

1 Elizabeth J. Cabraser (State Bar No. 083151)  
Barry R. Himmelstein (State Bar No. 157736)  
2 Michael W. Sobol (State Bar No. 194857)  
Eric B. Fastiff (State Bar No. 182260)  
3 Allison S. Elgart (State Bar No. 241901)  
LIEFF, CABRASER, HEIMANN & BERNSTEIN, LLP  
4 275 Battery Street, 30th Floor  
San Francisco, CA 94111-3339  
5 Telephone: (415) 956-1000  
Facsimile: (415) 956-1008

6 Interim Class Counsel for MCI Class  
7

8 UNITED STATES DISTRICT COURT  
9 NORTHERN DISTRICT OF CALIFORNIA  
10 (San Francisco Division)

11  
12 IN RE NATIONAL SECURITY  
AGENCY TELECOMMUNICATIONS  
13 RECORDS LITIGATION

14 THIS DOCUMENT RELATES TO:

15 All Class Actions Against MCI, Verizon,  
16 Sprint, BellSouth, Cingular, and  
Transworld Defendants

17 *Campbell v. AT&T Communications of*  
18 *California* (No. 06-3596); *Riordan v.*  
19 *Verizon Communications, Inc.* (No. 06-  
3574)

MDL Docket No. 06-1791 (VRW)

DECLARATION OF BARRY HIMMELSTEIN  
AND REQUEST FOR JUDICIAL NOTICE IN  
SUPPORT OF CLASS PLAINTIFFS'  
CONSOLIDATED RESPONSE TO ORDER TO  
SHOW CAUSE WHY RULINGS ON *HEPTING*  
MOTIONS TO DISMISS SHOULD NOT  
APPLY

Date: February 9, 2007  
Time: 2:00 p.m.  
Courtroom: 6, 17<sup>th</sup> Floor  
Judge: Hon. Vaughn R. Walker

20  
21  
22  
23  
24  
25  
26  
27  
28

**DECLARATION OF BARRY HIMMELSTEIN**

I, BARRY HIMMELSTEIN, declare and state:

1. I am a member in good standing of the State Bar of California, and admitted to practice in this district. I am a partner in the law firm of Lief, Cabraser, Heimann & Bernstein, LLP, which has been appointed as Interim Class Counsel for the MCI Class in this multidistrict litigation proceeding. I have personal knowledge of the matters set forth herein, and could and would testify competently thereto if called upon to do so.

2. Attached hereto are true and correct copies of the following documents:

|           |  |
|-----------|--|
| Exhibit A | James Risen & Eric Lichtblau, <i>Bush Lets U.S. Spy on Callers Without Courts</i> , The New York Times, December 16, 2005.   |
| Exhibit B | Transcript of <i>President's Radio Address</i> (December 17, 2005), available at <a href="http://www.whitehouse.gov/news/releases/2005/12/print/20051217.html">http://www.whitehouse.gov/news/releases/2005/12/print/20051217.html</a> .   |
| Exhibit C | Transcript of <i>Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence</i> (December 19, 2005), available at <a href="http://www.whitehouse.gov/news/releases/2005/12/print/20051219-1.html">http://www.whitehouse.gov/news/releases/2005/12/print/20051219-1.html</a> . |
| Exhibit D | Eric Lichtblau & James Risen, <i>Spy Agency Mined Vast Data Trove, Officials Report</i> , The New York Times, December 24, 2005.   |
| Exhibit E | Shane Harris & Tim Naftali, <i>Tinker, Tailor, Miner, Spy</i> (January 3, 2006), Slate.com, available at <a href="http://www.slate.com/toolbar.aspx?action=print&amp;id=2133564">http://www.slate.com/toolbar.aspx?action=print&amp;id=2133564</a> .   |
| Exhibit F | Lowell Bergman, Eric Lichtblau, Scott Shane, & Don Van Natta Jr., <i>Spy Agency Data After Sept. 11 Led F.B.I. To Dead Ends</i> , The New York Times, January 17, 2006.  |
| Exhibit G | Shane Harris, <i>NSA Spy Program Hinges On State-of-the-Art Technology</i> , National Journal, January 20, 2006, available at <a href="http://www.govexec.com/story_page.cfm?articleid=33212&amp;printerfriendlyVers=1&amp;">http://www.govexec.com/story_page.cfm?articleid=33212&amp;printerfriendlyVers=1&amp;</a> .                                |

|    |           |   |
|----|-----------|---|
| 1  | Exhibit H | Jeff Bliss, <i>Conyers Asks Companies Whether They Aided Wiretaps</i> , Bloomberg   |
| 2  |           | News, January 20, 2006.   |
| 3  | Exhibit I | Barton Gellman, Dafna Linzer, & Carol D. Leonnig, <i>Surveillance Net Yields Few</i>  |
| 4  |           | <i>Suspects</i> , Washington Post, February 5, 2006.  |
| 5  | Exhibit J | Leslie Cauley & John Diamond, <i>Telecoms Let NSA Spy On Calls</i> , USA Today,   |
| 6  |           | February 6, 2006.   |
| 7  | Exhibit K | Lesley Cauley, <i>NSA Has Massive Database of Americans' Phone Calls</i> , USA  |
| 8  |           | Today, May 11, 2006.  |
| 9  | Exhibit L | Transcript of Senator Bond's Statements, <i>NSA Wire Tapping Program Revealed</i> ,   |
| 10 |           | PBS Online Newshour Debate, May 11, 2006.   |
| 11 | Exhibit M | News Release, <i>Verizon Issues Statement on NSA and Privacy Protection</i> (May 12,  |
| 12 |           | 2006), available at <a href="http://newscenter.verizon.com/press-releases/verizon/2006/page.jsp?itemID=29670741">http://newscenter.verizon.com/press-</a>     |
| 13 |           | <a href="http://newscenter.verizon.com/press-releases/verizon/2006/page.jsp?itemID=29670741">releases/verizon/2006/page.jsp?itemID=29670741</a> .             |
| 14 | Exhibit N | News Release, <i>Full Statement From Attorney Of Former Qwest CEO Nacchio</i> (May  |
| 15 |           | 12, 2006), The Wall Street Journal Online ( <a href="http://online.wsj.com">http://online.wsj.com</a> ).  |
| 16 | Exhibit O | John Markoff, <i>Questions Raised For Phone Giants In Spy Data Furor</i> , The New  |
| 17 |           | York Times, May 13, 2006.   |
| 18 | Exhibit P | Transcript of Senate Majority Leader William Frist's Statements, <i>CNN Late Edition</i>  |
| 19 |           | <i>with Wolf Blitzer</i> , May 14, 2006.  |
| 20 | Exhibit Q | News Release, <i>BellSouth Statement On Governmental Data Collection</i> (May 15,   |
| 21 |           | 2006), available at   |
| 22 |           | <a href="http://bellsouth.mediaroom.com/index.php?s=press_release&amp;item=2860">http://bellsouth.mediaroom.com/index.php?s=press_release&amp;item=2860</a> . |
| 23 | Exhibit R | News Release, <i>Verizon Issues Statement on NSA Media Coverage</i> (May 16, 2006),   |
| 24 |           | available at  |
| 25 |           | <a href="http://newscenter.verizon.com/proactive/newsroom/release.vtml?id=93450">http://newscenter.verizon.com/proactive/newsroom/release.vtml?id=93450</a> . |
| 26 | Exhibit S | Jim Drinkard, <i>Verizon Says It Isn't Giving Call Records To NSA</i> , USA Today, May  |
| 27 |           | 16, 2006.   |
| 28 |           |   |

|    |           |   |
|----|-----------|---|
| 1  | Exhibit T | Transcript of Senator Roberts' Statements, <i>Senate Intelligence Chair Readies for Hayden Hearings</i> , NPR All Things Considered, May 17, 2006.  |
| 2  |           |   |
| 3  | Exhibit U | Seymour M. Hersh, <i>Listening In</i> , The New Yorker, May 29, 2006.   |
| 4  | Exhibit V | Susan Page, <i>Lawmakers: NSA Database Incomplete; Some Who Were Briefed About The Database Identify Who Participated And Who Didn't</i> , USA Today, June 30, 2006.  |
| 5  |           |   |
| 6  |           |   |
| 7  | Exhibit W | CBS/AP, <i>Congress To Be Briefed On NSA</i> (May 16, 2006), available at <a href="http://www.cbsnews.com/stories/2006/05/17/national/printable1624039.shtml">http://www.cbsnews.com/stories/2006/05/17/national/printable1624039.shtml</a> .       |
| 8  |           |   |
| 9  | Exhibit X | Transcript of <i>Press Briefing by Tony Snow</i> (May 16, 2006), available at <a href="http://www.whitehouse.gov/news/releases/2006/05/print/2006/20060516-4.html">http://www.whitehouse.gov/news/releases/2006/05/print/2006/20060516-4.html</a> . |
| 10 |           |   |
| 11 | Exhibit Y | John D. Negroponte, <i>Letter from John D. Negroponte to Speaker of the House of Representatives J. Dennis Hastert Regarding Names of Members of Congress Who Attended Briefings on the Terrorist Surveillance Program</i> , May 17, 2006.          |
| 12 |           |   |
| 13 |           |   |
| 14 | Exhibit Z | Transcript of <i>Press Briefing by Tony Snow</i> (May 17, 2006), available at <a href="http://www.whitehouse.gov/news/releases/2006/05/print/2006/20060517-4.html">http://www.whitehouse.gov/news/releases/2006/05/print/2006/20060517-4.html</a> . |
| 15 |           |   |
| 16 |           |   |

17 I declare under penalty of perjury of the laws of the United States that the  
 18 foregoing is true and correct. Executed this 1st day of February, 2007 at Oakland, California.

19 /s Barry Himmelstein  
 20 Barry Himmelstein

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21

**REQUEST FOR JUDICIAL NOTICE**

Pursuant to Rule 201 of the Federal Rules of Evidence, Class Plaintiffs respectfully request that, in support of with their Response to Order to Show Cause Why Rulings On *Hepting* Motions to Dismiss Should Not Apply, filed and served herewith, the Court take judicial notice of the fact that each of the documents listed in the foregoing Declaration of Barry Himmelstein is publicly available, and of its contents. Plaintiffs do not request the Court to take judicial notice that the facts reported in the documents are true, but rather than they are in the public domain.

Under Rule 201(d), courts shall take judicial notice of adjudicative facts if requested by a party and supplied with the necessary information. “A judicially noticed fact must be one not subject to reasonable dispute in that it is either (1) generally known within the territorial jurisdiction of the trial court or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned.” Fed. R. Evid. 201(b).

Each of the documents identified is either a published news article, press release, official correspondence of the Executive Branch, or a transcript of a radio address, press conference, or news broadcast. The publication and contents of these documents are “not subject to reasonable dispute in that . . . [they are] capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned.” Fed. R. Evid. 201(b). Specifically, these facts are easily verifiable by reviewing the documents and confirming sources and dates of the publications and broadcasts.<sup>1</sup>

22  
23  
24  
25  
26  
27  
28

---

<sup>1</sup> See *Heliotrope Gen., Inc. v. Ford Motor Co.*, 189 F.3d 971, 981 n. 18 (9th Cir. 1999) (“We take judicial notice that the market was aware of the information contained in news articles submitted by the defendants”); *Moonrunners L.P. v. Time Warner, Inc.*, 2005 U.S. Dist. LEXIS 41244, at \*34 n.12 (C.D. Cal. June 17, 2005) (“The court may take judicial notice of the fact that an article was published in a newspaper or periodical”); *Benak ex rel. Alliance Premier Growth Fund v. Alliance Capital Mgmt. L.P.*, 435 F.3d 396, 401 n. 15 (3d Cir. 2006) (holding that district court did not err in taking judicial notice of newspaper articles because “[t]hey serve only to indicate what was in the public realm at the time, not whether the contents of those articles were in fact true”); *In re Merrill Lynch & Co. Research Reports Sec. Litig.*, 289 F. Supp. 2d 416, 425 n.15 (S.D.N.Y. 2003) (“The Court may take judicial notice of newspaper articles for the fact of their publication without transforming the motion into one for summary judgment”); *In re Sterling Foster & Co., Sec. Litig.*, 222 F. Supp. 2d 312, 321 (E.D.N.Y. 2002) (taking judicial notice of newspaper articles to show media attention to defendant’s alleged conduct), *vacated and remanded on other grounds by Levitt v. Bear Stearns & Co., Inc.*, 340 F.3d 94 (2d Cir. 2003);

1                   Accordingly, Plaintiffs respectfully request that the Court take judicial notice that  
2 each of the identified documents is publicly available, and of their contents.

3  
4 Dated: February 1, 2007

Respectfully submitted,  
LIEFF, CABRASER, HEIMANN & BERNSTEIN, LLP

5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24

By:   /s/ Barry R. Himmelstein  
Barry R. Himmelstein  
Interim Class Counsel for MCI Class

---

25 *Schwenk v. Kavanaugh*, 4 F. Supp. 2d 116, 118 (N.D.N.Y. 1998) (taking judicial notice of the fact  
26 that a particular article appeared on the front page of the New York Law Journal); *Cerasani v.*  
27 *Sony Corp.*, 991 F. Supp. 343, 354 n.3 (S.D.N.Y. 1998) (taking judicial notice of the widespread  
28 newspaper coverage of the trial); *Cosmas v. Merrill Lynch & Co.*, 1993 U.S. Dist. LEXIS 21323,  
at \*4 n.2, 1993 WL 800778, at \*2 n.2 (S.D.N.Y. Jul. 1, 1993) (taking judicial notice of the fact  
that stock prices were listed in the Wall Street Journal); *Show-World Center, Inc. v. Walsh*, 438 F.  
Supp. 642, 655 (S.D.N.Y. 1977) (taking judicial notice of widespread publicity via newspaper  
and television news).

# **EXHIBIT A**

3 of 3 DOCUMENTS

Copyright 2005 The New York Times Company  
The New York Times

December 16, 2005 Friday  
Correction Appended  
Late Edition - Final

**SECTION:** Section A; Column 1; Foreign Desk; Pg. 1

**LENGTH:** 3633 words

**HEADLINE:** Bush Lets U.S. Spy on Callers Without Courts

**BYLINE:** By JAMES RISEN and ERIC LICHTBLAU; Barclay Walsh contributed research for this article.

**DATELINE:** WASHINGTON, Dec. 15

**BODY:**

Months after the Sept. 11 attacks, 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, according to government officials.

Under a presidential order signed in 2002, the intelligence agency has monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people inside the United States without warrants over the past three years in an effort to track possible "dirty numbers" linked to Al Qaeda, the officials said. The agency, they said, still seeks warrants to monitor entirely domestic communications.

The previously undisclosed decision to permit some eavesdropping inside the country without court approval was a major shift in American intelligence-gathering practices, particularly for the National Security Agency, whose mission is to spy on communications abroad. As a result, some officials familiar with the continuing operation have questioned whether the surveillance has stretched, if not crossed, constitutional limits on legal searches.

"This is really a sea change," said a former senior official who specializes in national security law. "It's almost a mainstay of this country that the N.S.A. only does foreign searches."

Nearly a dozen current and former officials, who were granted anonymity because of the classified nature of the program, discussed it with reporters for The New York Times because of their concerns about the operation's legality and oversight.

According to those officials and others, reservations about aspects of the program have also been expressed by Senator John D. Rockefeller IV, the West Virginia Democrat who is the vice chairman of the Senate Intelligence Committee, and a judge presiding over a secret court that oversees intelligence matters. Some of the questions about the agency's new powers led the administration to temporarily suspend the operation last year and impose more restrictions, the officials said.

The Bush administration views the operation as necessary so that the agency can move quickly to monitor communications that may disclose threats to the United States, the officials said. Defenders of the program say it has been a critical tool in helping disrupt terrorist plots and prevent attacks inside the United States.

Administration officials are confident that existing safeguards are sufficient to protect the privacy and civil liberties of Americans, the officials say. In some cases, they said, the Justice Department eventually seeks warrants if it wants to expand the eavesdropping to include communications confined within the United States. The officials said the



## Bush Lets U.S. Spy on Callers Without Courts The New York Times Decembe

administration had briefed Congressional leaders about the program and notified the judge in charge of the Foreign Intelligence Surveillance Court, the secret Washington court that deals with national security issues.

The White House asked The New York Times not to publish this article, arguing that it could jeopardize continuing investigations and alert would-be terrorists that they might be under scrutiny. After meeting with senior administration officials to hear their concerns, the newspaper delayed publication for a year to conduct additional reporting. Some information that administration officials argued could be useful to terrorists has been omitted.

## Dealing With a New Threat

While many details about the program remain secret, officials familiar with it say the N.S.A. 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. Overseas, about 5,000 to 7,000 people suspected of terrorist ties are monitored at one time, according to those officials.

Several officials said the eavesdropping program had helped uncover a plot by Iyman Faris, an Ohio trucker and naturalized citizen who pleaded guilty in 2003 to supporting Al Qaeda by planning to bring down the Brooklyn Bridge with blowtorches. What appeared to be another Qaeda plot, involving fertilizer bomb attacks on British pubs and train stations, was exposed last year in part through the program, the officials said. But they said most people targeted for N.S.A. monitoring have never been charged with a crime, including an Iranian-American doctor in the South who came under suspicion because of what one official described as dubious ties to Osama bin Laden.

The eavesdropping program grew out of concerns after the Sept. 11 attacks that the nation's intelligence agencies were not poised to deal effectively with the new threat of Al Qaeda and that they were handcuffed by legal and bureaucratic restrictions better suited to peacetime than war, according to officials. In response, President Bush significantly eased limits on American intelligence and law enforcement agencies and the military.

But some of the administration's antiterrorism initiatives have provoked an outcry from members of Congress, watchdog groups, immigrants and others who argue that the measures erode protections for civil liberties and intrude on Americans' privacy.

Opponents have challenged provisions of the USA Patriot Act, the focus of contentious debate on Capitol Hill this week, that expand domestic surveillance by giving the Federal Bureau of Investigation more power to collect information like library lending lists or Internet use. Military and F.B.I. officials have drawn criticism for monitoring what were largely peaceful antiwar protests. The Pentagon and the Department of Homeland Security were forced to retreat on plans to use public and private databases to hunt for possible terrorists. And last year, the Supreme Court rejected the administration's claim that those labeled "enemy combatants" were not entitled to judicial review of their open-ended detention.

Mr. Bush's executive order allowing some warrantless eavesdropping on those inside the United States -- including American citizens, permanent legal residents, tourists and other foreigners -- is based on classified legal opinions that assert that the president has broad powers to order such searches, derived in part from the September 2001 Congressional resolution authorizing him to wage war on Al Qaeda and other terrorist groups, according to the officials familiar with the N.S.A. operation.

The National Security Agency, which is based at Fort Meade, Md., is the nation's largest and most secretive intelligence agency, so intent on remaining out of public view that it has long been nicknamed "No Such Agency." It breaks codes and maintains listening posts around the world to eavesdrop on foreign governments, diplomats and trade negotiators as well as drug lords and terrorists. But the agency ordinarily operates under tight restrictions on any spying on Americans, even if they are overseas, or disseminating information about them.

What the agency calls a "special collection program" began soon after the Sept. 11 attacks, as it looked for new tools to attack terrorism. The program accelerated in early 2002 after the Central Intelligence Agency started capturing top Qaeda operatives overseas, including Abu Zubaydah, who was arrested in Pakistan in March 2002. The C.I.A. seized the terrorists' computers, cellphones and personal phone directories, said the officials familiar with the program. The N.S.A. surveillance was intended to exploit those numbers and addresses as quickly as possible, they said.

Bush Lets U.S. Spy on Callers Without Courts The New York Times Decembe

In addition to eavesdropping on those numbers and reading e-mail messages to and from the Qaeda figures, the N.S.A. began monitoring others linked to them, creating an expanding chain. While most of the numbers and addresses were overseas, hundreds were in the United States, the officials said.

Under the agency's longstanding rules, the N.S.A. can target for interception phone calls or e-mail messages on foreign soil, even if the recipients of those communications are in the United States. Usually, though, the government can only target phones and e-mail messages in the United States by first obtaining a court order from the Foreign Intelligence Surveillance Court, which holds its closed sessions at the Justice Department.

Traditionally, the F.B.I., not the N.S.A., seeks such warrants and conducts most domestic eavesdropping. Until the new program began, the N.S.A. typically limited its domestic surveillance to foreign embassies and missions in Washington, New York and other cities, and obtained court orders to do so.

