al-Haramain a "specially designated global terrorist" in September 2004. Id. at

20-21.

The plaintiffs' suspicions that the lawyers' communications had been intercepted were based on documents Treasury provided to Al-Haramain's lawyers in May, 2004 in connection with Al-Haramain's challenge to OFAC's freeze of Al-Haramain's assets in February of that year. It appears from the public record that Treasury officials provided the logs of the intercepted calls, determined this was an error, and demanded in November of 2004 that the documents, marked "top secret," be returned. By that time, however, the documents were also in the possession of a Washington Post reporter, David Ottaway. Mr. Ottaway had not written anything about them. Both Al-Haramain's lawyers and Mr. Ottaway complied with Treasury's demand. See Carol Leonnig, "Paper Said to Show NSA Spying Given to Post Reporter in 2004", The Washington Post (March 3, 2006). The Justice Department has also indicated, in the ACLU v. NSA litigation, that "some plaintiffs might have more reason to be concerned than others. Lawyers who represent suspected terrorists, he said, 'come closer to being in the ballpark of the terrorist surveillance program.'" See Adam Liptak, "Arguments on Spy Program Are Heard by Federal Judge," The New York Times (June 13, 2006).

3. The Government Uses the NSA Program or Other Programs to Conduct Warrantless Surveillance and Maintain Databases of Political Dissidents

Through media reports and Congressional hearings, it has become clear that there are likely still other warrantless electronic surveillance programs that have not been disclosed. On February 6, 2006, Attorney General Gonzalez testified before the Senate Judiciary Committee concerning the "Terrorist Surveillance Program" that the President had publicly disclosed. In part, he reiterated the administration's previous statements that the only communications involving anyone in the United States that were being monitored were those involving at least one person outside the United States and in which there was reasonable grounds to believe that one party is an agent of Al Qaeda or an affiliated terrorist organization. See Transcript, U.S. Senate Judiciary Committee Holds a Hearing on Wartime Executive Power and the NSA's Surveillance Authority, Part I of IV, washingtonpost.com (February 6, 2006) at http://www.washingtonpost.com/wp-dyn/content/article/2006/02/06/AR2006020600931.html.

Weeks later, the Attorney General issued a letter to Sen. Arlen Specter in which he carefully limited his remarks to "the Terrorist Surveillance Program as described by the President." Letter from Atty. Gen. Alberto Gonzales to Sen. Arlen Specter, at 4 (February 28, 2006). He stated that he "did not and could not address … any other classified intelligence activates." Id. See also Charles Babbington and Dan Eggen, "Gonzales Seeks to Clarify Testimony On

Spying; Extent of Eavesdropping May Go Beyond NSA Work," The Washington Post (March 1, 2006); Shane Harris, "NSA Program Broader Than Previously Described," National Journal (March 17, 2006).

Finally, in subsequent testimony before the House Judiciary Committee, Mr. Gonzales was asked directly whether he could rule out purely domestic warrantless surveillance between two Americans. Mr. Gonzales responded "I'm not going to rule it out …" House Judiciary Committee Members' Questions for Attorney General Gonzalez on the NSA Warrantless Surveillance Activity (April 6, 2006) at p.7 at http://www.house.gov/lofgren/nsa_testimony_from_Gonzales.pdf. See also Mark Sherman, "Gonzales Draws Criticism From Panel Chief," The Associated Press (April 6, 2006); Dan Eggen, "Gonzales: Bush Could Order Domestic Wiretaps," The Washington Post (April 6, 2006).