Since 2002, the agency has been conducting some warrantless eavesdropping on people in the United States who are linked, even if indirectly, to suspected terrorists through the chain of phone numbers and e-mail addresses, according to several officials who know of the operation. Under the special program, the agency monitors their international communications, the officials said. The agency, for example, can target phone calls from someone in New York to someone in Afghanistan.

Warrants are still required for eavesdropping on entirely domestic-to-domestic communications, those officials say, meaning that calls from that New Yorker to someone in California could not be monitored without first going to the Federal Intelligence Surveillance Court.

#### A White House Briefing

After the special program started, Congressional leaders from both political parties were brought to Vice President Dick Cheney's office in the White House. The leaders, who included the chairmen and ranking members of the Senate and House intelligence committees, learned of the N.S.A. operation from Mr. Cheney, Lt. Gen. Michael V. Hayden of the Air Force, who was then the agency's director and is now a full general and the principal deputy director of national intelligence, and George J. Tenet, then the director of the C.I.A., officials said.

It is not clear how much the members of Congress were told about the presidential order and the eavesdropping program. Some of them declined to comment about the matter, while others did not return phone calls.

Later briefings were held for members of Congress as they assumed leadership roles on the intelligence committees, officials familiar with the program said. After a 2003 briefing, Senator Rockefeller, the West Virginia Democrat who became vice chairman of the Senate Intelligence Committee that year, wrote a letter to Mr. Cheney expressing concerns about the program, officials knowledgeable about the letter said. It could not be determined if he received a reply. Mr. Rockefeller declined to comment. Aside from the Congressional leaders, only a small group of people, including several cabinet members and officials at the N.S.A., the C.I.A. and the Justice Department, know of the program.

Some officials familiar with it say they consider warrantless eavesdropping inside the United States to be unlawful and possibly unconstitutional, amounting to an improper search. One government official involved in the operation said he privately complained to a Congressional official about his doubts about the program's legality. But nothing came of his inquiry. "People just looked the other way because they didn't want to know what was going on," he said.

A senior government official recalled that he was taken aback when he first learned of the operation. "My first reaction was, 'We're doing what?'" he said. While he said he eventually felt that adequate safeguards were put in place, he added that questions about the program's legitimacy were understandable.

Some of those who object to the operation argue that is unnecessary. By getting warrants through the foreign intelligence court, the N.S.A. and F.B.I. could eavesdrop on people inside the United States who might be tied to terrorist groups without skirting longstanding rules, they say.

The standard of proof required to obtain a warrant from the Foreign Intelligence Surveillance Court is generally considered lower than that required for a criminal warrant -- intelligence officials only have to show probable cause that someone may be "an agent of a foreign power," which includes international terrorist groups -- and the secret court has turned down only a small number of requests over the years. In 2004, according to the Justice Department, 1,754 war-

Bush Lets U.S. Spy on Callers Without Courts The New York Times Decembe

rants were approved. And the Foreign Intelligence Surveillance Court can grant emergency approval for wiretaps within hours, officials say.

Administration officials counter that they sometimes need to move more urgently, the officials said. Those involved in the program also said that the N.S.A.'s eavesdroppers might need to start monitoring large batches of numbers all at once, and that it would be impractical to seek permission from the Foreign Intelligence Surveillance Court first, according to the officials.

The N.S.A. domestic spying operation has stirred such controversy among some national security officials in part because of the agency's cautious culture and longstanding rules.

Widespread abuses -- including eavesdropping on Vietnam War protesters and civil rights activists -- by American intelligence agencies became public in the 1970's and led to passage of the Foreign Intelligence Surveillance Act, which imposed strict limits on intelligence gathering on American soil. Among other things, the law required search warrants, approved by the secret F.I.S.A. court, for wiretaps in national security cases. The agency, deeply scarred by the scandals, adopted additional rules that all but ended domestic spying on its part.

After the Sept. 11 attacks, though, the United States intelligence community was criticized for being too risk-averse. The National Security Agency was even cited by the independent 9/11 Commission for adhering to self-imposed rules that were stricter than those set by federal law.

#### Concerns and Revisions

Several senior government officials say that when the special operation began, there were few controls on it and little formal oversight outside the N.S.A. The agency can choose its eavesdropping targets and does not have to seek approval from Justice Department or other Bush administration officials. Some agency officials wanted nothing to do with the program, apparently fearful of participating in an illegal operation, a former senior Bush administration official said. Before the 2004 election, the official said, some N.S.A. personnel worried that the program might come under scrutiny by Congressional or criminal investigators if Senator John Kerry, the Democratic nominee, was elected president.

In mid-2004, concerns about the program expressed by national security officials, government lawyers and a judge prompted the Bush administration to suspend elements of the program and revamp it.

For the first time, the Justice Department audited the N.S.A. program, several officials said. And to provide more guidance, the Justice Department and the agency expanded and refined a checklist to follow in deciding whether probable cause existed to start monitoring someone's communications, several officials said.

A complaint from Judge Colleen Kollar-Kotelly, the federal judge who oversees the Federal Intelligence Surveillance Court, helped spur the suspension, officials said. The judge questioned whether information obtained under the N.S.A. program was being improperly used as the basis for F.I.S.A. wiretap warrant requests from the Justice Department, according to senior government officials. While not knowing all the details of the exchange, several government lawyers said there appeared to be concerns that the Justice Department, by trying to shield the existence of the N.S.A. program, was in danger of misleading the court about the origins of the information cited to justify the warrants.

One official familiar with the episode said the judge insisted to Justice Department lawyers at one point that any material gathered under the special N.S.A. program not be used in seeking wiretap warrants from her court. Judge Kollar-Kotelly did not return calls for comment.

A related issue arose in a case in which the F.B.I. was monitoring the communications of a terrorist suspect under a F.I.S.A.-approved warrant, even though the National Security Agency was already conducting warrantless eavesdropping.

According to officials, F.B.I. surveillance of Mr. Faris, the Brooklyn Bridge plotter, was dropped for a short time because of technical problems. At the time, senior Justice Department officials worried what would happen if the N.S.A. picked up information that needed to be presented in court. The government would then either have to disclose the N.S.A. program or mislead a criminal court about how it had gotten the information.

Several national security officials say the powers granted the N.S.A. by President Bush go far beyond the expanded counterterrorism powers granted by Congress under the USA Patriot Act, which is up for renewal. The House

## Bush Lets U.S. Spy on Callers Without Courts The New York Times Decembe

on Wednesday approved a plan to reauthorize crucial parts of the law. But final passage has been delayed under the threat of a Senate filibuster because of concerns from both parties over possible intrusions on Americans' civil liberties and privacy.

Under the act, law enforcement and intelligence officials are still required to seek a F.I.S.A. warrant every time they want to eavesdrop within the United States. A recent agreement reached by Republican leaders and the Bush administration would modify the standard for F.B.I. wiretap warrants, requiring, for instance, a description of a specific target. Critics say the bar would remain too low to prevent abuses.

Bush administration officials argue that the civil liberties concerns are unfounded, and they say pointedly that the Patriot Act has not freed the N.S.A. to target Americans. "Nothing could be further from the truth," wrote John Yoo, a former official in the Justice Department's Office of Legal Counsel, and his co-author in a Wall Street Journal opinion article in December 2003. Mr. Yoo worked on a classified legal opinion on the N.S.A.'s domestic eavesdropping program.

At an April hearing on the Patriot Act renewal, Senator Barbara A. Mikulski, Democrat of Maryland, asked Attorney General Alberto R. Gonzales and Robert S. Mueller III, the director of the F.B.I., "Can the National Security Agency, the great electronic snooper, spy on the American people?"

"Generally," Mr. Mueller said, "I would say generally, they are not allowed to spy or to gather information on American citizens."

President Bush did not ask Congress to include provisions for the N.S.A. domestic surveillance program as part of the Patriot Act and has not sought any other laws to authorize the operation. Bush administration lawyers argued that such new laws were unnecessary, because they believed that the Congressional resolution on the campaign against terrorism provided ample authorization, officials said.

#### The Legal Line Shifts

Seeking Congressional approval was also viewed as politically risky because the proposal would be certain to face intense opposition on civil liberties grounds. The administration also feared that by publicly disclosing the existence of the operation, its usefulness in tracking terrorists would end, officials said.

The legal opinions that support the N.S.A. operation remain classified, but they appear to have followed private discussions among senior administration lawyers and other officials about the need to pursue aggressive strategies that once may have been seen as crossing a legal line, according to senior officials who participated in the discussions.

For example, just days after the Sept. 11, 2001, attacks on New York and the Pentagon, Mr. Yoo, the Justice Department lawyer, wrote an internal memorandum that argued that the government might use "electronic surveillance techniques and equipment that are more powerful and sophisticated than those available to law enforcement agencies in order to intercept telephonic communications and observe the movement of persons but without obtaining warrants for such uses."

Mr. Yoo noted that while such actions could raise constitutional issues, in the face of devastating terrorist attacks "the government may be justified in taking measures which in less troubled conditions could be seen as infringements of individual liberties."

The next year, Justice Department lawyers disclosed their thinking on the issue of warrantless wiretaps in national security cases in a little-noticed brief in an unrelated court case. In that 2002 brief, the government said that "the Constitution vests in the President inherent authority to conduct warrantless intelligence surveillance (electronic or otherwise) of foreign powers or their agents, and Congress cannot by statute extinguish that constitutional authority."

Administration officials were also encouraged by a November 2002 appeals court decision in an unrelated matter. The decision by the Foreign Intelligence Surveillance Court of Review, which sided with the administration in dismantling a bureaucratic "wall" limiting cooperation between prosecutors and intelligence officers, cited "the president's inherent constitutional authority to conduct warrantless foreign intelligence surveillance."

But the same court suggested that national security interests should not be grounds "to jettison the Fourth Amendment requirements" protecting the rights of Americans against undue searches. The dividing line, the court acknowledged, "is a very difficult one to administer."

Bush Lets U.S. Spy on Callers Without Courts The New York Times Decembe

**URL:** <http://www.nytimes.com>

**CORRECTION-DATE:** December 28, 2005

**CORRECTION:**

Because of an editing error, a front-page article on Dec. 16 about a decision by President Bush to authorize the National Security Agency to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without warrants ordinarily required for domestic spying misstated the name of the court that would normally issue those warrants. It is the Foreign -- not Federal -- Intelligence Surveillance Court.

**GRAPHIC:** Photo: In 2002, President Bush toured the National Security Agency at Fort Meade, Md., with Lt. Gen. Michael V. Hayden, who was then the agency's director and is now a full general and the principal deputy director of national intelligence. (Photo by Doug Mills/Associated Press)(pg. A16)Chart: "A Half-Century of Surveillance" **HISTORY** -- Created in 1952, the National Security Agency is the biggest American intelligence agency, with more than 30,000 employees at Fort Meade, Md., and listening posts around the world. Part of the Defense Department, it is the successor to the State Department's "Black Chamber" and American military eavesdropping and code-breaking operations that date to the early days of telegraph and telephone communications. **MISSION** -- The N.S.A. runs the eavesdropping hardware of the American intelligence system, operating a huge network of satellites and listening devices around the world. Traditionally, its mission has been to gather intelligence overseas on foreign enemies by breaking codes and tapping into telephone and computer communications. **SUCSESSES** -- Most of the agency's successes remain secret, but a few have been revealed. The agency listened to Soviet pilots and ground controllers during the shooting down of a civilian South Korean airliner in 1983

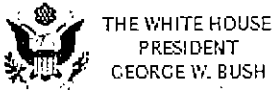
traced a disco bombing in Berlin in 1986 to Libya through diplomatic messages

and, more recently, used the identifying chips in cellphones to track terrorist suspects after the 2001 attacks. **DOMESTIC ACTIVITY** -- The disclosure in the 1970's of widespread surveillance on political dissenters and other civil rights abuses led to restrictions at the N.S.A. and elsewhere on the use of domestic wiretaps. The N.S.A. monitors United Nations delegations and some foreign embassy lines on American soil, but is generally prohibited from listening in on the conversations of anyone inside the country without a special court order. **OFFICIAL RULES** -- Since the reforms of the late 1970's, the N.S.A. has generally been permitted to target the communications of people on American soil only if they are believed to be "agents of a foreign power" -- a foreign nation or international terrorist group -- and a warrant is obtained from the Foreign Intelligence Surveillance Court. **EXPANDED ROLE** -- Months after the terror attacks of Sept. 11, 2001, President Bush signed a secret executive order that relaxed restrictions on domestic spying by the N.S.A., according to officials with knowledge of the order. The order allows the agency to monitor without warrants the international phone calls and e-mail messages of some Americans and others inside the United States.(pg. A16)

**LOAD-DATE:** December 16, 2005

# **EXHIBIT B**





CLICK HERE TO PRINT



For Immediate Release  
Office of the Press Secretary  
December 17, 2005

## President's Radio Address

The Roosevelt Room

- [In Focus: Homeland Security](#)
- [\[en Español\]](#)

10:06 A.M. EST

THE PRESIDENT: Good morning.



**VIDEO** Multimedia

President's Remarks

[view](#)

As President, I took an oath to defend the Constitution, and I have no greater responsibility than to protect our people, our freedom, and our way of life. On September the 11th, 2001, our freedom and way of life came under attack by brutal enemies who killed nearly 3,000 innocent Americans. We're fighting these enemies across the world. Yet in this first war of the 21st century, one of the most critical battlefronts is the home front. And since September the 11th, we've been on the offensive against the terrorists plotting within our borders.

One of the first actions we took to protect America after our nation was attacked was to ask Congress to pass the Patriot Act. The Patriot Act tore down the legal and bureaucratic wall that kept law enforcement and intelligence authorities from sharing vital information about terrorist threats. And the Patriot Act allowed federal investigators to pursue terrorists with tools they already used against other criminals. Congress passed this law with a large, bipartisan majority, including a vote of 98-1 in the United States Senate.



Since then, America's law enforcement personnel have used this critical law to prosecute terrorist operatives and supporters, and to break up terrorist cells in New York, Oregon, Virginia, California, Texas and Ohio. The Patriot Act has accomplished exactly what it was designed to do: it has protected American liberty and saved American lives.

Yet key provisions of this law are set to expire in two weeks. The terrorist threat to our country will not expire in two weeks. The terrorists want to attack America again, and inflict even greater damage than they did on September the 11th. Congress has a responsibility to ensure that law enforcement and intelligence officials have the tools they need to protect the American people.

The House of Representatives passed reauthorization of the Patriot Act. Yet a minority of senators filibustered to block the renewal of the Patriot Act when it came up for a vote yesterday. That decision is irresponsible, and it endangers the lives of our citizens. The senators who are filibustering must stop their delaying tactics, and the Senate must vote to reauthorize the Patriot Act. In the war on terror, we cannot afford to be without this law for a single moment.

To fight the war on terror, I am using authority vested in me by Congress, including the Joint Authorization for Use

of Military Force, which passed overwhelmingly in the first week after September the 11th. I'm also using constitutional authority vested in me as Commander-in-Chief.

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.

This is a highly classified program that is crucial to our national security. Its purpose is to detect and prevent terrorist attacks against the United States, our friends and allies. Yesterday the existence of this secret program was revealed in media reports, after being improperly provided to news organizations. As a result, our enemies have learned information they should not have, and the unauthorized disclosure of this effort damages our national security and puts our citizens at risk. Revealing classified information is illegal, alerts our enemies, and endangers our country.

As the 9/11 Commission pointed out, it was clear that terrorists inside the United States were communicating with terrorists abroad before the September the 11th attacks, and the commission criticized our nation's inability to uncover links between terrorists here at home and terrorists abroad. Two of the terrorist hijackers who flew a jet into the Pentagon, Nawaf al Hamzi and Khalid al Mihdhar, communicated while they were in the United States to other members of al Qaeda who were overseas. But we didn't know they were here, until it was too late.

The authorization I gave the National Security Agency after September the 11th helped address that problem in a way that is fully consistent with my constitutional responsibilities and authorities. The activities I have authorized make it more likely that killers like these 9/11 hijackers will be identified and located in time. And the activities conducted under this authorization have helped detect and prevent possible terrorist attacks in the United States and abroad.

The activities I authorized are reviewed approximately every 45 days. Each review is based on a fresh intelligence assessment of terrorist threats to the continuity of our government and the threat of catastrophic damage to our homeland. During each assessment, previous activities under the authorization are reviewed. The review includes approval by our nation's top legal officials, including the Attorney General and the Counsel to the President. I have reauthorized this program more than 30 times since the September the 11th attacks, and I intend to do so for as long as our nation faces a continuing threat from al Qaeda and related groups.

The NSA's activities under this authorization are thoroughly reviewed by the Justice Department and NSA's top legal officials, including NSA's general counsel and inspector general. Leaders in Congress have been briefed more than a dozen times on this authorization and the activities conducted under it. Intelligence officials involved in this activity also receive extensive training to ensure they perform their duties consistent with the letter and intent of the authorization.

This authorization is a vital tool in our war against the terrorists. It is critical to saving American lives. The American people expect me to do everything in my power under our laws and Constitution to protect them and their civil liberties. And that is exactly what I will continue to do, so long as I'm the President of the United States.

Thank you.

END 10:13 A.M. EST

**Return to this article at:**

<http://www.whitehouse.gov/news/releases/2005/12/20051217.html>

 [CLICK HERE TO PRINT](#)

**ARCHIVES**  
↓ **Radio Address**

- [2006](#)
- [2005](#)
- [2004](#)
- [2003](#)
- [2002](#)
- [2001](#)

↓ **Radio Interviews**

- [2005](#)
- [2004](#)



# **EXHIBIT C**



THE WHITE HOUSE  
PRESIDENT  
GEORGE W. BUSH

 [CLICK HERE TO PRINT](#)

For Immediate Release  
Office of the Press Secretary  
December 19, 2005

**Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden,  
Principal Deputy Director for National Intelligence**  
James S. Brady Briefing Room

8:30 A.M. EST

MR. McCLELLAN: Good morning, everybody. I've got with me the Attorney General and General Hayden here this morning to brief you on the legal issues surrounding the NSA authorization and take whatever questions you have for them on that. The Attorney General will open with some comments and then they'll be glad to take your questions.

And with that, I'll turn it over to General Gonzales.

ATTORNEY GENERAL GONZALES: Thanks, Scott.

The President confirmed the existence of a highly classified program on Saturday. The program remains highly classified; there are many operational aspects of the program that have still not been disclosed and we want to protect that because those aspects of the program are very, very important to protect the national security of this country. So I'm only going to be talking about the legal underpinnings for what has been disclosed by the President.

The President has authorized a program to engage in electronic surveillance of a particular kind, and this would be the intercepts of contents of communications where one of the -- one party to the communication is outside the United States. And this is a very important point -- people are running around saying that the United States is somehow spying on American citizens calling their neighbors. Very, very important to understand that one party to the communication has to be outside the United States.

Another very important point to remember is that we have to have a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda. We view these authorities as authorities to confront the enemy in which the United States is at war with -- and that is al Qaeda and those who are supporting or affiliated with al Qaeda.

What we're trying to do is learn of communications, back and forth, from within the United States to overseas with members of al Qaeda. And that's what this program is about.

Now, in terms of legal authorities, the Foreign Intelligence Surveillance Act provides -- requires a court order before engaging in this kind of surveillance that I've just discussed and the President announced on Saturday, unless there is somehow -- there is -- unless otherwise authorized by statute or by Congress. That's what the law requires. Our position is, is that the authorization to use force, which was passed by the Congress in the days following September 11th, constitutes that other authorization, that other statute by Congress, to engage in this kind of signals intelligence.

Now, that -- one might argue, now, wait a minute, there's nothing in the authorization to use force that specifically mentions electronic surveillance. Let me take you back to a case that the Supreme Court reviewed this past -- in 2004, the Hamdi decision. As you remember, in that case, Mr. Hamdi was a U.S. citizen who was contesting his detention by the United States government. What he said was that there is a statute, he said, that specifically prohibits the detention of American citizens without permission, an act by Congress -- and he's right, 18 USC 4001a requires that the United States government cannot detain an American citizen except by an act of

Congress.

We took the position -- the United States government took the position that Congress had authorized that detention in the authorization to use force, even though the authorization to use force never mentions the word "detention." And the Supreme Court, a plurality written by Justice O'Connor agreed. She said, it was clear and unmistakable that the Congress had authorized the detention of an American citizen captured on the battlefield as an enemy combatant for the remainder -- the duration of the hostilities. So even though the authorization to use force did not mention the word, "detention," she felt that detention of enemy soldiers captured on the battlefield was a fundamental incident of waging war, and therefore, had been authorized by Congress when they used the words, "authorize the President to use all necessary and appropriate force."