In addition to uncovering the NSA's Program, the media has disclosed surveillance activities of other agencies. The Pentagon has reportedly been involved in assembling databases to track political dissidents within the United States. As reported in The Wall Street Journal, based on documents reviewed by its reporters, the Pentagon has monitored the activities of more than 20 antiwar groups around the country over the past three years. "It has reviewed photographs and records of vehicles and protestors at marches to see if different activities were being organized by the same instigators." Robert Black & Jay Solomon, "Pentagon Steps Up Intelligence Efforts Inside U.S. Borders," The Wall Street

Journal (April 27, 2006). According to the article, the Department of Defense's Counter Intelligence Field Activity program has also been "data-mining" through its "Threat and Local Observation Notice" ("TALON") reporting process. Id. See also Ted Bridis, "ACLU Says FBI Misused Terror Powers," The Associated Press (December 20, 2005) (explaining that the FBI launched a domestic terrorism investigation against People for the Ethical Treatment of Animals because it was "'suspected of providing material support and resources to known domestic terrorism organizations,' including the [ALF] and [ELF].").

IV. BACKGROUND ON GOVERNMENT ALLEGATIONS OF TERRORISM IN THIS CASE

The defendant in this case is charged with conspiracy to commit arson. The government, through their press releases and press conferences, has made it abundantly clear, however, that it considers the alleged acts at issue to be acts of terrorism, and that it has pursued persons it believes to be part of the ELF or ALF as terrorists. It has made use of the full panoply of terrorism-related investigative resources.

A. Government Characterization of ELF and ALF as "Terrorist" Organizations

Government and law enforcement reports consistently refer to actions claimed by ALF and ELF as "terrorism" and to the perpetrators as "terrorists." See, e.g., U.S. Department of Justice, Federal Bureau of Investigation, Terrorism 2000/2001, FBI Publication #0308 at http://www.fbi.gov/publications/terror/terror2000_2001.htm#page_35 (noting, among other references to "terrorism" that

"[m]uch like terrorist groups of the past, animal rights and environmental terrorists are adopting increasingly militant positions with respect to their ideology and chosen tactics. Terrorists who engage in criminal activity on behalf of these causes have continued to distinguish themselves from their counterparts in the mainstream animal welfare and conservation movements, who oppose the inhumane treatment of animals and environmental degradation but choose legal and nonviolent means of opposition."). The Terrorism 2000/2001 publication lists incidents of property damage and arson purportedly claimed by ELF and ALF on its comprehensive list of "terrorism" incidents in the United States from 1990 to 2001, a list which includes the attacks of September 11, 2001 by Al Qaeda, the 1995 bombing of the federal building in Oklahoma City, and the fatal anthrax mailings in the Autumn of 2001. In its concluding statement, the FBI explains that in December of 2001, it "merged the analytical resources of its Investigative Services Division into the Counterterrorism Division to improve its ability to gather, analyze, and share critical national security information with the broader Intelligence Community and the FBI's law enforcement partners. At the beginning of the 21st century the problem of terrorism has become a global one, and the FBI continues to improve the capacity of its counterterrorism program to accurately assess and effectively counter the dynamic variety of domestic and international terrorist threats." Id.

In annual reports to Congress, FBI and Justice Department officials have emphasized their view that the ALF and ELF

constitute a terrorist threat. In 2004, John E. Lewis testified in the Senate Judiciary Committee that over the past several years, "special interest extremism, as characterized by the [ALF], the [ELF], and related extremists, has emerged as a serious domestic terrorist threat. Statement of John E. Lewis, Deputy Asst. Dir., Counterterrorism Division, FBI, before the Senate Judiciary Committee (May 18, 2004) at http://www.fbi.gov/congress/congress04/lewis051804.htm (hereafter "Lewis 2004 Testimony). The next year, Mr. Lewis told members of Congress that ELF and ALF were "[o]ne of today's most serious domestic terrorism threats." Statement of John E. Lewis, Deputy Asst. Dir., Counterterrorism Division, FBI, before the Senate Committee on Environment and Public Works (May 18, 2005) at http://www.fbi.gov/congress/congress05/ lewis051805.htm (hereafter "Lewis 2005 Testimony").

Most importantly, the U.S. Attorney has referred directly to this defendant and this prosecution using the term "terrorism." In a January 25, 2006 press conference announcing the Indictment in this case, the U.S. Attorney states just that.