For the same reason, we believe signals intelligence is even more a fundamental incident of war, and we believe has been authorized by the Congress. And even though signals intelligence is not mentioned in the authorization to use force, we believe that the Court would apply the same reasoning to recognize the authorization by Congress to engage in this kind of electronic surveillance.

I might also add that we also believe the President has the inherent authority under the Constitution, as Commander-in-Chief, to engage in this kind of activity. Signals intelligence has been a fundamental aspect of waging war since the Civil War, where we intercepted telegraphs, obviously, during the world wars, as we intercepted telegrams in and out of the United States. Signals intelligence is very important for the United States government to know what the enemy is doing, to know what the enemy is about to do. It is a fundamental incident of war, as Justice O'Connor talked about in the Hamdi decision. We believe that -- and those two authorities exist to allow, permit the United States government to engage in this kind of surveillance.

The President, of course, is very concerned about the protection of civil liberties, and that's why we've got strict parameters, strict guidelines in place out at NSA to ensure that the program is operating in a way that is consistent with the President's directives. And, again, the authorization by the President is only to engage in surveillance of communications where one party is outside the United States, and where we have a reasonable basis to conclude that one of the parties of the communication is either a member of al Qaeda or affiliated with al Qaeda.

Mike, do you want to -- have anything to add?

GENERAL HAYDEN: I'd just add, in terms of what we do globally with regard to signals intelligence, which is a critical part of defending the nation, there are probably no communications more important to what it is we're trying to do to defend the nation; no communication is more important for that purpose than those communications that involve al Qaeda, and one end of which is inside the homeland, one end of which is inside the United States. Our purpose here is to detect and prevent attacks. And the program in this regard has been successful.

Q General, are you able to say how many Americans were caught in this surveillance?

ATTORNEY GENERAL GONZALES: I'm not -- I can't get into the specific numbers because that information remains classified. Again, this is not a situation where -- of domestic spying. To the extent that there is a moderate and heavy communication involving an American citizen, it would be a communication where the other end of the call is outside the United States and where we believe that either the American citizen or the person outside the United States is somehow affiliated with al Qaeda.

Q General, can you tell us why you don't choose to go to the FISA court?

ATTORNEY GENERAL GONZALES: Well, we continue to go to the FISA court and obtain orders. It is a very important tool that we continue to utilize. Our position is that we are not legally required to do, in this particular case, because the law requires that we -- FISA requires that we get a court order, unless authorized by a statute, and we believe that authorization has occurred.

The operators out at NSA tell me that we don't have the speed and the agility that we need, in all circumstances, to deal with this new kind of enemy. You have to remember that FISA was passed by the Congress in 1978. There have been tremendous advances in technology --

Q But it's been kind of retroactively, hasn't it?

ATTORNEY GENERAL GONZALES: -- since then. Pardon me?

Q It's been done retroactively before, hasn't it?

ATTORNEY GENERAL GONZALES: What do you mean, "retroactively"?

Q You just go ahead and then you apply for the FISA clearance, because it's damn near automatic.

ATTORNEY GENERAL GONZALES: If we -- but there are standards that have to be met, obviously, and you're right, there is a procedure where we -- an emergency procedure that allows us to make a decision to authorize -- to utilize FISA, and then we go to the court and get confirmation of that authority.

But, again, FISA is very important in the war on terror, but it doesn't provide the speed and the agility that we need in all circumstances to deal with this new kind of threat.

Q But what -- go ahead.

GENERAL HAYDEN: Let me just add to the response to the last question. As the Attorney General says, FISA is very important, we make full use of FISA. But if you picture what FISA was designed to do, FISA is designed to handle the needs in the nation in two broad categories: there's a law enforcement aspect of it; and the other aspect is the continued collection of foreign intelligence. I don't think anyone could claim that FISA was envisaged as a tool to cover armed enemy combatants in preparation for attacks inside the United States. And that's what this authorization under the President is designed to help us do.

Q Have you identified armed enemy combatants, through this program, in the United States?

GENERAL HAYDEN: This program has been successful in detecting and preventing attacks inside the United States.

Q General Hayden, I know you're not going to talk about specifics about that, and you say it's been successful. But would it have been as successful -- can you unequivocally say that something has been stopped or there was an imminent attack or you got information through this that you could not have gotten through going to the court?

GENERAL HAYDEN: I can say unequivocally, all right, that we have got information through this program that would not otherwise have been available.

Q Through the court? Because of the speed that you got it?

GENERAL HAYDEN: Yes, because of the speed, because of the procedures, because of the processes and requirements set up in the FISA process, I can say unequivocally that we have used this program in lieu of that and this program has been successful.

Q But one of the things that concerns people is the slippery slope. If you said you absolutely need this program, you have to do it quickly -- then if you have someone you suspect being a member of al Qaeda, and they're in the United States, and there is a phone call between two people in the United States, why not use that, then, if it's so important? Why not go that route? Why not go further?

GENERAL HAYDEN: Across the board, there is a judgment that we all have to make -- and I made this speech a day or two after 9/11 to the NSA workforce -- I said, free peoples always have to judge where they want to be on that spectrum between security and liberty; that there will be great pressures on us after those attacks to move our national banner down in the direction of security. What I said to the NSA workforce is, our job is to keep Americans free by making Americans feel safe again. That's been the mission of the National Security Agency since the day after the attack, is when I talked -- two days after the attack is when I said that to the workforce.

There's always a balancing between security and liberty. We understand that this is a more -- I'll use the word "aggressive" program than would be traditionally available under FISA. It is also less intrusive. It deals only with international calls. It is generally for far shorter periods of time. And it is not designed to collect reams of intelligence, but to detect and warn and prevent about attacks. And, therefore, that's where we've decided to draw that balance between security and liberty.

Q Gentlemen, can you say when Congress was first briefed, who was included in that, and will there be a leaks investigation?

ATTORNEY GENERAL GONZALES: Well of course, we're not going to -- we don't talk about -- we try not to talk about investigations. As to whether or not there will be a leak investigation, as the President indicated, this is really hurting national security, this has really hurt our country, and we are concerned that a very valuable tool has been compromised. As to whether or not there will be a leak investigation, we'll just have to wait and see.

And your first question was?

Q When was Congress first briefed --

ATTORNEY GENERAL GONZALES: I'm not going to -- I'm not going to talk about -- I'll let others talk about when Congress was first briefed. What I can say is, as the President indicated on Saturday, there have been numerous briefings with certain key members of Congress. Obviously, some members have come out since the revelations on Saturday, saying that they hadn't been briefed. This is a very classified program. It is probably the most classified program that exists in the United States government, because the tools are so valuable, and therefore, decisions were made to brief only key members of Congress. We have begun the process now of reaching out to other members of Congress. I met last night, for example, with Chairman Specter and other members of Congress to talk about the legal aspects of this program.

And so we are engaged in a dialogue now to talk with Congress, but also -- but we're still mindful of the fact that still -- this is still a very highly classified program, and there are still limits about what we can say today, even to certain members of Congress.

Q General, what's really compromised by the public knowledge of this program? Don't you assume that the other side thinks we're listening to them? I mean, come on.

GENERAL HAYDEN: The fact that this program has been successful is proof to me that what you claim to be an assumption is certainly not universal. The more we discuss it, the more we put it in the face of those who would do us harm, the more they will respond to this and protect their communications and make it more difficult for us to defend the nation.

Q Mr. Attorney General --

Q -- became public, have you seen any evidence in a change in the tactics or --

ATTORNEY GENERAL GONZALES: We're not going to comment on that kind of operational aspect.

Q You say this has really hurt the American people. Is that based only on your feeling about it, or is there some empirical evidence to back that up, even if you can't --

ATTORNEY GENERAL GONZALES: I think the existence of this program, the confirmation of the -- I mean, the fact that this program exists, in my judgment, has compromised national security, as the President indicated on Saturday.

Q I'd like to ask you, what are the constitutional limits on this power that you see laid out in the statute and in your inherent constitutional war power? And what's to prevent you from just listening to everyone's conversation and trying to find the word "bomb," or something like that?

ATTORNEY GENERAL GONZALES: Well, that's a good question. This was a question that was raised in some of

my discussions last night with members of Congress. The President has not authorized -- has not authorized blanket surveillance of communications here in the United States. He's been very clear about the kind of surveillance that we're going to engage in. And that surveillance is tied with our conflict with al Qaeda.

You know, we feel comfortable that this surveillance is consistent with requirements of the 4th Amendment. The touchstone of the 4th Amendment is reasonableness, and the Supreme Court has long held that there are exceptions to the warrant requirement in -- when special needs outside the law enforcement arena. And we think that that standard has been met here. When you're talking about communications involving al Qaeda, when you -- obviously there are significant privacy interests implicated here, but we think that those privacy interests have been addressed; when you think about the fact that this is an authorization that's ongoing, it's not a permanent authorization, it has to be reevaluated from time to time. There are additional safeguards that have been in place -- that have been imposed out at NSA, and we believe that it is a reasonable application of these authorities.

Q Mr. Attorney General, haven't you stretched --

Q -- adequate because of technological advances? Wouldn't you do the country a better service to address that issue and fix it, instead of doing a backdoor approach --

ATTORNEY GENERAL GONZALES: This is not a backdoor approach. We believe Congress has authorized this kind of surveillance. We have had discussions with Congress in the past -- certain members of Congress -- as to whether or not FISA could be amended to allow us to adequately deal with this kind of threat, and we were advised that that would be difficult, if not impossible.

Q If this is not backdoor, is this at least a judgment call? Can you see why other people would look at it and say, well, no, we don't see it that way?

ATTORNEY GENERAL GONZALES: I think some of the concern is because people had not been briefed; they don't understand the specifics of the program, they don't understand the strict safeguards within the program. And I haven't had a discussion -- an opportunity to have a discussion with them about our legal analysis. So, obviously, we're in that process now. Part of the reason for this press brief today is to have you help us educate the American people and the American Congress about what we're doing and the legal basis for what we're doing.

Q Al, you talk about the successes and the critical intercepts of the program. Have there also been cases in which after listening in or intercepting, you realize you had the wrong guy and you listened to what you shouldn't have?

GENERAL HAYDEN: That's why I mentioned earlier that the program is less intrusive. It deals only with international calls. The time period in which we would conduct our work is much shorter, in general, overall, than it would be under FISA. And one of the true purposes of this is to be very agile, as you described.

If this particular line of logic, this reasoning that took us to this place proves to be inaccurate, we move off of it right away.

Q Are there cases in which --

GENERAL HAYDEN: Yes, of course.

Q Can you give us some idea of percentage, or how often you get it right and how often you get it wrong?

GENERAL HAYDEN: No, it would be very -- no, I cannot, without getting into the operational details. I'm sorry.

Q But there are cases where you wind up listening in where you realize you shouldn't have?

GENERAL HAYDEN: There are cases like we do with regard to the global SIGIN system -- you have reasons to go after particular activities, particular communications. There's a logic; there is a standard as to why you would go after that, not just in a legal sense, which is very powerful, but in a practical sense. We can't waste resources on targets that simply don't provide valuable information. And when we decide that is the case -- and in this



program, the standards, in terms of re-evaluating whether or not this coverage is worthwhile at all, are measured in days and weeks.

Q Would someone in a case in which you got it wrong have a cause of action against the government?

ATTORNEY GENERAL GONZALES: That is something I'm not going to answer, Ken.

Q I wanted to ask you a question. Do you think the government has the right to break the law?

ATTORNEY GENERAL GONZALES: Absolutely not. I don't believe anyone is above the law.

Q You have stretched this resolution for war into giving you carte blanche to do anything you want to do.

ATTORNEY GENERAL GONZALES: Well, one might make that same argument in connection with detention of American citizens, which is far more intrusive than listening into a conversation. There may be some members of Congress who might say, we never --

Q That's your interpretation. That isn't Congress' interpretation.

ATTORNEY GENERAL GONZALES: Well, I'm just giving you the analysis --

Q You're never supposed to spy on Americans.

ATTORNEY GENERAL GONZALES: I'm just giving the analysis used by Justice O'Connor -- and she said clearly and unmistakably the Congress authorized the President of the United States to detain an American citizen, even though the authorization to use force never mentions the word "detention" --

Q -- into wiretapping everybody and listening in on --

ATTORNEY GENERAL GONZALES: This is not about wiretapping everyone. This is a very concentrated, very limited program focused at gaining information about our enemy.

Q Now that the cat is out of the bag, so to speak, do you expect your legal analysis to be tested in the courts?

ATTORNEY GENERAL GONZALES: I'm not going to, you know, try to guess as to what's going to happen about that. We're going to continue to try to educate the American people and the American Congress about what we're doing and the basis -- why we believe that the President has the authority to engage in this kind of conduct.

Q Because there are some very smart legal minds who clearly think a law has been broken here.

ATTORNEY GENERAL GONZALES: Well, I think that they may be making or offering up those opinions or assumptions based on very limited information. They don't have all the information about the program. I think they probably don't have the information about our legal analysis.

Q Judge Gonzales, will you release then, for the reasons you're saying now, the declassified versions of the legal rationale for this from OLC? And if not, why not? To assure the American public that this was done with the legal authority that you state.

ATTORNEY GENERAL GONZALES: We're engaged now in a process of educating the American people, again, and educating the Congress. We'll make the appropriate evaluation at the appropriate time as to whether or not additional information needs to be provided to the Congress or the American people.

Q You declassified OLC opinions before, after the torture -- why not do that here to show, yes, we went through a process?

ATTORNEY GENERAL GONZALES: I'm not confirming the existence of opinions or the non-existence of opinions. I've offered up today our legal analysis of the authorities of this President.

Q Sir, can you explain, please, the specific inadequacies in FISA that have prevented you from sort of going through the normal channels?

GENERAL HAYDEN: One, the whole key here is agility. And let me re-trace some grounds I tried to suggest earlier. FISA was built for persistence. FISA was built for long-term coverage against known agents of an enemy power. And the purpose involved in each of those -- in those cases was either for a long-term law enforcement purpose or a long-term intelligence purpose.

This program isn't for that. This is to detect and prevent. And here the key is not so much persistence as it is agility. It's a quicker trigger. It's a subtly softer trigger. And the intrusion into privacy -- the intrusion into privacy is significantly less. It's only international calls. The period of time in which we do this is, in most cases, far less than that which would be gained by getting a court order. And our purpose here, our sole purpose is to detect and prevent.

Again, I make the point, what we are talking about here are communications we have every reason to believe are al Qaeda communications, one end of which is in the United States. And I don't think any of us would want any inefficiencies in our coverage of those kinds of communications, above all. And that's what this program allows us to do -- it allows us to be as agile as operationally required to cover these targets.

Q But how does FISA --

GENERAL HAYDEN: FISA involves the process -- FISA involves marshaling arguments; FISA involves looping paperwork around, even in the case of emergency authorizations from the Attorney General. And beyond that, it's a little -- it's difficult for me to get into further discussions as to why this is more optimized under this process without, frankly, revealing too much about what it is we do and why and how we do it.

Q If FISA didn't work, why didn't you seek a new statute that allowed something like this legally?

ATTORNEY GENERAL GONZALES: That question was asked earlier. We've had discussions with members of Congress, certain members of Congress, about whether or not we could get an amendment to FISA, and we were advised that that was not likely to be -- that was not something we could likely get, certainly not without jeopardizing the existence of the program, and therefore, killing the program. And that -- and so a decision was made that because we felt that the authorities were there, that we should continue moving forward with this program.

Q And who determined that these targets were al Qaeda? Did you wiretap them?

GENERAL HAYDEN: The 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 created the operational imperative to cover any target, but particularly with regard to those inside the United States.

Q So a shift supervisor is now making decisions that a FISA judge would normally make? I just want to make sure I understand. Is that what you're saying?

GENERAL HAYDEN: What we're trying to do is to use the approach we have used globally against al Qaeda, the operational necessity to cover targets. And the reason I emphasize that this is done at the operational level is to remove any question in your mind that this is in any way politically influenced. This is done to chase those who would do harm to the United States.

Q Building on that, during --

Q Thank you, General. Roughly when did those conversations occur with members of Congress?



ATTORNEY GENERAL GONZALEZ: I'm not going to get into the specifics of when those conversations occurred, but they have occurred.

Q May I just ask you if they were recently or if they were when you began making these exceptions?

ATTORNEY GENERAL GONZALEZ: They weren't recently.

MR. McCLELLAN: The President indicated that those -- the weeks after September 11th.

Q What was the date, though, of the first executive order? Can you give us that?

GENERAL HAYDEN: If I could just, before you ask that question, just add -- these actions that I described taking place at the operational level -- and I believe that a very important point to be made -- have intense oversight by the NSA Inspector General, by the NSA General Counsel, and by officials of the Justice Department who routinely look into this process and verify that the standards set out by the President are being followed.

Q Can you absolutely assure us that all of the communications intercepted --

Q Have you said that you -- (inaudible) -- anything about this program with your international partners -- with the partners probably in the territories of which you intercept those communications?

ATTORNEY GENERAL GONZALEZ: I'm not aware of discussions with other countries, but that doesn't mean that they haven't occurred. I simply have no personal knowledge of that.

Q Also, is it only al Qaeda, or maybe some other terrorist groups?

ATTORNEY GENERAL GONZALEZ: Again, with respect to what the President discussed on Saturday, this program -- it is tied to communications where we believe one of the parties is affiliated with al Qaeda or part of an organization or group that is supportive of al Qaeda.

Q Sir, during his confirmation hearings, it came out that now-Ambassador Bolton had sought and obtained NSA intercepts of conversations between American citizens and others. Who gets the information from this program; how do you guarantee that it doesn't get too widely spread inside the government, and used for other purposes?

Q And is it destroyed afterwards?

GENERAL HAYDEN: We report this information the way we report any other information collected by the National Security Agency. And the phrase you're talking about is called minimization of U.S. identities. The same minimalization standards apply across the board, including for this program. To make this very clear -- U.S. identities are minimized in all of NSA's activities, unless, of course, the U.S. identity is essential to understand the inherent intelligence value of the intelligence report. And that's the standard that's used.

Q General, when you discussed the emergency powers, you said, agility is critical here. And in the case of the emergency powers, as I understand it, you can go in, do whatever you need to do, and within 72 hours just report it after the fact. And as you say, these may not even last very long at all. What would be the difficulty in setting up a paperwork system in which the logs that you say you have the shift supervisors record are simply sent to a judge after the fact? If the judge says that this is not legitimate, by that time probably your intercept is over, wouldn't that be correct?

GENERAL HAYDEN: What you're talking about now are efficiencies. What you're asking me is, can we do this program as efficiently using the one avenue provided to us by the FISA Act, as opposed to the avenue provided to us by subsequent legislation and the President's authorization.

Our operational judgment, given the threat to the nation that the difference in the operational efficiencies between those two sets of authorities are such that we can provide greater protection for the nation operating under this authorization.

Q But while you're getting an additional efficiency, you're also operating outside of an existing law. If the law would allow you to stay within the law and be slightly less efficient, would that be --

ATTORNEY GENERAL GONZALEZ: I guess I disagree with that characterization. I think that this electronic surveillance is within the law, has been authorized. I mean, that is our position. We're only required to achieve a court order through FISA if we don't have authorization otherwise by the Congress, and we think that that has occurred in this particular case.

Q Can you just give us one assurance before you go, General?

ATTORNEY GENERAL GONZALEZ: It depends on what it is. (Laughter.)

Q Can you assure us that all of these intercepts had an international component and that at no time were any of the intercepts purely domestic?

GENERAL HAYDEN: The authorization given to NSA by the President requires that one end of these communications has to be outside the United States. I can assure you, by the physics of the intercept, by how we actually conduct our activities, that one end of these communications are always outside the United States of America.

END 9:02 A.M. EST

---

**Return to this article at:**

<http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html>

 [CLICK HERE TO PRINT](#)

# **EXHIBIT D**

December 24, 2005

## Spy Agency Mined Vast Data Trove, Officials Report

By ERIC LICHTBLAU and JAMES RISEN

WASHINGTON, Dec. 23 - The National Security Agency has traced and analyzed large volumes of telephone and Internet communications flowing into and out of the United States as part of the eavesdropping program that President Bush approved after the Sept. 11, 2001, attacks to hunt for evidence of terrorist activity, according to current and former government officials.

The volume of information harvested from telecommunication data and voice networks, without court-approved warrants, is much larger than the White House has acknowledged, the officials said. It was collected by tapping directly into some of the American telecommunication system's main arteries, they said.