B. Government Use of the Joint Terrorism Task Force Resources

The government has also clearly indicated that it employs the wide range of terrorism-related investigatory resources at its disposal to investigate alleged acts of the ELF and ALF. As explained by Deputy Assistant Director Lewis in his Congressional testimony:

We draw on the resources of our Terrorist Financing

Operations Section to support field investigations into domestic terrorism, just as we do for international terrorism investigations. We also draw upon our expertise in the area of communication analysis to provide investigative direction. Second, we have strengthened our intelligence capabilities. . . . And we have developed an intelligence requirement set for animal rights/eco-terrorism, enabling us to better collect, analyze, and share information. Finally, we have strengthened our partnerships. We have combined our expertise and resources with those of our federal, state, and local law enforcement partners nationwide through our 103 Joint Terrorism Task Forces. We have increased training for JTTF members and have strong liaison with foreign law enforcement agencies. Lewis 2005 Testimony at http://www.fbi.gov/congress/congress05/lewis051805.htm.

Documents provided to the defense in discovery are equally plain that the Joint Terrorism Task Force resources were employed in this investigation, and that this was, in every practical and logical sense, a terrorism investigation, as the FBI conceives of such.

V. DISCUSSION

The prosecutor plays a special role in the search for truth in criminal trials. See Strickler v. Greene, 527 U.S. 263, 280 (1999). "The United States Attorney is the representative not of an ordinary party to a controversy, but of a sovereignty whose obligation to govern impartially is as compelling as its obligation to govern at all; and whose interest, therefore, in a criminal prosecution is not that it

shall win a case, but that justice shall be done." Berger v. United States, 295 U.S. 78, 88 (1935).

Consonant with the special role of the United States Attorney, the Supreme Court held in Brady v. Maryland "that the suppression by the prosecution of evidence favorable to an accused upon request violates due process where the evidence is material either to guilt or punishment, irrespective of the good faith or bad faith of the prosecution." Brady, 373 U.S. 83, 87 (1963). The duty encompasses impeachment evidence as well as exculpatory evidence, United States v. Bagley, 473 U.S. 667, 676 (1985), and it covers information "known to the others acting on the government's behalf in the case, including the police." Kyles v. Whitley, 514 U.S. 419, 436-37 (1995).

The withholding of impeachment evidence violates the strictures of Brady whenever the evidence is "material." As explained in Bagley, impeachment evidence is material when "if disclosed and used effectively, it may make the difference between conviction and acquittal." Bagley, 473 U.S. at 676.

Rule 16(a) also addresses the government's duty to disclose material to the defense: Fed. R. Crim. P. 16(a)(e) requires the government to provide access to material "within the government's possession, custody or control" where "(i) the item is material to preparing the defense; (ii) the government intends to use the item in its case-in-chief at trial; or (iii) the item was obtained from or belongs to the defendant."

A. Government's Duty to Disclose the Existence of any NSA Surveillance

It has long been settled that a defendant has the right to know whether his communications have been intercepted and whether such interceptions contributed in any way to the government's investigation and prosecution of the case against him. See, e.g., Gelbard v. United States, 408 U.S. 41 (1972) (government required to inform grand jury witness whether questions to be posed were the product of unlawful electronic surveillance); Alderman v. United States, 394 U.S. 165 (1969) (government required to produce to defendant all intercepts resulting from illegal electronic surveillance in advance of evidentiary hearing). Justice Douglas, in a prescient concurring opinion in Gelbard, stated that "[t]oday's remedy assumes an added and critical measure of importance for, due to the clandestine nature of electronic eavesdropping, other inhibitions on officers' abuse, such as the threat of damage actions, reform through the political process, and adverse publicity, will be of little avail in guarding privacy." 408 U.S. at 67 (Douglas, J., concurring). See also United States v. Coplon, 185 F.2d 629, 637-38 (2d Cir. 1950).

That same concern is even more evidence today, in a technologically advanced world, and where the NSA's warrantless electronic surveillance program has thus far not been authorized or supervised by a court of law - and where the only court to have passed on its constitutionality has rejected it and enjoined the government from continuing it.

Congress's focus is on prospective action, rather than retrospective inquiry into the genesis and operation of the NSA Program. And the administration has effectively shut down other potential auditors, such as the Department of Justice Office of Professional Responsibility, leaving the courts as the sole vindicators of those whose rights have been infringed by the NSA Program.

In Alderman, the Court faced essentially the same issue. The defendants had been convicted, and while their appeals were pending "it was revealed that the United States had engaged in electronic surveillance which might have violated their Fourth Amendment rights and tainted their convictions." 394 U.S. at 167. In its analysis, the Supreme Court framed the issue, and the next necessary phase of the litigation, as follows:

> Such violation would occur if the United States unlawfully overheard conversations of a petitioner himself or conversations occurring on his premises, whether or not he was present or participated in those conversations. The United States concedes this much and agrees that for purposes of a hearing to determine whether the Government's evidence is tainted by illegal surveillance, the transcripts or recordings of the overheard conversations of any petitioner or of third persons on his premises must be duly and properly examined in the District Court.

Alderman, 394 U.S. at 176. Further, the Alderman the Court recognized that any fruits of such illegal electronic surveillance would also be tainted. The question as stated in Wong Sun v. United States, 371 U.S. 471, 488 (1963), is "whether, granting establishment of the primary illegality, the evidence to which instant objection is made has been come at by exploitation of that illegality or instead by means

sufficiently distinguishable to be purged of the primary taint." See also Nardone v. United States, 308 U.S. 338, 341 (1939). Id. at 180-81. See also 394 U.S. at 176-77. The Court noted in that case that the government acknowledged its responsibility to provide the defendants with the surveillance information in order to permit litigation of the issue:

> The Government concedes that it must disclose to petitioners any surveillance records which are relevant to the decision of this ultimate issue. And it recognizes that this disclosure must be made even though attended by potential danger to the reputation or safety of third parties or to the national security - unless the United States would prefer dismissal of the case to disclosure of the information.

Id. at 394 U.S. at 170-71.

The same inquiry and responses are necessary in this case to determine whether communications of the defendants or anyone else has played any role in the investigation or prosecution of this case.

In at least five other cases, the Courts have compelled the government to disclose whether the NSA Program contributed in any way to the investigation or prosecution of the particular cases. See, e.g., United States v. Al-Timimi, Case No. 05-4761 (4th Cir. January 24, 2006) (remanding the matter to the District Court for an evidentiary hearing, with authority to "order whatever relief or changes in the case, if any, it considers appropriate," although the case was already on appeal); United States v. Abu Ali, Case No. CR 05-053, Order on Motion to Stay (E.D. Va. Feb. 17, 2006.); United States v. Aref, Case No. 04 Cr. 402 (TJM) (N.D.N.Y.); Turkmen v. Ashcroft, Case No. 02 CV. 2307 (JG) (E.D.N.Y.

March 7, 2006); Al-Haramain Islamic Foundation, Inc., et al. v. Bush, et al., CV 06 274 MO (D. Oregon).

In Abu Ali, the District Court ordered the government to file with the court a declaration under oath of someone with personal knowledge, the authority to speak on behalf of the government, its intelligence agencies and contractors, and who can definitively answer whether presidentially approved warrantless interception of electronic communications information was (1) used to obtain a warrant from the FISA Court or (2) used in obtaining evidence that was presented to the jury at trial. See Abu-Ali, Order at 4. The court in that case specifically recognized the AUSA's assertion that neither he nor anyone on the investigation team was aware of any such information. Even accepting that at face value, the court concluded that the prosecutors might now know of the existence or use of such information. Id. at 3.

See also United States v. Libby, 2006 WL 574260, at *4-6 (D.D.C. March 10, 2006) (requiring Special Counsel to obtain from other government agencies certain discoverable documents and information, including those that might be classified).