As part of the program approved by President Bush for domestic surveillance without warrants, the N.S.A. has gained the cooperation of American telecommunications companies to obtain backdoor access to streams of domestic and international communications, the officials said.

The government's collection and analysis of phone and Internet traffic have raised questions among some law enforcement and judicial officials familiar with the program. One issue of concern to the Foreign Intelligence Surveillance Court, which has reviewed some separate warrant applications growing out of the N.S.A.'s surveillance program, is whether the court has legal authority over calls outside the United States that happen to pass through American-based telephonic "switches," according to officials familiar with the matter.

"There was a lot of discussion about the switches" in conversations with the court, a Justice Department official said, referring to the gateways through which much of the communications traffic flows. "You're talking about access to such a vast amount of communications, and the question was, How do you minimize something that's on a switch that's carrying such large volumes of traffic? The court was very, very concerned about that."

Since the disclosure last week of the N.S.A.'s domestic surveillance program, President Bush and his senior aides have stressed that his executive order allowing eavesdropping without warrants was limited to the monitoring of international phone and e-mail communications involving people with known links to Al Qaeda.

What has not been publicly acknowledged is that N.S.A. technicians, besides actually eavesdropping on specific conversations, have combed through large volumes of phone and Internet traffic in search of patterns that might point to terrorism suspects. Some officials describe the program as a large data-mining operation.

The current and former government officials who discussed the program were granted anonymity because it remains classified.

Bush administration officials declined to comment on Friday on the technical aspects of the operation and the N.S.A.'s use of broad searches to look for clues on terrorists. Because the program is highly classified, many details of how the N.S.A. is conducting it remain unknown, and members of Congress who have pressed for a full Congressional inquiry say they are eager to learn more about the program's operational details, as well as its legality.

Officials in the government and the telecommunications industry who have knowledge of parts of the program say the N.S.A. has sought to analyze communications patterns to glean clues from details like who is calling whom, how long a phone call lasts and what time of day it is made, and the origins and destinations of phone calls and e-mail messages. Calls to and from Afghanistan, for instance, are known to have been of particular interest to the N.S.A. since the Sept. 11 attacks, the officials said.

This so-called "pattern analysis" on calls within the United States would, in many circumstances, require a court warrant if the government wanted to trace who calls whom.

The use of similar data-mining operations by the Bush administration in other contexts has raised strong objections, most notably in connection with the Total Information Awareness system, developed by the Pentagon for tracking terror suspects, and the Department of Homeland Security's Capps program for screening airline passengers. Both programs were ultimately scrapped after public outcries over possible threats to privacy and civil liberties.

But the Bush administration regards the N.S.A.'s ability to trace and analyze large volumes of data as critical to its expanded mission to detect terrorist plots before they can be carried out, officials familiar with the program say. Administration officials maintain that the system set up by Congress in 1978 under the Foreign Intelligence Surveillance Act does not give them the speed and flexibility to respond fully to terrorist threats at home.

A former technology manager at a major telecommunications company said that since the Sept. 11 attacks, the leading companies in the industry have been storing information on calling patterns and giving it to the federal government to aid in tracking possible terrorists.

"All that data is mined with the cooperation of the government and shared with them, and since 9/11, there's been much more active involvement in that area," said the former manager, a telecommunications expert who did not want his name or that of his former company used because of concern about revealing trade secrets.

Such information often proves just as valuable to the government as eavesdropping on the calls themselves, the former manager said.

"If they get content, that's useful to them too, but the real plum is going to be the transaction data and the traffic analysis," he said. "Massive amounts of traffic analysis information - who is calling whom, who is in Osama Bin Laden's circle of family and friends - is used to identify lines of communication that are then given closer scrutiny."

Several officials said that after President Bush's order authorizing the N.S.A. program, senior government officials arranged with officials of some of the nation's largest telecommunications companies to gain access to switches that act as gateways at the borders between the United States' communications networks and international networks. The identities of the corporations involved could not be determined.

The switches are some of the main arteries for moving voice and some Internet traffic into and out of the United States, and, with the globalization of the telecommunications industry in recent years, many international-to-international calls are also routed through such American switches.

One outside expert on communications privacy who previously worked at the N.S.A. said that to exploit its technological capabilities, the American government had in the last few years been quietly encouraging the telecommunications industry to increase the amount of international traffic that is routed through American-based switches.

The growth of that transit traffic had become a major issue for the intelligence community, officials say, because it had not been fully addressed by 1970's-era laws and regulations governing the N.S.A. Now that foreign calls were being routed through switches on American soil, some judges and law enforcement officials regarded eavesdropping on those calls as a possible violation of those decades-old restrictions, including the Foreign Intelligence Surveillance Act, which requires court-approved warrants for domestic surveillance.

Historically, the American intelligence community has had close relationships with many communications and computer firms and related technical industries. But the N.S.A.'s backdoor access to major telecommunications switches on American soil with the cooperation of major corporations represents a significant expansion of the agency's operational capability, according to current and former government officials.

Phil Karn, a computer engineer and technology expert at a major West Coast telecommunications company, said access to such switches would be significant. "If the government is gaining access to the switches like this, what you're really talking about is the capability of an enormous vacuum operation to sweep up data," he said.

# **EXHIBIT E**



# Slate

## TAKING PUBLIC RADIO TO ANOTHER LEVEL



politics

### Tinker, Tailor, Miner, Spy

Why the NSA's snooping is unprecedented in scale and scope.

By Shane Harris and Tim Naftali

Posted Tuesday, Jan. 3, 2006, at 6:30 AM ET

Fifty years ago, officers from the Signal Security Agency, the predecessor to the National Security Agency, visited an executive from International Telephone and Telegraph and asked for copies of all foreign government cables carried by the company. The request was a direct violation of a 1934 law that banned the interception of domestic communications, but Attorney General Tom Clark backed it. Initially reluctant, ITT relented when told that its competitor, Western Union, had already agreed to supply this information. As James Bamford relates in his book *The Puzzle Palace*, the government told ITT it "would not desire to be the only non-cooperative company on the project." Codenamed Shamrock, the effort to collect cables sent through U.S.-controlled telegraph lines ultimately involved all the American telecom giants of the era, captured private as well as government cables, and lasted nearly 30 years. Like other illegal Cold War domestic snooping programs—such as the FBI's wiretaps without warrants and the CIA's mail-opening operations—it collapsed under the weight of public reaction to the abuses of executive power revealed by Vietnam and Watergate.

Today's generation of telecom leaders is similarly involved in the current controversy over spying by the NSA. The *New York Times* reported in December that since 9/11, leading telecommunications companies "have been storing information on calling patterns and giving it to the federal government to aid in tracking possible terrorists." Citing current and former government and corporate officials, the *Times* reported that the companies have granted the NSA access to their all-important switches, the hubs through which colossal volumes of voice calls and data transmissions move every second. A former telecom executive told us that efforts to obtain call details go back to early 2001, predating the 9/11 attacks and the president's now celebrated secret executive order. The source, who asked not to be identified so as not to out his former company, reports that the NSA approached U.S. carriers and asked for their cooperation in a "data-mining" operation, which might eventually cull "millions" of individual calls and e-mails.

Like the pressure applied to ITT a half-century ago, our source says the government was insistent, arguing that his competitors had already shown their patriotism by signing on. The NSA would not comment on the issue, saying that, "We do not discuss details of actual or alleged operational issues."

The magnitude of the current collection effort is unprecedented and indeed marks a shift in how the NSA spies in the United States. The current program seems to involve a remarkable level of cooperation with private companies and extraordinarily expansive data-mining of questionable legality. Before Bush authorized the NSA to expand its domestic snooping program after 9/11 in the secret executive order, the agency had to stay clear of the "protected communications" of American citizens or resident aliens unless supplied by a judge with a warrant. The program President Bush authorized reportedly allows the NSA to mine huge sets of domestic data for suspicious patterns, regardless of whether the source of the data is an American citizen or resident. The NSA needs the help of private companies to do this because commercial broadband now carries so many communications. In an earlier age, the NSA could pick up the bulk of what it needed by tapping into satellite or microwave transmissions. "Now," as the agency noted in a transition document prepared for the incoming Bush administration in December 2000, "communications are mostly digital, carry billions of bits of data, and contain voice, data and



multimedia. They are dynamically routed, globally networked and pass over traditional communications means such as microwave or satellite less and less."

The agency used to search the transmissions it monitors for key words, such as names and phone numbers, which are supplied by other intelligence agencies that want to track certain individuals. But now the NSA appears to be vacuuming up all data, generally without a particular phone line, name, or e-mail address as a target. Reportedly, the agency is analyzing the length of a call, the time it was placed, and the origin and destination of electronic transmissions. Those details would be crucial in mining the data for patterns—according to the officials the *Times* cited, the goal of the NSA's eavesdropping system.

Pattern-based searches are most useful when run against huge sets of data. Many calls and messages must be analyzed to determine which ones are benign and which deserve more attention. With large data sets, pattern-based searching can create more nuanced pictures of the connections among people, places, and messages. Deputy Director of National Intelligence Michael Hayden, who until this year was the NSA director, recently hinted that the NSA's eavesdropping program is not just looking for transmissions from specific individuals. It has a "subtly softer trigger" that initiates monitoring without exactly knowing in advance what specific transmissions to look for. Presumably, this trigger is a suspicious pattern. But officials have not actually described any triggers, raising the question of whether the NSA has been authorized to go on such fishing expeditions.

The government experimented with large-scale pattern-based searches under the auspices of the Defense Department's Total Information Awareness program in 2002. The aim was to sift through government intelligence data, and also privately held information, for telltale signs of the planning of a terrorist attack. TIA was ridiculed as Orwellian. But at least the program tried to create new technologies to protect personal information. Adm. John Poindexter, TIA's creator, believed in the potential intelligence benefits of data-mining broadband communications, but he was also well aware of the potential for excess. "We need a much more systematic approach" to data-mining and privacy protection, Poindexter said at a 2002 conference in Anaheim, Calif., sponsored by the Defense Advanced Research Projects Agency.

Poindexter envisioned a "privacy appliance," a device that would strip any identifiers from the information—such as names or addresses—so that government miners could see only patterns. Then if there was reason to believe that the information belonged to a group that was planning an attack, the government could seek a warrant and disable the privacy control for that specific data. TIA funded research on a privacy appliance at the Palo Alto Research Center, a subsidiary of Xerox Corp. "The idea is that this device, cryptographically protected to prevent tampering, would ensure that no one could abuse private information without an immutable digital record of their misdeeds," according to a 2003 government report to Congress about TIA. "The details of the operation of the appliance would be available to the public."

The NSA's domestic eavesdropping program, however, appears to have none of these safeguards. When Congress killed TIA's funding in 2003, it effectively ended research into privacy-protection technology. According to former officials associated with TIA, after the program was canceled, elements of it were transferred into the classified intelligence budget. But these did not include research on privacy protection.

In January, Congress plans to hold hearings into the legality of the Bush administration's eavesdropping program. Lawmakers will want to know why, if the NSA cannot do its job while remaining within the legal bounds established in the 1970s, the Bush administration did not address that problem in the context of the Patriot Act. Congress might also ask why in the rush to begin data-mining, the NSA has

abandoned the privacy controls planned for the TIA. As Adm. Poindexter himself noted in his resignation letter from the program in 2003, "it would be no good to solve the security problem and give up the privacy and civil liberties that make our country great."

*Shane Harris, a staff correspondent for National Journal, writes on intelligence and homeland security. Tim Naftali, the director of the Presidential Recordings Program at the University of Virginia's Miller Center of Public Affairs, is the author of Blind Spot: The Secret History of American Counterterrorism.*

Article URL: <http://www.slate.com/id/2133564/>

---

Copyright 2006 Washingtonpost.Newsweek Interactive Co. LLC

# **EXHIBIT F**

1 of 1 DOCUMENT

Copyright 2006 The New York Times Company  
The New York Times

January 17, 2006 Tuesday  
Late Edition - Final

**SECTION:** Section A; Column 6; National Desk; DOMESTIC SURVEILLANCE: THE PROGRAM; Pg. 1

**LENGTH:** 2354 words

**HEADLINE:** SPY AGENCY DATA AFTER SEPT. 11 LED F.B.I. TO DEAD ENDS

**BYLINE:** This article is by Lowell Bergman, Eric Lichtblau, Scott Shane and Don Van Natta Jr.; William K. Rashbaum contributed reporting from New York for this article.

**DATELINE:** WASHINGTON, Jan. 16

**BODY:**

In the anxious months after the Sept. 11 attacks, the National Security Agency began sending a steady stream of telephone numbers, e-mail addresses and names to the F.B.I. in search of terrorists. The stream soon became a flood, requiring hundreds of agents to check out thousands of tips a month.

But virtually all of them, current and former officials say, led to dead ends or innocent Americans.

F.B.I. officials repeatedly complained to the spy agency that the unfiltered information was swamping investigators. The spy agency was collecting much of the data by eavesdropping on some Americans' international communications and conducting computer searches of phone and Internet traffic. Some F.B.I. officials and prosecutors also thought the checks, which sometimes involved interviews by agents, were pointless intrusions on Americans' privacy.

As the bureau was running down those leads, its director, Robert S. Mueller III, raised concerns about the legal rationale for a program of eavesdropping without warrants, one government official said. Mr. Mueller asked senior administration officials about "whether the program had a proper legal foundation," but deferred to Justice Department legal opinions, the official said.

President Bush has characterized the eavesdropping program as a "vital tool" against terrorism; Vice President Dick Cheney has said it has saved "thousands of lives."

But the results of the program look very different to some officials charged with tracking terrorism in the United States. More than a dozen current and former law enforcement and counterterrorism officials, including some in the small circle who knew of the secret program and how it played out at the F.B.I., said the torrent of tips led them to few potential terrorists inside the country they did not know of from other sources and diverted agents from counterterrorism work they viewed as more productive.

"We'd chase a number, find it's a schoolteacher with no indication they've ever been involved in international terrorism -- case closed," said one former F.B.I. official, who was aware of the program and the data it generated for the bureau. "After you get a thousand numbers and not one is turning up anything, you get some frustration."

Intelligence officials disagree with any characterization of the program's results as modest, said Judith A. Emmel, a spokeswoman for the office of the director of national intelligence. Ms. Emmel cited a statement at a briefing last month by Gen. Michael V. Hayden, the country's second-ranking intelligence official and the director of the N.S.A. when the program was started.

## SPY AGENCY DATA AFTER SEPT. 11 LED F.B.I. TO DEAD ENDS The New York Times

"I can say unequivocally that we have gotten information through this program that would not otherwise have been available," General Hayden said. The White House and the F.B.I. declined to comment on the program or its results.

The differing views of the value of the N.S.A.'s foray into intelligence-gathering in the United States may reflect both bureaucratic rivalry and a culture clash. The N.S.A., an intelligence agency, routinely collects huge amounts of data from across the globe that may yield only tiny nuggets of useful information; the F.B.I., while charged with fighting terrorism, retains the traditions of a law enforcement agency more focused on solving crimes.

"It isn't at all surprising to me that people not accustomed to doing this would say, 'Boy, this is an awful lot of work to get a tiny bit of information,'" said Adm. Bobby R. Inman, a former N.S.A. director. "But the rejoinder to that is, 'Have you got anything better?'"

Several of the law enforcement officials acknowledged that they might not know of arrests or intelligence activities overseas that grew out of the domestic spying program. And because the program was a closely guarded secret, its role in specific cases may have been disguised or hidden even from key investigators.

Still, the comments on the N.S.A. program from the law enforcement and counterterrorism officials, many of them high level, are the first indication that the program was viewed with skepticism by key figures at the Federal Bureau of Investigation, the agency responsible for disrupting plots and investigating terrorism on American soil.

All the officials spoke on condition of anonymity because the program is classified. It is coming under scrutiny next month in hearings on Capitol Hill, which were planned after members of Congress raised questions about the legality of the eavesdropping. The program was disclosed in December by The New York Times.

The law enforcement and counterterrorism officials said the program had uncovered no active Qaeda networks inside the United States planning attacks. "There were no imminent plots -- not inside the United States," the former F.B.I. official said.

Some of the officials said the eavesdropping program might have helped uncover people with ties to Al Qaeda in Albany; Portland, Ore.; and Minneapolis. Some of the activities involved recruitment, training or fund-raising.

But, along with several British counterterrorism officials, some of the officials questioned assertions by the Bush administration that the program was the key to uncovering a plot to detonate fertilizer bombs in London in 2004. The F.B.I. and other law enforcement officials also expressed doubts about the importance of the program's role in another case named by administration officials as a success in the fight against terrorism, an aborted scheme to topple the Brooklyn Bridge with a blow torch.

Some officials said that in both cases, they had already learned of the plans through interrogation of prisoners or other means.

Immediately after the Sept. 11 attacks, the Bush administration pressed the nation's intelligence agencies and the F.B.I. to move urgently to thwart any more plots. The N.S.A., whose mission is to spy overseas, began monitoring the international e-mail messages and phone calls of people inside the United States who were linked, even indirectly, to suspected Qaeda figures.

Under a presidential order, the agency conducted the domestic eavesdropping without seeking the warrants ordinarily required from the secret Foreign Intelligence Surveillance Court, which handles national security matters. The administration has defended the legality of the program, pointing to what it says is the president's inherent constitutional power to defend the country and to legislation passed by Congress after the Sept. 11 attacks.

Administration officials told Mr. Mueller, the F.B.I. director, of the eavesdropping program, and his agency was enlisted to run down leads from it, several current and former officials said.

While he and some bureau officials discussed the fact that the program bypassed the intelligence surveillance court, Mr. Mueller expressed no concerns about that to them, those officials said. But another government official said Mr. Mueller had questioned the administration about the legal authority for the program.

Officials who were briefed on the N.S.A. program said the agency collected much of the data passed on to the F.B.I. as tips by tracing phone numbers in the United States called by suspects overseas, and then by following the domestic numbers to other numbers called. In other cases, lists of phone numbers appeared to result from the agency's computerized scanning of communications coming into and going out of the country for names and keywords that might

## SPY AGENCY DATA AFTER SEPT. 11 LED F.B.I. TO DEAD ENDS The New York Time

be of interest. The deliberate blurring of the source of the tips caused some frustration among those who had to follow up.

F.B.I. field agents, who were not told of the domestic surveillance programs, complained that they often were given no information about why names or numbers had come under suspicion. A former senior prosecutor who was familiar with the eavesdropping programs said intelligence officials turning over the tips "would always say that we had information whose source we can't share, but it indicates that this person has been communicating with a suspected Qaeda operative." He said, "I would always wonder, what does 'suspected' mean?"

"The information was so thin," he said, "and the connections were so remote, that they never led to anything, and I never heard any follow-up."

In response to the F.B.I. complaints, the N.S.A. eventually began ranking its tips on a three-point scale, with 3 being the highest priority and 1 the lowest, the officials said. Some tips were considered so hot that they were carried by hand to top F.B.I. officials. But in bureau field offices, the N.S.A. material continued to be viewed as unproductive, prompting agents to joke that a new bunch of tips meant more "calls to Pizza Hut," one official, who supervised field agents, said.

The views of some bureau officials about the value of the N.S.A.'s domestic surveillance offers a revealing glimpse of the difficulties law enforcement and intelligence agencies have had cooperating since Sept. 11.

The N.S.A., criticized by the national Sept. 11 commission for its "avoidance of anything domestic" before the attacks, moved aggressively into the domestic realm after them. But the legal debate over its warrantless eavesdropping has embroiled the agency in just the kind of controversy its secretive managers abhor. The F.B.I., meanwhile, has struggled over the last four years to expand its traditional mission of criminal investigation to meet the larger menace of terrorism.

Admiral Inman, the former N.S.A. director and deputy director of C.I.A., said the F.B.I. complaints about thousands of dead-end leads revealed a chasm between very different disciplines. Signals intelligence, the technical term for N.S.A.'s communications intercepts, rarely produces "the complete information you're going to get from a document or a witness" in a traditional F.B.I. investigation, he said.

Some F.B.I. officials said they were uncomfortable with the expanded domestic role played by the N.S.A. and other intelligence agencies, saying most intelligence officers lacked the training needed to safeguard Americans' privacy and civil rights. They said some protections had to be waived temporarily in the months after Sept. 11 to detect a feared second wave of attacks, but they questioned whether emergency procedures like the eavesdropping should become permanent.

That discomfort may explain why some F.B.I. officials may seek to minimize the benefits of the N.S.A. program or distance themselves from the agency. "This wasn't our program," an F.B.I. official said. "It's not our mess, and we're not going to clean it up."