In Al-Haramain, the Court not only ordered the government to respond, but refused to permit the government to file its response ex parte, finding, according to a news report quoting a transcript of telephonic court proceedings, that plaintiffs have "a right to know the legal and factual positions being taken by the government so they can respond to them." See Kevin Johnson, "Government Keeps Info From Defense Lawyers In Terror Cases," USA Today (May 21, 2006) .

Mr. McDavid is entitled to the same relief here. The reality is that the ELF and ALF were avowedly high-priorities for terrorism investigators. It is either probable, or at least reasonable to believe, that NSA surveillance resources were devoted to investigating the string of unsolved incidents that the FBI traces back to 1993. Furthermore, the discovery in this case and other documents obtained by the defense plainly indicate that Mr. McDavid himself was of particular interest to the government for his political activities and views beginning no later than August of 2004 when he met the informant, Anna. Based on the simplest review of the discovery, it appears that it is highly likely that government monitoring of Mr. McDavid's activities occurred prior to when he first became a suspect or a person of interest in the investigation of the crimes for which he is now charged. In other words, Mr. McDavid was already on the counter-terror radar of government agencies before he became a suspect in this case. Common sense, reason, and appreciation of the lessons of monitoring campaigns gone by teaches that a person such as Mr. McDavid would fall within the scope of a warrantless monitoring scheme now.

The appropriate initial step is that directed by the Abu-Ali court - an order requiring a declaration under oath of someone with personal knowledge, the authority to speak on behalf of the government, its intelligence agencies and contractors, and who can definitively answer whether warrantless interception of electronic communications information was either used to obtain a warrant from the FISA

Court or used in obtaining evidence that the government now possesses and intends to use in its case. If the answer is "yes" then the Court should further order the government to identify the specific information used, its nature and extent, and what specific constitutional or statutory authority the government relied on in obtaining the information without a warrant. See Abu-Ali, at 4. In this context, the defense notes that while one court has already held that the NSA Program is unlawful and unconstitutional, see ACLU v. NSA, no such finding is required to justify an order related to disclosure. If there is warrantless surveillance information to be disclosed, the defense will request the opportunity to brief more fully the issue of the illegality of the seizures, should the Court deem it necessary.

B. Government's Duty to Disclose Communications Data Pursuant to Brady

There is an independent basis for disclosure of the NSA Program data under the doctrines of Brady v. Maryland, 373 U.S. 83 (1963), Kyles v. Whitely, 514 U.S. 419, 436-37 (1995), and Giglio v. United States, 405 U.S. 150 (1972). It is well-settled that the AUSAs cannot simply rely on their own knowledge of the existence of impeachment evidence; they must affirmatively reach out to sister agencies who might reasonably be expected to have garnered such evidence. Here, government officials have repeatedly made statements that would qualify the ALF and ELF, and anyone the government suspected of being connected to the ALF and ELF, for

admission into the warrantless electronic eavesdropping program - they are asserted to be terrorists, they are asserted to have international origins, links, and finances, they are asserted to be at the top of the government's list of investigatory priorities.

While it is unnecessary for the defense to outline the types of impeachment material that may be in the government's possession but not yet disclosed, the defense notes that it could take several different forms:

Intercepted e-mail messages or phone calls between cooperating witnesses or cooperating defendants;

Intercepted communications in which cooperating witnesses or cooperating defendants make statements that are inconsistent with their statements to government prosecutors and agents.

Therefore, consistent with the duties imposed upon government prosecutors by the Constitution, the defense requests that the court order the government to affirmatively request the production of the NSA Program data and information pursuant to Brady, Kyles, and Giglio.

VI. CONCLUSION

For all of the reasons expressed above, the defense requests an order requiring the production of warrantless electronic surveillance information, data, and communications, including material garnered pursuant to the NSA Program.

Respectfully submitted this 19th day of December, 2006.

/S/

MARK J. REICHEL
Attorney for Defendant