The N.S.A.'s legal authority for collecting the information it passed to the F.B.I. is uncertain. The Foreign Intelligence Surveillance Act requires a warrant for the use of so-called pen register equipment that records American phone numbers, even if the contents of the calls are not intercepted. But officials with knowledge of the program said no warrants were sought to collect the numbers, and it is unclear whether the secret executive order signed by Mr. President Bush in 2002 to authorize eavesdropping without warrants also covered the collection of phone numbers and e-mail addresses.

Aside from the director, F.B.I. officials did not question the legal status of the tips, assuming that N.S.A. lawyers had approved. They were more concerned about the quality and quantity of the material, which produced "mountains of paperwork" often more like raw data than conventional investigative leads.

"It affected the F.B.I. in the sense that they had to devote so many resources to tracking every single one of these leads, and, in my experience, they were all dry leads," the former senior prosecutor said. "A trained investigator never would have devoted the resources to take those leads to the next level, but after 9/11, you had to."

By the administration's account, the N.S.A. eavesdropping helped lead investigators to Iyman Faris, an Ohio truck driver and friend of Khalid Shaikh Mohammed, who is believed to be the mastermind of the Sept. 11 attacks. Mr. Faris spoke of toppling the Brooklyn Bridge by taking a torch to its suspension cables, but concluded that it would not work. He is now serving a 20-year sentence in a federal prison.

SPY AGENCY DATA AFTER SEPT. 11 LED F.B.I. TO DEAD ENDS The New York Time

But as in the London fertilizer bomb case, some officials with direct knowledge of the Faris case dispute that the N.S.A. information played a significant role.

By contrast, different officials agree that the N.S.A.'s domestic operations played a role in the arrest of an imam and another man in Albany in August 2004 as part of an F.B.I. counterterrorism sting investigation. The men, Yassin Aref, 35, and Mohammed Hossain, 49, are awaiting trial on charges that they attempted to engineer the sale of missile launchers to an F.B.I. undercover informant.

In addition, government officials said the N.S.A. eavesdropping program might have assisted in the investigations of people with suspected Qaeda ties in Portland and Minneapolis. In the Minneapolis case, charges of supporting terrorism were filed in 2004 against Mohammed Abdullah Warsame, a Canadian citizen. Six people in the Portland case were convicted of crimes that included money laundering and conspiracy to wage war against the United States.

Even senior administration officials with access to classified operations suggest that drawing a clear link between a particular source and the unmasking of a potential terrorist is not always possible.

When Michael Chertoff, the homeland security secretary, was asked last week on "The Charlie Rose Show" whether the N.S.A. wiretapping program was important in deterring terrorism, he said, "I don't know that it's ever possible to attribute one strand of intelligence from a particular program."

But Mr. Chertoff added, "I can tell you in general the process of doing whatever you can do technologically to find out what is being said by a known terrorist to other people, and who that person is communicating with, that is without a doubt one of the critical tools we've used time and again."

**URL:** <http://www.nytimes.com>

**GRAPHIC:** Photos: Robert S. Mueller III (Photo by Spencer Platt/Getty Images)  
Michael Chertoff (Photo by Joshua Roberts/Getty Images)  
Yassin Aref (Photo by Chip East/Reuters)  
Iyman Faris (Photo by Department of Justice)(pg. A14)

**LOAD-DATE:** January 17, 2006

# **EXHIBIT G**



## **NSA spy program hinges on state-of-the-art technology**

By **Shane Harris**, National Journal

The furor over the National Security Agency's domestic eavesdropping, authorized by President Bush, has focused largely on legal questions -- whether the NSA has the authority to spy on Americans inside the United States and whether the commander-in-chief can order the agency to do so.

But that debate has largely smothered examination of how the nation's largest intelligence agency is collecting -- and analyzing -- information intercepted from hundreds, possibly thousands, of Americans. Since the 9/11 attacks, the NSA has abandoned the mantra that guided it in earlier decades -- Do not spy on Americans inside the nation's borders. Things have changed, and the NSA may be on the cusp of employing state-of-the-art technologies to uncover more information about potential terrorists, and about Americans here at home.

In the first days after 9/11, amid the palpable fear of another strike and an all-hands investigation of the attacks by the FBI and CIA, the NSA's then-director, Lt. Gen. Michael Hayden, took a broad view of his agency's power to conduct electronic eavesdropping.

Whereas existing laws, regulations, and executive orders restricted domestic monitoring of U.S. persons without a warrant, Hayden told House Intelligence Committee members on October 1, 2001, that he "had been operating since the September 11 attacks with an expansive view of [his] authorities," according to a declassified letter that Rep. Nancy Pelosi, D-Calif., then the committee's ranking Democrat, sent to the general after he briefed lawmakers.

Pelosi was troubled by the legal rationale for the NSA's activities. Although significant portions of her letter -- and most of Hayden's response -- are redacted, Pelosi wrote that she was "concerned whether, and to what extent, the [NSA] has received specific presidential authorization for the operations you are conducting." According to the letter, those operations included the NSA's sharing of intercepted communications with the FBI without first receiving a request for such reports -- the normal procedure, to avoid the co-mingling of intelligence and law enforcement operations.

According to sources who are knowledgeable about the NSA's domestic operations but who would not be identified because those operations are still classified, just after 9/11, the NSA targeted and intercepted the communications of specific foreign persons and groups, an indication that at least some of the targets were previously known to U.S. intelligence. The sources didn't specify whether any persons inside the United States were also monitored. But, Pelosi wrote, Hayden informed lawmakers that the NSA was making the call about what intercepted information was of "foreign-intelligence interest" before passing it to the FBI.

*The New York Times* reported this week that "in the anxious months after the September 11 attacks, the [NSA] began sending a steady stream of telephone numbers, e-mail addresses, and names to the FBI, in search of terrorists." Some of that information led to Americans inside the

United States. It appears that the NSA was handing over just about any information it could find that might be useful to investigators. *The Times* reported that the NSA eventually provided thousands of tips a month.

The agency conducted these activities without presidential authorization for at least three months following 9/11. In early 2002, Bush authorized the current program, which, he has said, targets only known members of Al Qaeda and affiliated groups, and people linked to them. But even before Bush's order -- which remains classified -- the NSA's work was evolving from targeted interceptions to broader sifting and sorting of huge volumes of communications data.

Officials with some of the nation's leading telecommunications companies have said they gave the NSA access to their switches, the hubs through which enormous volumes of phone and e-mail traffic pass every day, to aid the agency's effort to determine exactly whom suspected Qaeda figures were calling in the United States and abroad and who else was calling those numbers. The NSA used the intercepts to construct webs of potentially interrelated persons. (*The Times*, citing FBI sources, reported that most of these tips led to dead ends or to innocent Americans.)

Analyzing large amounts of telecom traffic would give security officials valuable information about potential adversaries, revealing the times of day that terrorist suspects tended to conduct their communications, and the means they used -- land-line phones, mobile phones, or the Internet -- according to telecommunications experts.

One telecom executive told *National Journal* that NSA officials approached him shortly after the 9/11 attacks and insisted, to the point of questioning his company's patriotism, that executives hand over the company's "call detail records." Those documents, known as CDRs, trace the history of every call placed on a network, including a call's origin and destination, the time it started and ended, how long it lasted, and how it was routed through the network.

Having wholesale access to many companies' records would, in theory, give the NSA a picture of telecom usage across the country. And, since many U.S.-based carriers route international calls through their domestic switches, a picture of the wider world could emerge as well. The telecom executive said he believed that the NSA wanted the information to conduct a "data-mining" analysis of call and e-mail traffic.

Fifty years ago, intelligence officers had to manually scan communications intercepts for keywords, names, or other tantalizing intelligence nuggets. The NSA has long since automated that process with sophisticated supercomputers that can read huge stores of intercepts at speeds human beings can barely contemplate.

But more recently, the NSA has pursued cutting-edge data-mining technologies that don't just find key words but also uncover hidden relationships among data points. These technologies can even detect how a particular analyst thinks, identify what his or her biases are, and then suggest alternative hypotheses.

Data-mining systems, which the NSA has publicly pursued and spent millions of dollars researching, don't just "connect the dots" but also alert analysts about which dots to connect, which to disregard, and how to connect them in ways they may never have considered. It is unclear which, if any, of these data-mining tools the NSA is using to analyze the domestic information gathered in the current eavesdropping program, but the tools themselves offer a telling look into the agency's potential to exploit what it collects, regardless of its legal basis for

doing so.

In September 2002, one year after the 9/11 attacks, a technology research-and-development office located at the NSA's Fort Meade, Md., headquarters awarded \$64 million in research contracts for a new program called Novel Intelligence from Massive Data. The NIMD project, set to last for three and a half years, is intended to keep intelligence analysts from drowning under the massive flow of information they encounter and therefore missing key pieces of intelligence. In essence, it is an early-warning system.

"NIMD funds research to ... help analysts deal with information-overload, detect early indicators of strategic surprise, and avoid analytic errors," reads a "Call for 2005 Challenge Workshop Proposals" released by the Advanced Research and Development Activity (ARDA), the group at Fort Meade that was founded in 1998 to field new technologies for intelligence agencies, especially the NSA.

The administration has informed some lawmakers that the eavesdropping program the president authorized in 2002 is also designed to be an early-warning system. In late December, Assistant Attorney General William E. Moschella wrote to the top Democrats and Republicans on the House and Senate Intelligence committees, "The president determined that it was necessary following September 11 to create an early-warning detection system" to prevent more attacks.

Tellingly, Moschella wrote that the Foreign Intelligence Surveillance Act, which allows the government to obtain warrants to conduct domestic eavesdropping or wiretapping, "could not have provided the speed and agility required for the early-warning detection system."

The administration hasn't elaborated on why the system needs to operate independently of FISA, but officials may believe that it cannot meet the law's minimum threshold for surveillance, which requires a probable cause that the target is a terrorist, said Steven Aftergood, an expert on intelligence and government secrecy with the Federation of American Scientists.

"Logistically speaking, the early-warning approach may involve a significant increase in the number of surveillance actions," Aftergood said. "It may be that neither the Justice Department nor the [Foreign Intelligence Surveillance Court, which approves wiretapping warrants] is prepared to prepare and process several thousand additional FISA applications per year, beyond the 1,700 or so approved in 2004."

If the NSA is monitoring large numbers of communications -- *The Times* has reported that the agency has monitored as many as 500 Americans and other residents of the United States at one time -- then it stands to reason that applications for warrants could take time to process.

The NIMD project, as well as some others that ARDA is pursuing, closely resembles those of another controversial data-mining program aimed at discovering terrorist plots -- the Defense Department's Total Information Awareness program. Suspended in 2003, TIA was also designed as an early-warning system that would mine intelligence databases, but also private databases of credit card records and other transactions, for telltale signals of terrorist plots.

Of the companies and research institutions that won NIMD contracts in September 2002, six also held contracts for the earlier TIA project. Their TIA work focused on key areas of interest to NIMD, including challenging analytic assumptions and building prototype data-mining devices.

Like NIMD, TIA aimed to challenge analysts' traditional notions about what a given piece of intelligence might signify. It did this by creating a database of what TIA creator John Poindexter called "plausible futures," or likely terrorism scenarios. Another ARDA project also envisions such a database.

The Advanced Capabilities for Intelligence Analysis program, which is a cousin of NIMD, looks for ways "to construct and use plausible futures in order to provide additional, novel interpretations for today's collection" of intelligence information, according to the 2005 call for proposals.

TIA was distinct from NIMD and other projects in that it specifically focused on counter-terrorism, according to Tom Armour, a former program manager in Poindexter's office at the Defense Advanced Research Projects Agency. However, Armour says, the two research teams had "good coordination" and discussed their projects on a regular basis.

When Congress eliminated funding for most of Poindexter's projects, a number of them (the exact number is classified) were transferred to intelligence agencies. Armour and others associated with TIA would not disclose the names of those agencies, but a former Army intelligence analyst also involved in data mining and counter-terrorism confirms that TIA tools were transferred to other agencies, where work on them continues to this day.

Asked whether data-mining programs, such as NIMD, that the NSA may still be pursuing would be useful for analyzing large amounts of phone and e-mail traffic, Armour said, "Absolutely. That's, in fact, what the interest is." The former No. 2 official in Poindexter's office, Robert Popp, said that he and his colleagues wanted to know whether intercepted phone calls and e-mail would help find terrorists but not ensnare innocent people. "We didn't know," Popp said. "That was the hypothesis. That was the question that Poindexter and I wanted to do research on, to be better able to understand."

The similarities between TIA and the NSA's current data-mining operations were enough to prompt one senior lawmaker to signal his discomfort in a letter to Vice President Cheney. Sen. Jay Rockefeller IV, D-W.Va., the vice chairman of the Senate Intelligence Committee, was briefed by Cheney, Hayden, and then-Director of Central Intelligence George Tenet in July 2003.

"As I reflected on the meeting today," Rockefeller wrote, "John Poindexter's TIA project sprung to mind, exacerbating my concern regarding the direction the administration is moving with regard to security, technology, and surveillance."

Whether the NSA research shares another similarity with Poindexter's work remains, troublingly, unanswered. Poindexter's office spent between \$4 million and \$5 million researching technology and policy that would protect the privacy of innocent people whose names might turn up in a data search, Popp said. "No one else was, or is, to our knowledge, putting that kind of investment in the privacy R&D area, certainly not in 2002 and 2003, like we were."

The Senate Judiciary Committee plans to hold hearings in the coming weeks on the NSA's domestic operations. In addition to the specifics of how the NSA collects and mines information, senators undoubtedly will want to know what assurances American citizens have that they won't be ensnared in a vast data-search net.

Poindexter addressed the trade-off between privacy and security in 2003, when he was forced to

resign as the TIA manager amid criticism that it was an Orwellian assault on civil liberties. In his resignation letter, Poindexter wrote, "It would be no good to solve the security problem and give up the privacy and civil liberties that make our country great."

*This document is located at <http://www.govexec.com/dailyfed/0106/012006nj1.htm>*

©2007 by National Journal Group Inc. All rights reserved.

# **EXHIBIT H**

## SEATTLE POST-INTELLIGENCER

[http://seattlepi.nwsourc.com/attack/256521\\_wiretap21.html](http://seattlepi.nwsourc.com/attack/256521_wiretap21.html)

### Lawmaker queries Microsoft, other companies on NSA wiretaps

*Saturday, January 21, 2006*

**By JEFF BLISS**  
BLOOMBERG NEWS

Rep. John Conyers, the House Judiciary Committee's senior Democrat, is asking 20 telephone companies and Internet providers, including Microsoft Corp. and AT&T Inc., whether they cooperated in the government's wiretapping program.

Conyers, a Michigan lawmaker, is asking in the letters sent Friday whether the companies "allowed the federal government to eavesdrop on customer communications through your facilities or turned over customer records when not compelled to do so by law."

BellSouth Corp., Verizon Communications Inc., EarthLink Inc. and Google Inc. are among the companies being sent the inquiries, as Conyers seeks to highlight what Democrats say are the Bush administration's excesses in authorizing eavesdropping on international phone calls and e-mails without court approvals.

"There can be no doubt that today we are in a constitutional crisis that threatens the systems of checks and balances," Conyers said during a forum held by Democrats in Washington on the National Security Agency's wiretapping program.

No Republican lawmakers participated in the forum.

Senate Judiciary Committee Chairman Arlen Specter, a Pennsylvania Republican, has scheduled a hearing Feb. 6 to discuss whether President Bush could legally authorize the wiretaps without warrants. Senate Intelligence Chairman Pat Roberts, a Kansas Republican, has said his panel also will look into the wiretaps.

The Justice Department released a 42-page analysis on Thursday saying Bush has authority to conduct the wiretapping under his constitutional role as commander-in-chief to protect the United States from attack, and under the resolution passed by Congress after the Sept. 11 attacks authorizing military force.

Under the program, the NSA listens to hundreds and perhaps thousands of calls made to and from the United States.

While the NSA has declined to comment on the program, telecommunications specialists familiar with the government's methods said phone companies are essential to the widespread surveillance the agency conducts.

In the past, the NSA has gotten permission from phone companies to gain access to so-called switches, high-powered computers into which phone traffic flows and is redirected, at 600 locations across the nation, said Daniel Berninger, a senior analyst at Tier 1 Research in Plymouth, Minn. From these corporate relationships, the NSA can get the content of calls and records on their date, time, length, origin and destination.



Information on the characteristics of a call can be used to figure out patterns in phone traffic that may indicate if terrorists are planning an attack, said Steve Bellovin, a computer science professor at Columbia University in New York.

To look at e-mails and other Internet traffic, the NSA would need the help of Internet service providers, Bellovin said. If terrorists encrypted their messages, it would be very difficult if not impossible to read them without the companies' help, he said.

© 1998-2007 *Seattle Post-Intelligencer*

# **EXHIBIT I**

washingtonpost.com

# Surveillance Net Yields Few Suspects

## NSA's Hunt for Terrorists Scrutinizes Thousands of Americans, but Most Are Later Cleared

By Barton Gellman, Dafna Linzer and Carol D. Leonnig  
Washington Post Staff Writers  
Sunday, February 5, 2006; A01

Intelligence officers who eavesdropped on thousands of Americans in overseas calls under authority from President Bush have dismissed nearly all of them as potential suspects after hearing nothing pertinent to a terrorist threat, according to accounts from current and former government officials and private-sector sources with knowledge of the technologies in use.

Bush has recently described the warrantless operation as "terrorist surveillance" and summed it up by declaring that "if you're talking to a member of al Qaeda, we want to know why." But officials conversant with the program said a far more common question for eavesdroppers is whether, not why, a terrorist plotter is on either end of the call. The answer, they said, is usually no.

Fewer than 10 U.S. citizens or residents a year, according to an authoritative account, have aroused enough suspicion during warrantless eavesdropping to justify interception of their domestic calls, as well. That step still requires a warrant from a federal judge, for which the government must supply evidence of probable cause.

The Bush administration refuses to say -- in public or in closed session of Congress -- how many Americans in the past four years have had their conversations recorded or their e-mails read by intelligence analysts without court authority. Two knowledgeable sources placed that number in the thousands; one of them, more specific, said about 5,000.

The program has touched many more Americans than that. Surveillance takes place in several stages, officials said, the earliest by machine. Computer-controlled systems collect and sift basic information about hundreds of thousands of faxes, e-mails and telephone calls into and out of the United States before selecting the ones for scrutiny by human eyes and ears.

Successive stages of filtering grow more intrusive as artificial intelligence systems rank voice and data traffic in order of likeliest interest to human analysts. But intelligence officers, who test the computer judgments by listening initially to brief fragments of conversation, "wash out" most of the leads within days or weeks.

The scale of warrantless surveillance, and the high proportion of bystanders swept in, sheds new light on Bush's circumvention of the courts. National security lawyers, in and out of government, said the washout rate raised fresh doubts about the program's lawfulness under the Fourth Amendment, because a search cannot be judged "reasonable" if it is based on evidence that experience shows to be unreliable. Other officials said the disclosures might shift the terms of public debate, altering perceptions about the balance between privacy lost and security gained.

Advertisement:

### \$510,000 Mortgage for Under \$1,698/Month!

Think You Pay Too Much For Your Mortgage? Find Out!

© 2006 LowerMyBills.com



Click Your State

Alabama

Click Your Rate

3.00% - 3.99%

Click Credit Type

Good

LowerMyBills.com

Air Force Gen. Michael V. Hayden, the nation's second-ranking intelligence officer, acknowledged in a news briefing last month that eavesdroppers "have to go down some blind alleys to find the tips that pay off." Other officials, nearly all of whom spoke on the condition of anonymity because they are not permitted to discuss the program, said the prevalence of false leads is especially pronounced when U.S. citizens or residents are surveilled. No intelligence agency, they said, believes that "terrorist . . . operatives inside our country," as Bush described the surveillance targets, number anywhere near the thousands who have been subject to eavesdropping.

The Bush administration declined to address the washout rate or answer any other question for this article about the policies and operations of its warrantless eavesdropping.

Vice President Cheney has made the administration's strongest claim about the program's intelligence value, telling CNN in December that eavesdropping without warrants "has saved thousands of lives." Asked about that Thursday, Hayden told senators he "cannot personally estimate" such a figure but that the program supplied information "that would not otherwise have been available." FBI Director Robert S. Mueller III said at the same hearing that the information helped identify "individuals who were providing material support to terrorists."

Supporters speaking unofficially said the program is designed to warn of unexpected threats, and they argued that success cannot be measured by the number of suspects it confirms. Even unwitting Americans, they said, can take part in communications -- arranging a car rental, for example, without knowing its purpose -- that supply "indications and warnings" of an attack. Contributors to the technology said it is a triumph for artificial intelligence if a fraction of 1 percent of the computer-flagged conversations guide human analysts to meaningful leads.

Those arguments point to a conflict between the program's operational aims and the legal and political limits described by the president and his advisers. For purposes of threat detection, officials said, the analysis of a telephone call is indifferent to whether an American is on the line. Since Sept. 11, 2001, a former CIA official said, "there is a lot of discussion" among analysts "that we shouldn't be dividing Americans and foreigners, but terrorists and non-terrorists." But under the Constitution, and in the Bush administration's portrait of its warrantless eavesdropping, the distinction is fundamental.

Valuable information remains valuable even if it comes from one in a thousand intercepts. But government officials and lawyers said the ratio of success to failure matters greatly when eavesdropping subjects are Americans or U.S. visitors with constitutional protection. The minimum legal definition of probable cause, said a government official who has studied the program closely, is that evidence used to support eavesdropping ought to turn out to be "right for one out of every two guys at least." Those who devised the surveillance plan, the official said, "knew they could never meet that standard -- that's why they didn't go through" the court that supervises the Foreign Intelligence Surveillance Act, or FISA.

Michael J. Woods, who was chief of the FBI's national security law unit until 2002, said in an e-mail interview that even using the lesser standard of a "reasonable basis" requires evidence "that would lead a prudent, appropriately experienced person" to believe the American is a terrorist agent. If a factor returned "a large number of false positives, I would have to conclude that the factor is not a sufficiently reliable indicator and thus would carry less (or no) weight."

Bush has said his program covers only overseas calls to or from the United States and stated categorically that "we will not listen inside this country" without a warrant. Hayden said the government goes to the intelligence court when an eavesdropping subject becomes important enough to "drill down," as he put it, "to the degree that we need all communications."

Yet a special channel set up for just that purpose four years ago has gone largely unused, according to an authoritative account. Since early 2002, when the presiding judge of the federal intelligence court first learned of Bush's program, he agreed to a system in which prosecutors may apply for a domestic warrant after warrantless eavesdropping on the same person's overseas communications. The annual number of such applications, a source said, has been in the single digits.

Many features of the surveillance program remain unknown, including what becomes of the non-threatening U.S. e-mails and conversations that the NSA intercepts. Participants, according to a national security lawyer who represents one of them privately, are growing "uncomfortable with the mountain of data they have now begun to accumulate." Spokesmen for the Bush administration declined to say whether any are discarded.

### **New Imperatives**

Recent interviews have described the program's origins after Sept. 11 in what Hayden has called a three-way collision of "operational, technical and legal imperatives."

Intelligence agencies had an urgent mission to find hidden plotters before they could strike again.

About the same time, advances in technology -- involving acoustic engineering, statistical theory and efficient use of computing power to apply them -- offered new hope of plucking valuable messages from the vast flow of global voice and data traffic. And rapidly changing commercial trends, which had worked against the NSA in the 1990s as traffic shifted from satellites to fiber-optic cable, now presented the eavesdroppers with a gift. Market forces were steering as much as a third of global communications traffic on routes that passed through the United States.

The Bush administration had incentive and capabilities for a new kind of espionage, but 23 years of law and White House policy stood in the way.

FISA, passed in 1978, was ambiguous about some of the president's plans, according to current and retired government national security lawyers. But other features of the eavesdropping program fell outside its boundaries.

One thing the NSA wanted was access to the growing fraction of global telecommunications that passed through junctions on U.S. territory. According to former senator Bob Graham (D-Fla.), who chaired the Intelligence Committee at the time, briefers told him in Cheney's office in October 2002 that Bush had authorized the agency to tap into those junctions. That decision, Graham said in an interview first reported in The Washington Post on Dec. 18, allowed the NSA to intercept "conversations that . . . went through a transit facility inside the United States."

According to surveys by TeleGeography Inc., nearly all voice and data traffic to and from the United States now travels by fiber-optic cable. About one-third of that volume is in transit from one foreign country to another, traversing U.S. networks along its route. The traffic passes through cable landing stations, where undersea communications lines meet the East and West coasts; warehouse-size gateways where competing international carriers join their networks; and major Internet hubs known as metropolitan area ethernets.

Until Bush secretly changed the rules, the government could not tap into access points on U.S. soil without a warrant to collect the "contents" of any communication "to or from a person in the United States." But the FISA law was silent on calls and e-mails that began and ended abroad.

Even for U.S. communications, the law was less than clear about whether the NSA could harvest information about that communication that was not part of its "contents."

"We debated a lot of issues involving the 'metadata,'" one government lawyer said. Valuable for analyzing calling patterns, the metadata for telephone calls identify their origin, destination, duration and time. E-mail headers carry much the same information, along with the numeric address of each network switch through which a message has passed.

Intelligence lawyers said FISA plainly requires a warrant if the government wants real-time access to that information for any one person at a time. But the FISA court, as some lawyers saw it, had no explicit jurisdiction over wholesale collection of records that do not include the content of communications. One high-ranking intelligence official who argued for a more cautious approach said he found himself pushed aside. Awkward silences began to intrude on meetings that discussed the evolving rules.

"I became aware at some point of things I was not being told about," the intelligence official said.

### 'Subtly Softer Trigger'

Hayden has described a "subtly softer trigger" for eavesdropping, based on a powerful "line of logic," but no Bush administration official has acknowledged explicitly that automated filters play a role in selecting American targets. But Sen. Arlen Specter (R-Pa.), who chairs the Judiciary Committee, referred in a recent letter to "mechanical surveillance" that is taking place before U.S. citizens and residents are "subject to human surveillance."

Machine selection would be simple if the typical U.S. eavesdropping subject took part in direct calls to or from the "phone numbers of known al Qaeda" terrorists, the only criterion Bush has mentioned.

That is unusual. The NSA more commonly looks for less-obvious clues in the "terabytes of speech, text, and image data" that its global operations collect each day, according to an unclassified report by the National Science Foundation soliciting research on behalf of U.S. intelligence.

NSA Inspector General Joel F. Brenner said in 2004 that the agency's intelligence officers have no choice but to rely on "electronic filtering, sorting and dissemination systems of amazing sophistication but that are imperfect."

One method in use, the NSF report said, is "link analysis." It takes an established starting point -- such as a terrorist just captured or killed -- and looks for associated people, places, things and events. Those links can be far more tenuous than they initially appear.

In an unclassified report for the Pentagon's since-abandoned Total Information Awareness program, consultant Mary DeRosa showed how "degrees of separation" among the Sept. 11 conspirators concealed the significance of clues that linked them.

Khalid Almihdhar, one of the hijackers, was on a government watch list for terrorists and thus a known suspect. Mohamed Atta, another hijacker, was linked to Almihdhar by one degree of separation because he used the same contact address when booking his flight. Wail M. Alshehri, another hijacker, was linked by two degrees of separation because he shared a telephone number with Atta. Satam M.A. Al Suqami, still another hijacker, shared a post office box with Alshehri and, therefore, had three degrees of separation from the original suspect.



## 'Look for Patterns'

Those links were not obvious before the identity of the hijackers became known. A major problem for analysts is that a given suspect may have hundreds of links to others with one degree of separation, including high school classmates and former neighbors in a high-rise building who never knew his name. Most people are linked to thousands or tens of thousands of people by two degrees of separation, and hundreds of thousands or millions by three degrees.

Published government reports say the NSA and other data miners use mathematical techniques to form hypotheses about which of the countless theoretical ties are likeliest to represent a real-world relationship.

A more fundamental problem, according to a high-ranking former official with firsthand knowledge, is that "the number of identifiable terrorist entities is decreasing." There are fewer starting points, he said, for link analysis.

"At that point, your only recourse is to look for patterns," the official said.

Pattern analysis, also described in the NSF and DeRosa reports, does not depend on ties to a known suspect. It begins with places terrorists go, such as the Pakistani province of Waziristan, and things they do, such as using disposable cell phones and changing them frequently, which U.S. officials have publicly cited as a challenge for counterterrorism.

"These people don't want to be on the phone too long," said Russell Tice, a former NSA analyst, offering another example.

Analysts build a model of hypothetical terrorist behavior, and computers look for people who fit the model. Among the drawbacks of this method is that nearly all its selection criteria are innocent on their own. There is little precedent, lawyers said, for using such a model as probable cause to get a court-issued warrant for electronic surveillance.

Jeff Jonas, now chief scientist at IBM Entity Analytics, invented a data-mining technology used widely in the private sector and by the government. He sympathizes, he said, with an analyst facing an unknown threat who gathers enormous volumes of data "and says, 'There must be a secret in there.'"

But pattern matching, he argued, will not find it. Techniques that "look at people's behavior to predict terrorist intent," he said, "are so far from reaching the level of accuracy that's necessary that I see them as nothing but civil liberty infringement engines."

## 'A Lot Better Than Chance'

Even with 38,000 employees, the NSA is incapable of translating, transcribing and analyzing more than a fraction of the conversations it intercepts. For years, including in public testimony by Hayden, the agency has acknowledged use of automated equipment to analyze the contents and guide analysts to the most important ones.

According to one knowledgeable source, the warrantless program also uses those methods. That is significant to the public debate because this kind of filtering intrudes into content, and machines "listen" to more Americans than humans do. NSA rules since the late 1970s, when machine filtering was far less capable, have said "acquisition" of content does not take place until a conversation is intercepted and



processed "into an intelligible form intended for human inspection."

The agency's filters are capable of comparing spoken language to a "dictionary" of key words, but Roger W. Cressey, a senior White House counterterrorism official until late 2002, said terrorists and other surveillance subjects make frequent changes in their code words. He said, " 'Wedding' was martyrdom day and the 'bride' and 'groom' were the martyrs." But al Qaeda has stopped using those codes.

An alternative approach, in which a knowledgeable source said the NSA's work parallels academic and commercial counterparts, relies on "decomposing an audio signal" to find qualities useful to pattern analysis. Among the fields involved are acoustic engineering, behavioral psychology and computational linguistics.

A published report for the Defense Advanced Research Projects Agency said machines can easily determine the sex, approximate age and social class of a speaker. They are also learning to look for clues to deceptive intent in the words and "paralinguistic" features of a conversation, such as pitch, tone, cadence and latency.

This kind of analysis can predict with results "a hell of a lot better than chance" the likelihood that the speakers are trying to conceal their true meaning, according to James W. Pennebaker, who chairs the psychology department at the University of Texas at Austin.

"Frankly, we'll probably be wrong 99 percent of the time," he said, "but 1 percent is far better than 1 in 100 million times if you were just guessing at random. And this is where the culture has to make some decisions."

*Researcher Julie Tate and staff writer R. Jeffrey Smith contributed to this report.*

© 2006 The Washington Post Company

**Ads by Google**

**Help Save the Children.**

Make a difference in the lives of children in need. Donate online now  
[www.SaveTheChildren.org/donate](http://www.SaveTheChildren.org/donate)

**Belize Island Property**


Parcels for sale on magnificent Caribbean island eco-paradise  
[www.belizeislandrealestate.com](http://www.belizeislandrealestate.com)

**MedSpanish International**

Spanish and International Health Flexible, Clinical, CME, Elective  
[www.MedSpanish.Com](http://www.MedSpanish.Com)

# **EXHIBIT J**

Advertisement



**EARN 3% CASH BACK FOR EVERY ELIGIBLE PURCHASE**

CHASEFREEDOM



Powered by

## Telecoms let NSA spy on calls

By Leslie Cauley and John Diamond, USA TODAY

The National Security Agency has secured the cooperation of large telecommunications companies, including AT&T, MCI and Sprint, in its efforts to eavesdrop without warrants on international calls by suspected terrorists, according to seven telecommunications executives.



Michael Hayden, former head of the NSA, during a hearing last week on Capitol Hill.

Alex Wong, Getty Images

The executives asked to remain anonymous because of the sensitivity of the program. AT&T, MCI and Sprint had no official comment.

The Senate Judiciary Committee begins hearings today on the government's program of monitoring international calls and e-mails of a domestic target without first obtaining court orders. At issue: whether the surveillance is legal, as President Bush insists, or an illegal intrusion into the lives of Americans, as lawsuits by civil libertarians contend. **(Related: Committee chief says program violates law)**


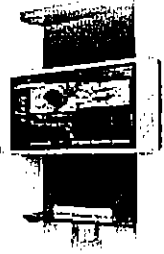
In domestic investigations, phone companies routinely require court orders before cooperating.

A majority of international calls are handled by long-distance carriers AT&T, MCI and Sprint. All three own "gateway" switches capable of routing calls to points around the globe. AT&T was recently acquired by SBC Communications, which has since adopted the AT&T name as its corporate moniker. MCI, formerly known as WorldCom, was recently acquired by Verizon. Sprint recently merged with Nextel.

*The New York Times*, which disclosed the clandestine operation in December, previously reported that telecommunications companies have been cooperating with the government, but it did not name the companies involved. **(Related: Bush says NSA program is legal)**


Decisions about monitoring calls are made in four steps, according to two U.S. intelligence officials familiar with the program who insisted on anonymity because it

Advertisement

**Thinking about making a major purchase?**

[▶ Learn More](#)



remains classified:

- Information from U.S. or allied intelligence or law enforcement points to a terrorism-related target either based in the United States or communicating with someone in the United States.
- Using a 48-point checklist to identify possible links to al-Qaeda, one of three NSA officials authorized to approve a warrantless intercept decides whether the surveillance is justified. Gen. Michael Hayden, the nation's No. 2 intelligence officer, said the checklist focuses on ensuring that there is a "reasonable basis" for believing there is a terrorist link involved.
- Technicians work with phone company officials to intercept communications pegged to a particular person or phone number. Telecommunications executives say MCI, AT&T and Sprint grant the access to their systems without warrants or court orders. Instead, they are cooperating on the basis of oral requests from senior government officials.
- If the surveillance yields information about a terror plot, the NSA notifies the FBI or other appropriate agencies but does not always disclose the source of its information. Call-routing information provided by the phone companies can help intelligence officials eavesdrop on a conversation. It also helps them physically locate the parties, which is important if cellphones are being used. If the U.S. end of a communication has nothing to do with terrorism, the identity of the party is suppressed and the content of the communication destroyed, Hayden has said.

The government has refused to publicly discuss the precise number of individuals targeted.

*The Times* and *The Washington Post* have said thousands have had communications intercepted.

The two intelligence officials said that number has been whittled down to about 600 people in the United States who have been targeted for repeated surveillance since the Sept. 11 attacks.

▪ REFRINTS & PERMISSIONS

**Find this article at:**

[http://www.usatoday.com/news/washington/2006-02-05-nsa-telecoms\\_x.htm?POE=NEWISVA](http://www.usatoday.com/news/washington/2006-02-05-nsa-telecoms_x.htm?POE=NEWISVA)

Check the box to include the list of links referenced in the article.

Related Advertising Links

|   |  |   |
|---|--|---|
| <input checked="" type="checkbox"/> <b>Get A Sports Industry Patent Idea?</b><br>We have helped our clients secure more than 10,000 patents. Free info.<br><a href="http://www.inventhelp.com">www.inventhelp.com</a> | <b>Free Air Jordan Shoe Pack</b><br>4 pairs of Jordan's are yours for free! Act now.<br><a href="http://sports-fitness-rewardpath.com">sports-fitness-rewardpath.com</a> | <b>Free Terrell Owens Jersey</b><br>We'll send you an official T.O. Cowboy jersey for free! Survey req.<br><a href="http://www.ontheweb-offer.com">www.ontheweb-offer.com</a> |
|---|--|---|

# **EXHIBIT K**

Search

How do I find it?

ADVERTISEMENT



introducing  
**LB** mat



Home News Travel Money Sports Life Tech Weather

Washington/Politics  ▼

# NSA has massive database of Americans' phone calls

Updated 5/11/2006 10:38 AM ET

E-mail | Save | Print | Reprints & Permissions | Subscribe to stories like this

Rela

Ref  
ww

Mo  
ww

Ref  
ww



Enlarge By Roger Wollenberg, Getty Images

Gen. Michael Hayden, nominated by President Bush to become the director of the CIA, headed the NSA from March 1999 to April 2005. In that post, Hayden would have overseen the agency's domestic phone record collection program.

By Leslie Cauley, USA TODAY

The National Security Agency has been secretly collecting the phone call records of tens of millions of Americans, using data provided by AT&T, Verizon and BellSouth, people with direct knowledge of the arrangement told USA TODAY.

The NSA program 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. This program does not involve the NSA listening to or recording conversations. But the spy agency is using the data to analyze calling patterns in an effort to detect terrorist activity, sources said in separate interviews.

**QUESTIONS AND ANSWERS:** The NSA record collection program

"It's the largest database ever assembled in the world," said one person, who, like the others who agreed to talk about the NSA's activities, declined to be identified by name or affiliation. The agency's goal is "to create a database of every call ever made" within the nation's borders, this person added.

For the customers of these companies, it means that the government has detailed records of calls they made — across town or across the country — to family members, co-workers, business contacts and others.

The three telecommunications companies are working under contract with the NSA, which launched the program in 2001 shortly after the Sept. 11 terrorist attacks, the sources said. The program is aimed at identifying and tracking suspected terrorists, they said.

The sources would talk only under a guarantee of anonymity

## REACTION

### From the White House:

The White House defended its overall eavesdropping program and said no domestic surveillance is conducted without court approval.

"The intelligence activities undertaken by the United States government are lawful, necessary and required to protect Americans from terrorist attacks," said Dana Perino, the deputy White House press secretary, who added that appropriate members of Congress have been briefed on intelligence activities.

### From Capitol Hill:

Sen. Arlen Specter, R-Pa., the chairman of the Senate Judiciary Committee, said he would call the phone companies to appear before the panel "to find out exactly what is going on."

Sen. Patrick Leahy of Vermont, the ranking

E-m:

E-r  
Sig  
nev  
yot

E-r

Sel  
Bre  
Ge

Democrat on the panel, sounded incredulous about the latest report and railed against what he called a lack of congressional oversight. He argued that the media was doing the job of Congress.

"Are you telling me that tens of millions of Americans are involved with al Qaeda?" Leahy asked. "These are tens of millions of Americans who are not suspected of anything ... Where does it stop?"

The Democrat, who at one point held up a copy of the newspaper, added: "Shame on us for being so far behind and being so willing to rubber stamp anything this administration does. We ought to fold our tents."

The report came as the former NSA director, Gen. Michael Hayden - Bush's choice to take over leadership of the CIA - had been scheduled to visit lawmakers on Capitol Hill Thursday. However, the meetings with Republican Sens. Rick Santorum of Pennsylvania and Lisa Murkowski of Alaska were postponed at the request of the White House, said congressional aides in the two Senate offices.

Source: *The Associated Press*

because the NSA program is secret.

Air Force Gen. Michael Hayden, nominated Monday by President Bush to become the director of the CIA, headed the NSA from March 1999 to April 2005. In that post, Hayden would have overseen the agency's domestic call-tracking program. Hayden declined to comment about the program.

The NSA's domestic program, as described by sources, is far more expansive than what the White House has acknowledged. Last year, Bush said he had authorized the NSA to eavesdrop — without warrants — on international calls and international e-mails of people suspected of having links to terrorists when one party to the communication is in the USA. Warrants have also not been used in the NSA's efforts to create a national call database.

In defending the previously disclosed program, Bush insisted that the NSA was focused exclusively on international calls. "In other words," Bush explained, "one end of the communication must be outside the United States."

As a result, domestic call records — those of calls that originate and terminate within U.S. borders — were believed to be private.

Sources, however, say that is not the case. With access to records of billions of domestic calls, the NSA has gained a secret window into the communications habits of millions of Americans. Customers' names, street addresses and other personal information are not being handed over as part of NSA's domestic program, the sources said. But the phone numbers the NSA collects can easily be cross-checked with other databases to obtain that information.

Don Weber, a senior spokesman for the NSA, declined to discuss the agency's operations. "Given the nature of the work we do, it would be irresponsible to comment on actual or alleged operational issues; therefore, we have no information to provide," he said. "However, it is important to note that NSA takes its legal responsibilities seriously and operates within the law."

The White House would not discuss the domestic call-tracking program. "There is no domestic surveillance without court approval," said Dana Perino, deputy press secretary, referring to actual eavesdropping.

She added that all national intelligence activities undertaken by the federal government "are lawful, necessary and required for the pursuit of al-Qaeda and affiliated terrorists." All government-sponsored intelligence activities "are carefully reviewed and monitored," Perino said. She also noted that "all appropriate members of Congress have been briefed on the intelligence efforts of the United States."

The government is collecting "external" data on domestic phone

### NSA SURVEILLANCE

**Opinion:** Congress in the dark | Specter: My bill would provide light



ACLU, NSA to head to court

VP pressured panel, Specter says



Senators won't grill phone companies

FCC: NSA probe impossible

Pre-9/11 records help flag suspicious calling



More

### TIMELINE

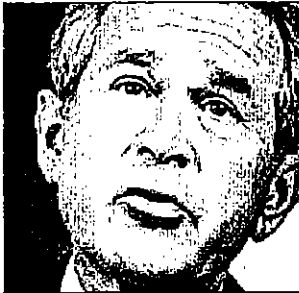


Key events in the NSA domestic spying story:

Select for details

MAY 11

As Democrats and Republicans criticize the secret phone call database program disclosed by USA TODAY, Bush says the government is not "mining or trolling through the personal lives of millions of innocent Americans."



By Ron Edmonds, AP  
President: Bush

Sources: The Associated Press; USA TODAY archives; The New York Times

By Anne R. Carey and Ron Coddington, USA TODAY

calls but is not intercepting "internals," a term for the actual content of the communication, according to a U.S. intelligence official familiar with the program. This kind of data collection from phone companies is not uncommon; it's been done before, though never on this large a scale, the official said. The data are used for "social network analysis," the official said, meaning to study how terrorist networks contact each other and how they are tied together.

### Carriers uniquely positioned

AT&T recently merged with SBC and kept the AT&T name. Verizon, BellSouth and AT&T are the nation's three biggest telecommunications companies; they provide local and wireless phone service to more than 200 million customers.

The three carriers control vast networks with the latest communications technologies. They provide an array of services: local and long-distance calling, wireless and high-speed broadband, including video. Their direct access to millions of homes and businesses has them uniquely positioned to help the government keep tabs on the calling habits of Americans.

Among the big telecommunications companies, only Qwest has refused to help the NSA, the sources said. According to multiple sources, Qwest declined to participate because it was uneasy about the legal implications of handing over customer information to the government without warrants.

Qwest's refusal to participate has left the NSA with a hole in its database. Based in Denver, Qwest provides local phone service to 14 million customers in 14 states in the West and Northwest. But AT&T and Verizon also provide some services — primarily long-distance and wireless — to people who live in Qwest's region. Therefore, they can provide the NSA with at least some access in that area.

Created by President Truman in 1952, during the Korean War, the NSA is charged with protecting the United States from foreign security threats. The agency was considered so secret that for years the government refused to even confirm its existence. Government insiders used to joke that NSA stood for "No Such Agency."

In 1975, a congressional investigation revealed that the NSA had been intercepting, without warrants, international communications for more than 20 years at the behest of the CIA and other agencies. The spy campaign, code-named "Shamrock," led to the Foreign Intelligence Surveillance Act (FISA), which was designed to protect Americans from illegal eavesdropping.

Enacted in 1978, FISA lays out procedures that the U.S. government must follow to conduct electronic surveillance and physical searches of people believed to be engaged in espionage or international terrorism against the United States. A special court, which has 11 members, is responsible for

## OFFICIAL WORDS ON SURVEILLANCE

Bush administration officials have said repeatedly that the warrantless surveillance program authorized by President Bush after the Sept. 11 terrorist attacks is carefully targeted to include only international calls and e-mails into or out of the USA, and only those that involve at least one party suspected of being a member or ally of al-Qaeda or a related terror group.

Some comments related to what the administration calls the "Terrorist Surveillance Program," and surveillance in general:

Gen. Michael Hayden, principal deputy director of national intelligence, and now Bush's nominee to head the CIA, at the National Press Club, Jan. 23, 2006:

"The program ... is not a drift net over (U.S. cities such as) Dearborn or Lackawanna or Fremont, grabbing conversations that we then sort out by these alleged keyword searches or data-mining tools or other devices that so-called experts keep talking about.

"This is targeted and focused. This is not about intercepting conversations between people in the United States. This is not pursuit of communications entering or leaving America involving someone we believe is associated with al-Qaeda. ... This is focused. It's targeted. It's very carefully done. You shouldn't worry."

Senate Judiciary Committee hearing, Feb. 6, 2006:

**Attorney General Alberto Gonzales:** "Only international communications are authorized for interception under this program. That is, communications between a foreign country and this country. ..."

"To protect the privacy of Americans still further, the NSA employs safeguards to minimize the unnecessary collection and dissemination of information about U.S. persons."

**Sen. Joseph Biden, D-Del.:** "I don't understand why you would limit your eavesdropping only to foreign conversations. ..."

**Gonzales:** "I believe it's because of trying to balance concerns that might arise that, in fact, the NSA was engaged in electronic surveillance with respect to domestic calls."

adjudicating requests under FISA.

Over the years, NSA code-cracking techniques have continued to improve along with technology. The agency today is considered expert in the practice of "data mining" — sifting through reams of information in search of patterns. Data mining is just one of many tools NSA analysts and mathematicians use to crack codes and track international communications.

Paul Butler, a former U.S. prosecutor who specialized in terrorism crimes, said FISA approval generally isn't necessary for government data-mining operations. "FISA does not prohibit the government from doing data mining," said Butler, now a partner with the law firm Akin Gump Strauss Hauer & Feld in Washington, D.C.

The caveat, he said, is that "personal identifiers" — such as names, Social Security numbers and street addresses — can't be included as part of the search. "That requires an additional level of probable cause," he said.

The usefulness of the NSA's domestic phone-call database as a counterterrorism tool is unclear. Also unclear is whether the database has been used for other purposes.

The NSA's domestic program raises legal questions. Historically, AT&T and the regional phone companies have required law enforcement agencies to present a court order before they would even consider turning over a customer's calling data. Part of that owed to the personality of the old Bell

Telephone System, out of which those companies grew.

Ma Bell's bedrock principle — protection of the customer — guided the company for decades, said Gene Kimmelman, senior public policy director of Consumers Union. "No court order, no customer information — period. That's how it was for decades," he said.

The concern for the customer was also based on law: Under Section 222 of the Communications Act, first passed in 1934, telephone companies are prohibited from giving out information regarding their customers' calling habits: whom a person calls, how often and what routes those calls take to reach their final destination. Inbound calls, as well as wireless calls, also are covered.

The financial penalties for violating Section 222, one of many privacy reinforcements that have been added to the law over the years, can be stiff. The Federal Communications Commission, the nation's top telecommunications regulatory agency, can levy fines of up to \$130,000 per day per violation, with a cap of \$1.325 million per violation. The FCC has no hard definition of "violation." In practice, that means a single "violation" could cover one customer or 1 million.

In the case of the NSA's international call-tracking program, Bush signed an executive order allowing the NSA to engage in eavesdropping without a warrant. The president and his representatives have since argued that an executive order was sufficient for the agency to proceed. Some civil liberties groups, including the American Civil Liberties Union, disagree.

### Companies approached

The NSA's domestic program began soon after the Sept. 11 attacks, according to the sources. Right around that time, they said, NSA representatives approached the nation's biggest telecommunications companies. The agency made an urgent pitch: National security is at risk, and we need your help to protect the country from attacks.

The agency told the companies that it wanted them to turn over their "call-detail records," a complete listing of the calling histories of their millions of customers. In addition, the NSA wanted the carriers to provide updates, which would enable the agency to keep tabs on the nation's calling habits.

The sources said the NSA made clear that it was willing to pay for the cooperation. AT&T, which at the time was headed by C. Michael Armstrong, agreed to help the NSA. So did BellSouth, headed by F. Duane Ackerman; SBC, headed by Ed Whitacre; and Verizon, headed by Ivan Seidenberg.

With that, the NSA's domestic program began in earnest.

AT&T, when asked about the program, replied with a comment prepared for USA TODAY: "We do not comment on matters of national security, except to say that we only assist law enforcement and government agencies charged with protecting national security in strict accordance with the law."

In another prepared comment, BellSouth said: "BellSouth does not provide any confidential customer information to the NSA or any governmental agency without proper legal authority."

Verizon, the USA's No. 2 telecommunications company behind AT&T, gave this statement: "We do not comment on national security matters, we act in full compliance with the law and we are committed to safeguarding our customers' privacy."

Qwest spokesman Robert Charlton said: "We can't talk about this. It's a classified situation."

In December, *The New York Times* revealed that Bush had authorized the NSA to wiretap, without warrants, international phone calls and e-mails that travel to or from the USA. The following month, the Electronic Frontier Foundation, a civil liberties group, filed a class-action lawsuit against AT&T. The lawsuit accuses the company of helping the NSA spy on U.S. phone customers.

Last month, U.S. Attorney General Alberto Gonzales alluded to that possibility. Appearing at a House Judiciary Committee hearing, Gonzales was asked whether he thought the White House has the legal authority to monitor domestic traffic without a warrant. Gonzales' reply: "I wouldn't rule it out." His comment marked the first time a Bush appointee publicly asserted that the White House might have that authority.

### **Similarities in programs**

The domestic and international call-tracking programs have things in common, according to the sources. Both are being conducted without warrants and without the approval of the FISA court. The Bush administration has argued that FISA's procedures are too slow in some cases. Officials, including Gonzales, also make the case that the USA Patriot Act gives them broad authority to protect the safety of the nation's citizens.

The chairman of the Senate Intelligence Committee, Sen. Pat Roberts, R-Kan., would not confirm the existence of the program. In a statement, he said, "I can say generally, however, that our subcommittee has been fully briefed on all aspects of the Terrorist Surveillance Program. ... I remain convinced that the program authorized by the president is lawful and absolutely necessary to protect this nation from future attacks."

The chairman of the House Intelligence Committee, Rep. Pete Hoekstra, R-Mich., declined to comment.

### **One company differs**

One major telecommunications company declined to participate in the program: Qwest.

According to sources familiar with the events, Qwest's CEO at the time, Joe Nacchio, was deeply troubled by the NSA's assertion that Qwest didn't need a court order — or approval under FISA — to proceed. Adding to the tension, Qwest was unclear about who, exactly, would have access to its customers' information and how that information might be used.

Financial implications were also a concern, the sources said. Carriers that illegally divulge calling information can be subjected to heavy fines. The NSA was asking Qwest to turn over millions of records. The fines, in the aggregate, could have been substantial.

The NSA told Qwest that other government agencies, including the FBI, CIA and DEA, also might have access to the database, the sources said. As a matter of practice, the NSA regularly shares its information — known as "product" in intelligence circles — with other intelligence groups. Even so, Qwest's lawyers were troubled by the expansiveness of the NSA request, the sources said.

The NSA, which needed Qwest's participation to completely cover the country, pushed back hard.

Trying to put pressure on Qwest, NSA representatives pointedly told Qwest that it was the lone holdout among the big telecommunications companies. It also tried appealing to Qwest's patriotic side: In one meeting, an NSA representative suggested that Qwest's refusal to contribute to the database could compromise national security, one person recalled.

In addition, the agency suggested that Qwest's foot-dragging might affect its ability to get future classified work with the government. Like other big telecommunications companies, Qwest already had classified contracts and hoped to get more.

Unable to get comfortable with what NSA was proposing, Qwest's lawyers asked NSA to take its proposal to the FISA court. According to the sources, the agency refused.

The NSA's explanation did little to satisfy Qwest's lawyers. "They told (Qwest) they didn't want to do that because FISA might not agree with them," one person recalled. For similar reasons, this person said, NSA rejected Qwest's suggestion of getting a letter of authorization from the U.S. attorney general's office. A second person confirmed this version of events.


In June 2002, Nacchio resigned amid allegations that he had misled investors about Qwest's financial health. But Qwest's legal questions about the NSA request remained.

Unable to reach agreement, Nacchio's successor, Richard Notebaert, finally pulled the plug on the NSA talks in late 2004, the sources said.

*Contributing: John Diamond*

Posted 5/10/2006 11:16 PM ET

Updated 5/11/2006 10:38 AM ET

E-mail | Save | Print | Reprints & Permissions | Subscribe to stories like this 

---

### Related Advertising Links

[What's this?](#)

#### Calculate Your New Mortgage Payment

\$310K loan for under \$998/mo. Think you pay too much? Refi now.  
[www.lowermybills.com](http://www.lowermybills.com)

#### Scottrade Online Broker

\$7 online trades. Fast, accurate executions. 285+ offices nationwide.  
[www.scottrade.com](http://www.scottrade.com)

#### Mortgage Rates Near 40-yr Lows

As featured on Oprah.com - Compare free quotes & calculate new payment.  
[www.lowermybills.com](http://www.lowermybills.com)

[Get listed here](#)

Advertisement

# **EXHIBIT L**



Online NewsHour

REGION: North America  
TOPIC: Law

TRANSCRIPT

Originally Aired: May 11, 2006

Debate

## NSA Wire Tapping Program Revealed

An article in Thursday's USA Today reported that three of the largest U.S. phone companies have been providing the National Security Agency with phone records from millions of Americans since 9/11. Two senators discuss the program's legal and security issues now that the public is aware of it.



RealAudio | Download | Streaming Video

SEN. PATRICK LEAHY, D-Vt.: Look at this headline.

KWAME HOLMAN: Only hours after it appeared in print, the story that the National Security Agency secretly has been gathering a giant database of phone records set off a firestorm on Capitol Hill. Vermont Democrat Patrick Leahy was visibly angry about it and lashed out at the Bush administration at a Senate Judiciary Committee meeting scheduled to discuss judicial nominations.

SEN. PATRICK LEAHY: Only through the press, we begin to learn the truth. The secret collection of phone call records tens of millions of Americans. Now, are you telling me that tens of millions of Americans are involved with al-Qaida? If that's the case, we've really failed in any kind of a war on terror.

KWAME HOLMAN: Arizona Republican Jon Kyl responded.

SEN. JON KYL, R-Ariz.: This is nuts. We are in a war, and we've got to collect intelligence on enemy, and you can't tell the enemy in advance how you're going to do it.

KWAME HOLMAN: Emblazoned across the front page of USA Today, the lengthy report said the code-breaking National Security Agency contracted three of the nation's largest phone companies to provide records of home and business telephone calls made by their customers.

The NSA earlier was revealed to have been monitoring, without warrants, international phone calls and e-mails thought to be linked to terrorists.

USA Today telecommunications reporter Leslie Cauley spent the last several months preparing today's story.

LESLIE CAULEY, USA Today: The NSA is collecting the call detail records of millions of ordinary Americans.

KWAME HOLMAN: The companies reportedly contracted by the spy agency are AT&T, Bell South and Verizon.

LESLIE CAULEY: The pitch to the phone companies was: We feel this information can be very helpful in smoking out, you know, and tracking suspected terrorists. And, again, three out of the four agreed.

KWAME HOLMAN: But Qwest, a telecommunications company that provides local phone service to 14 million customers in 14 western and northwestern states, reportedly refused to participate.

All of the telephone companies that worked with the agency refused to comment on specifics, saying only that they are assisting the government in accordance with the law.

Judiciary Committee Chairman Arlen Specter, who had voiced earlier concerns about the NSA surveillance program, this morning said he wanted to bring the phone company officials before his panel.

SEN. ARLEN SPECTER, R-Pa., Judiciary Committee Chairman: We're going to call on those telephone companies to provide information to try to figure out exactly what is going on.

KWAME HOLMAN: According to the USA Today report, this NSA program does not involve the listening to or recording of calls.

LESLIE CAULEY: This program is referring to in-country calls only, meaning calls that originate and terminate within U.S. borders. There is no eavesdropping as part of this particular program.

KWAME HOLMAN: Alabama Republican Jeff Sessions.

SEN. JEFF SESSIONS, R-Ala.: But it is not a warrantless wiretapping of the American people. And I don't think this action is nearly as troublesome as being made out here.

KWAME HOLMAN: But on the House side, Majority Leader John Boehner said the report was troubling.

REP. JOHN BOEHNER, R-Ohio, House Majority Leader: I am concerned about what I read, with regard to the NSA database of phone calls. I don't know enough about the details, except that I'm going to find out, because I am not sure why it would be necessary for us to keep and have that kind of information.

KWAME HOLMAN: The report came out as former NSA Director General Michael Hayden, who President Bush nominated this week to be the CIA's new director, was scheduled for another round of meetings with congressional members. Hayden spoke after meeting with the Senate's number-two Republican, Mitch McConnell, this afternoon.

GEN. MICHAEL HAYDEN, CIA Director-Designate: All I would want to say is that everything that NSA does is lawful and very carefully done, and that the appropriate members of the Congress -- House and Senate -- are briefed on all NSA activities. And I think I'd just leave it at that.

KWAME HOLMAN: California Democrat Dianne Feinstein said that, as a result of today's revelations, Hayden would have an uphill battle seeking confirmation.

SEN. DIANNE FEINSTEIN, D-Calif.: I happen to believe we're on our way to a major constitutional confrontation on Fourth Amendment guarantees of unreasonable search and seizure. And I think this is also going to be present a growing impediment to the confirmation of General Hayden, and I think that is very regretted.

KWAME HOLMAN: The Senate Intelligence Committee is expected to open Hayden's



confirmation hearings a week from today.

## The President Speaks Out

JIM LEHRER: As the story gained momentum this morning, President Bush made a statement at the White House. And here it is in full.

PRESIDENT GEORGE W. BUSH: After September the 11th, I vowed to the American people that our government would do everything within the law to protect them against another terrorist attack.

As part of this effort, I authorized the National Security Agency to intercept the international communications of people with known links to al-Qaida and related terrorist organizations. In other words, if al-Qaida or their associates are making calls into the United States or out of the United States, we want to know what they're saying.



George W. Bush

Today, there are new claims about other ways we are tracking down the al-Qaida to prevent attacks on America. I want to make some important points about what the government is doing and what the government is not doing.

First, our intelligence activities strictly target al-Qaida and their known affiliates. Al-Qaida is our enemy, and we want to know their plans.

Second, the government does not listen to domestic phone calls without court approval.

Third, the intelligence activities I authorized are lawful and have been briefed to appropriate members of Congress, both Republican and Democrat.

Fourth, the privacy of ordinary Americans is fiercely protected in all our activities. We're not mining or trolling through the personal lives of millions of innocent Americans. Our efforts are focused on links to al-Qaida and their known affiliates.

So far, we've been very successful in preventing another attack on our soil. As a general matter, every time sensitive intelligence is leaked, it hurts our ability to defeat this enemy.

Our most important job is to protect the American people from another attack, and we will do so within the laws of our country.

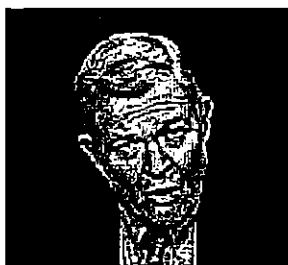
Thank you.

## Crossing the Line?

JIM LEHRER: More on this now from Sen. Kit Bond, a Republican of Missouri, a member of the Senate Intelligence Committee, and Sen. Patrick Leahy of Vermont, the senior Democrat on the Senate Judiciary Committee.

Senator Leahy, did the president's statement resolve your concerns about this?

SEN. PATRICK LEAHY, D-Vt.: No, and I'll tell you why. I think the president was probably wise and well-advised to give the statement he did, but we have a major credibility issue.



Senator Kit Bond  
(R) Missouri

Regrettably, since December, when word started coming out about the president's program, and terrorists have learned about what is going on, and it makes us less safe. The more we talk about it, the less safe we are.

Every time something new comes out in the press, we hear from the White House: Well, well, we've either just told you about that, or we're going to tell you about it.

And then we find nobody was told fully about it, as Jay Rockefeller, the vice chairman of the Senate Intelligence Committee said today.

I wonder what they're doing, so that you can know whether it's legal or not. All of us want to fight terrorists. The 9/11 happened on this administration's watch; they don't want it to happen again, but I don't want it to happen again. No American does.

We want to make sure that we're not just talking about being safe, but we are being safe. If we're going and running lines on every single phone call in this country, I wonder just what that does. They should come and explain.

First, I want to know if they're breaking the law. If they don't want to follow the law, then come to us and ask us to change the law.

I mean, these are the people that have a list now -- a terrorist watch list of 320,000 people. They say that makes it safe -- makes it safer. Well, on that list is Senator Edward Kennedy of Massachusetts -- he was unable to get on a plane -- a nine-month old baby, a nun, and on, and on, and on. Mistakes happen if things are not done right.

JIM LEHRER: Senator Bond, how do you respond to that, that -- you're a member -- first of all, let me ask you directly. You're a member of the Senate Intelligence Committee. Did you know about this?

SEN. KIT BOND, R-Mo.: Yes. I'm a member of the subcommittee of the Intelligence Committee that's been thoroughly briefed on this program and other programs.

And the first point I would make is every time we have a leak of classified information like this, it makes us significantly less safe. Regrettably, since December, when word started coming out about the president's program, and terrorists have learned about what is going on, and it makes us less safe. The more we talk about it, the less safe we are.

Now, to move on to the points, number one, my colleague, Senator Leahy, is a good lawyer, and I believe that he knows, as any lawyer should know, that business records are not protected by the Fourth Amendment.

The case of Smith v. Maryland in 1979, the U.S. Supreme Court said that the government could continue to use phone records, who called from where to where, at what time, for what length, for intelligence and criminal investigations without a warrant.

This has been going on, and this has been gone on long before the president's program started. And the president's program, as he designed, as he explained it, has been designed, and is carefully monitored by the lawyers from the NSA and the Department of Justice to make sure that they target telephone communications from or to overseas al-Qaida or al-Qaida known affiliates.

And this program has given us significant leads and allowed us to identify terrorists and to break up planned plots in the United States. Telephone calls from domestic to domestic-foreign phone calls are not targeted, are not used -- their content is not used -- unless there is a court order.

SEN. PATRICK LEAHY: If I could just...

JIM LEHRER: Excuse me, Senator Leahy, and let me just ask just one follow-up question to Senator Bond so we understand what this is about.

What these are, are records. And nobody then -- now, these are -- but there are tens of millions of records that are in this database, right? And they say somebody, Billy Bob called Sammy Sue or whatever, and that's all it says, and then they go and try to match them with other people?

SEN. KIT BOND: First, let me say that I'm not commenting on in any way any of the allegations made in the news story today. I can tell you about the president's program.

The president's program uses information collected from phone companies. The phone companies keep their records. They have a record. And it shows what telephone number called what other telephone number.

Now, if it's domestic to domestic, they are not targeting -- they're not going after that. What they are looking at are telephone calls coming into our going out of the United States to known al-Qaida phones or their people.

JIM LEHRER: OK.

SEN. KIT BOND: That's what the program focuses on. The government has, in the past, and could look at all of the records of purely domestic phone calls; that's not the purpose of this program.

## **The Price for Safety**

JIM LEHRER: All right. Now, Senator Leahy, as described by Senator Bond, does that strike you as being legal?

SEN. PATRICK LEAHY: No, and I'll tell you why: The Maryland case, in 1979 -- Kit Bond was former attorney general and is a very good lawyer. He's absolutely right. That would have allowed it.

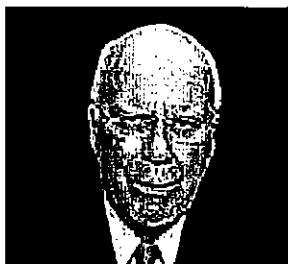
Since then, however, we passed several laws. We passed the so-called CALEA, ECPA, FISA, and the Patriot Act. And we make it very specific in those what you can do and can not do.

As this was described today, I'm hard-pressed -- and most lawyers are hard-pressed -- to say what exception this would fall under one of these laws; it doesn't. And there is a strong question of legality.

When Attorney General Gonzales basically stonewalled the Senate Judiciary Committee, but did admit that there may be domestic wiretapping going on. I would say what the vice chairman of the Senate Intelligence Committee said today. He said: Significant questions remain surrounding the legality of the program and whether the White House has misrepresented the program to the public, through the selective declassification.

He's seen everything that's been shown to...

JIM LEHRER: That's Senator Rockefeller you're talking about?



Sen. Patrick Leahy  
(D) Vermont

The president has more times than all presidents put together in history, through signing statements, that said he will follow only parts of the law that he signs.

SEN. PATRICK LEAHY: I'm talking about Senator Rockefeller. But the point is that we haven't done adequate oversight.

Unfortunately, the Congress has acted like a wholly-owned subsidiary of the White House and has rubber-stamped everything that's gone on. And then we usually find out through the press, whoops, they weren't following the law.

Let's go through. Let's find out what parts of the law is being followed, what part's not being followed. The president has more times than all presidents put together in history, through signing statements, that said he will follow only parts of the law that he signs.

Let's get this on the record for the American people. We can make ourselves safe, but it's not enough to say, "Gee, we're doing a great job." That's sort of like telling the head of FEMA, "Brownie, you've done a heck of a job."

JIM LEHRER: Senator Bond, do you...

SEN. KIT BOND: Let me correct a number of things.

JIM LEHRER: OK.

SEN. KIT BOND: First, every time we get something on the record, we are making our country less safe. We have classified information because intelligence is only useful when it is kept out of the knowledge of the terrorists that we're trying to intercept. So every time we talk more about it, then they know more about how to avoid it.

Number two, unfortunately, the vice chairman has been sick and has missed, I think, three in-depth hearings we've had to learn more about the program. He and all of the members of the subcommittee are fully encouraged to ask all of the questions. We have asked those questions.

I've visited NSA. I have seen the steps that they take to make sure the law is followed.

Now, as for the law, the Maryland case, the Smith v. Maryland case, said business records are not protected by the Fourth Amendment. You don't have to get a search warrant.

And the other thing is the FISA court, the court of review in Enray Seal case [ph], said the president has the constitutional authority to conduct foreign intelligence surveillance, what this is, and they said, if the statute limits that ability, it is probably unconstitutional.

JIM LEHRER: Senator Bond, would you have any objection to what Senator Leahy is proposing here, though, that it all be laid out on the table at a -- you're talking about a public hearing, Senator Leahy?

SEN. PATRICK LEAHY: No, I'm asking having the appropriate people of the clearance look at it first, what's going on. Then, we have to make a determination whether it's legal. You know, simply because something is classified doesn't make it legal.

JIM LEHRER: But you're not saying...

SEN. PATRICK LEAHY: Our torture program was classified, didn't make it legal.

JIM LEHRER: But you're not satisfied with what Senator Bond and others have said, that the key members of the Senate Intelligence Committee have been briefed on that. You're suggesting there should be something beyond that, Senator Leahy?

SEN. PATRICK LEAHY: Well, you had a cut on here earlier of Senator Feinstein, who is one of those who's been briefed on it, and she obviously is not satisfied with the legality of this. She is a supporter -- has been a supporter of General Hayden, and she's the one that raised the question, because of this, his own confirmation may be in trouble.

SEN. KIT BOND: Let me answer a couple of things. Number one, General Hayden was not the one who ordered the program. General Hayden is not the one who cleared it. It's the lawyers at the Department of Justice. General Hayden carried out the orders pursuant to the directions of the lawyers.

And I'll be happy to discuss with members of the Intelligence Committee the appropriate laws. And, for a non-lawyer, these areas are very confusing, but they have walked me through this.

Number one, the records, phone records are not personal records. They are not entitled to the Fourth Amendment protections.

The president has the foreign intelligence surveillance powers; that's what they're using. I could cite cases...

JIM LEHRER: Sure.

SEN. KIT BOND: ... and I will do it, in the classified hearings. But the more we talk about it in public, the more our country is in danger. And we are much more likely to have a terrorist attack since the discussion of this program has begun.

## **Putting the Nation at Risk**

JIM LEHRER: That's what I wanted to ask Senator Leahy. I wanted to -- Senator Leahy, what about Senator Bond's point? He's made this two or three times now that just talking about this, the public disclosure in the USA Today, and I guess even the discussion we're having now, is endangering U.S. security?

SEN. PATRICK LEAHY: If anybody thinks that Osama bin Laden, a man who was able to mastermind an attack on us, thinks that we're trying to tap his phone, then they're crazy.

I mean, I was a prosecutor. I got search warrants. I knew how to go after, and I made darn sure that people didn't know exactly what you were doing. We can do that.

But simply saying we're making it safer doesn't mean we're making it...

JIM LEHRER: But he's saying just the opposite. He's saying this is making it un-safer, the public disclosure.

SEN. PATRICK LEAHY: We have so many things that neither Senator Bond or I would talk about here they've done all the time that are perfectly legal, perfectly proper. None of them have been disclosed. They do make us safer.



**Jim Lehrer**  
Executive Editor and  
Anchor

I just want to make sure that we do not set precedence that removes the privacy of normal, law-abiding Americans. And I think that's why Senator Specter, Republican chairman of the Judiciary Committee, is calling these telephone companies to say: Under what law are you acting?

JIM LEHRER: Senator Bond, do you oppose that? Do you think that's a bad idea, to have phone companies come to the Senate Judiciary Committee?

SEN. KIT BOND: That's a very bad idea, to have a public hearing. And, unfortunately, I've not had the opportunity to discuss the laws with -- and apparently Senator Specter has not been briefed on the program.

What the president said is correct. Number one, that we meticulously -- they meticulously keep the privacy of American citizens protected to the fullest extent of the law.

Number two, Porter Goss, the former director of the Central Intelligence Agency, in response to my question in a public forum in February, said our ability to collect intelligence is very severely damaged, very severely damaged by the leaks. That's what the president said today, and he was correct.

And, by the way, torture has never been tolerated, and the people who engaged in those malicious acts in Abu Ghraib have been punished, and it is incumbent that we punish anybody who violates the law.

SEN. PATRICK LEAHY: And the official policy either was changed once it became...

JIM LEHRER: We're not going -- gentlemen, we're not going there tonight. Thank you both very much.

SEN. PATRICK LEAHY: Thanks, Jim.

SEN. KIT BOND: Thanks.

Funded, in part, by:



Support the kind of journalism done by the NewsHour...Become a member of your local PBS station.

PBS Online Privacy Policy

Copyright ©1996-2006 MacNeil/Lehrer Productions. All Rights Reserved.

# **EXHIBIT M**





[About Us](#) [Search](#)

[RESIDENTIAL](#) [SMALL BUSINESS](#) [MEDIUM BUSINESS](#) [LARGE BUSINESS](#) [WIRELES](#)

[News Center Main Page](#)

[News Archive](#)

[Media Contacts](#)

[Press Kits](#)

[Executive Center](#)

[Video & Image Feed](#)

## News Release

### Verizon Issues Statement on NSA and Privacy Protection

May 12, 2006

**Media Contact:**  
[Peter Thonis](#), 212-395-2355

**NEW YORK --** *Verizon Communications Inc. (NYSE:VZ) today issued the following statement:*

The President has referred to an NSA program, which he authorized, directed against al-Qaeda. Because that program is highly classified, Verizon cannot comment on that program, nor can we confirm or deny whether we have had any relationship to it.

Having said that, there have been factual errors in press coverage about the way Verizon handles customer information in general. Verizon puts the interests of our customers first and has a longstanding commitment to vigorously safeguard our customers' privacy -- a commitment we've highlighted in our privacy principles, which are available at [www.verizon.com/privacy](http://www.verizon.com/privacy).

Verizon will provide customer information to a government agency only where authorized by law for appropriately-defined and focused purposes. When information is provided, Verizon seeks to ensure it is properly used for that purpose and is subject to appropriate safeguards against improper use. Verizon does not, and will not, provide any government agency unfettered access to our customer records or provide information to the government under circumstances that would allow a fishing expedition.

In January 2006, Verizon acquired MCI, and we are ensuring that Verizon's policies are implemented at that entity and that all its activities fully comply with law.

Verizon hopes that the Administration and the Congress can come together and agree on a process in an appropriate setting, and with safeguards for protecting classified information, to examine any issues that have been raised about the program. Verizon is fully prepared to participate in such a process.

####

Register for news delivered e-mail

RSS Feed: Click here for available RSS feeds  
Verizon press releases

En español: Click here to view the News Center in Spanish.

[Contact Us](#) | [Careers](#) | [Our Stores](#) | [Site Map](#) | [Privacy Policy](#) | © 2007 Verizon

# EXHIBIT N



May 12, 2006 11:08 a.m. EDT

## Full Statement From Attorney Of Former Qwest CEO Nacchio

May 12, 2006 11:08 a.m.

*Full text of the statement of Herbert J. Stern, attorney for former Qwest Communications International Inc. Chief Executive Joseph N. Nacchio*

In light of pending litigation, I have been reluctant to issue any public statements. However, because of apparent confusion concerning Joe Nacchio and his role in refusing to make private telephone records of Qwest customers available to the NSA immediately following the Patriot Act, and in order to negate misguided attempts to relate Mr. Nacchio's conduct to present litigation, the following are the facts.

In the Fall of 2001, at a time when there was no investigation of Qwest or Mr. Nacchio by the Department of Justice or the Securities Exchange Commission, and while Mr. Nacchio was Chairman and CEO of Qwest and was serving pursuant to the President's appointment as the Chairman of the National Security Telecommunications Advisory Committee, Qwest was approached to permit the Government access to the private telephone records of Qwest customers.


Mr. Nacchio made inquiry as to whether a warrant or other legal process had been secured in support of that request. When he learned that no such authority had been granted and that there was a disinclination on the part of the authorities to use any legal process, including the Special Court which had been established to handle such matters, Mr. Nacchio concluded that these requests violated the privacy requirements of the Telecommunications Act. Accordingly, Mr. Nacchio issued instructions to refuse to comply with these requests. These requests continued throughout Mr. Nacchio's tenure and until his departure in June of 2002.

URL for this article:  
<http://online.wsj.com/article/SB114744615734351338.html>

Copyright 2007 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our **Subscriber Agreement** and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit [www.djreprints.com](http://www.djreprints.com).

### DOW JONES REPRINTS

 This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit: [www.djreprints.com](http://www.djreprints.com).

- See a sample reprint in PDF format.
- Order a reprint of this article now.

# **EXHIBIT O**

2 of 2 DOCUMENTS

Copyright 2006 The New York Times Company  
The New York Times

May 13, 2006 Saturday  
Late Edition - Final

**SECTION:** Section A; Column 6; National Desk; Pg. 1

**LENGTH:** 1398 words

**HEADLINE:** QUESTIONS RAISED FOR PHONE GIANTS IN SPY DATA FUROR

**BYLINE:** By JOHN MARKOFF; Reporting for this article was contributed by Ken Belson, Brenda Goodman, Stephen Labaton, Matt Richtel and Katie Zezima.

**BODY:**

The former chief executive of Qwest, the nation's fourth-largest phone company, rebuffed government requests for the company's calling records after 9/11 because of "a disinclination on the part of the authorities to use any legal process," his lawyer said yesterday.

The statement on behalf of the former Qwest executive, Joseph P. Nacchio, followed a report that the other big phone companies -- AT&T, BellSouth and Verizon -- had complied with an effort by the National Security Agency to build a vast database of calling records, without warrants, to increase its surveillance capabilities after the Sept. 11 attacks.

Those companies insisted yesterday that they were vigilant about their customers' privacy, but did not directly address their cooperation with the government effort, which was reported on Thursday by USA Today. Verizon said that it provided customer information to a government agency "only where authorized by law for appropriately defined and focused purposes," but that it could not comment on any relationship with a national security program that was "highly classified."

Legal experts said the companies faced the prospect of lawsuits seeking billions of dollars in damages over cooperation in the program, citing communications privacy legislation stretching back to the 1930's. A federal lawsuit was filed in Manhattan yesterday seeking as much as \$50 billion in civil damages against Verizon on behalf of its subscribers.

For a second day, there was political fallout on Capitol Hill, where Senate Democrats intend to use next week's confirmation hearings for a new C.I.A. director to press the Bush administration on its broad surveillance programs. [Page A13.]

As senior lawmakers in Washington vowed to examine the phone database operation and possibly issue subpoenas to the telephone companies, executives at some of the companies said they would comply with requests to appear on Capitol Hill but stopped short of describing how much would be disclosed, at least in public sessions.

"If Congress asks us to appear, we will appear," said Selim Bingol, a spokesman at AT&T. "We will act within the laws and rules that apply."

Qwest was apparently alone among the four major telephone companies to have resisted the requests to cooperate with the government effort. A statement issued on behalf of Mr. Nacchio yesterday by his lawyer, Herbert J. Stern, said that after the government's first approach in the fall of 2001, "Mr. Nacchio made inquiry as to whether a warrant or other legal process had been secured in support of that request."

## QUESTIONS RAISED FOR PHONE GIANTS IN SPY DATA FUROR The New York Times M

"When he learned that no such authority had been granted, and that there was a disinclination on the part of the authorities to use any legal process," Mr. Nacchio concluded that the requests violated federal privacy requirements "and issued instructions to refuse to comply."

The statement said the requests continued until Mr. Nacchio left in June 2002. His departure came amid accusations of fraud at the company, and he now faces federal charges of insider trading.

The database reportedly assembled by the security agency from calling records has dozens of fields of information, including called and calling numbers and the duration of calls, but nothing related to the substance of the calls. But it could permit what intelligence analysts and commercial data miners refer to as "link analysis," a statistical technique for investigators to identify calling patterns in a seemingly impenetrable mountain of digital data.

The law governing the release of phone company data has been modified repeatedly to grapple with changing computer and communications technologies that have increasingly bedeviled law enforcement agencies. The laws include the Communications Act, first passed in 1934, and a variety of provisions of the Electronic Communications and Privacy Act, including the Stored Communications Act, passed in 1986.

Wiretapping -- actually listening to phone calls -- has been tightly regulated by these laws. But in general, the laws have set a lower legal standard required by the government to obtain what has traditionally been called pen register or trap-and-trace information -- calling records obtained when intelligence and police agencies attached a specialized device to subscribers' telephone lines.

Those restrictions still hold, said a range of legal scholars, in the face of new computer databases with decades' worth of calling records. AT&T created such technology during the 1990's for use in fraud detection and has previously made such information available to law enforcement with proper warrants.

Orin Kerr, a former federal prosecutor and assistant professor at George Washington University, said his reading of the relevant statutes put the phone companies at risk for at least \$1,000 per person whose records they disclosed without a court order.

"This is not a happy day for the general counsels" of the phone companies, he said. "If you have a class action involving 10 million Americans, that's 10 million times \$1,000 -- that's 10 billion."

The New Jersey lawyers who filed the federal suit against Verizon in Manhattan yesterday, Bruce Afran and Carl Mayer, said they would consider filing suits against BellSouth and AT&T in other jurisdictions.

"This is almost certainly the largest single intrusion into American civil liberties ever committed by any U.S. administration," Mr. Afran said. "Americans expect their phone records to be private. That's our bedrock governing principle of our phone system." In addition to damages, the suit seeks an injunction against the security agency to stop the collection of phone numbers.

Several legal experts cited ambiguities in the laws that may be used by the government and the phone companies to defend the National Security Agency program.

"There's a loophole," said Mark Rasch, the former head of computer-crime investigations for the Justice Department and now the senior vice president of Solutionary, a computer security company. "Records of phones that have called each other without identifying information are not covered by any of these laws."

Civil liberties lawyers were quick to dispute that claim.

"This is an incredible red herring," said Kevin Bankston, a lawyer for the Electronic Frontier Foundation, a privacy rights group that has sued AT&T over its cooperation with the government, including access to calling records. "There is no legal process that contemplates getting entire databases of data."

The group sued AT&T in late January, contending that the company was violating the law by giving the government access to its customer call record data and permitting the agency to tap its Internet network. The suit followed reports in The New York Times in December that telecommunications companies had cooperated with such government requests without warrants.

A number of industry executives pointed to the national climate in the wake of the Sept. 11 attacks to explain why phone companies might have risked legal entanglement in cooperating with the requests for data without warrants.

QUESTIONS RAISED FOR PHONE GIANTS IN SPY DATA FUROR The New York Times M

An AT&T spokesman said yesterday that the company had gotten some calls and e-mail messages about the news reports, but characterized the volume as "not heavy" and said there were responses on both sides of the issue.

Reaction around the country also appeared to be divided.

Cathy Reed, 45, a wealth manager from Austin, Tex., who was visiting Boston, said she did not see a problem with the government's reviewing call logs. "I really don't think it matters," she said. "I bet every credit card company already has them."

Others responded critically. Pat Randall, 63, a receptionist at an Atlanta high-rise, said, "Our phone conversations are just personal, and to me, the phone companies that cooperated, I think we should move our phone services to the company that did not cooperate."

While the telephone companies have both business contracts and regulatory issues before the federal government, executives in the industry yesterday dismissed the notion that they felt pressure to take part in any surveillance programs. The small group of executives with the security clearance necessary to deal with the government on such matters, they said, are separate from the regulatory and government contracting divisions of the companies.

**URL:** <http://www.nytimes.com>

**LOAD-DATE:** May 13, 2006