


# EXHIBIT A

**ZIP REALTY** Search for **BAY AREA** homes on the **MLS.**

BED/BATH:  SQ. FT.:



[NYTimes.com](#)

Welcome, [mhof1218](#) - [Member Center](#) - [Log Out](#)

SEARCH

# Bush Lets U.S. Spy on Callers Without Courts

By **JAMES RISEN** and **[ERIC LICHTBLAU](#)**  
Published: December 16, 2005

## Correction Appended

[Enlarge This Image](#)



Doug Mills/Associated Press

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.

[E-Mail This](#)  
[Printer-Friendly](#)  
[Reprints](#)  
[Save Article](#)

ARTICLE TOOLS  
SPONSORED BY  
**THE SAVAGES**

WASHINGTON, Dec. 15 - 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,

Advertisement

Yes  No

Yes  No

Yes  No

 **Most E-Mailed Articles** *The New York Times*

Past 24 Hours | [Past 7 Days](#)

- [1 in 100 U.S. Adults Behind Bars, New Study Says](#)
- [Findings: The Advantages of Closing a Few Doors](#)
- [Gail Collins: Hillary, Buckeye Girl](#)
- [Facing Default, Some Walk Out on New Homes](#)
- [Blood Thinner Might Be Tied to More Deaths](#)

[Go to Complete List](#)

ADVERTISEMENTS

All the news that's fit to personalize.

**THREATS AND RESPONSES**[▶ GO TO COMPLETE COVERAGE](#)**Related**[A Half-Century of Surveillance](#)

(December 16, 2005)

[In the Blogs: Reaction to Relaxed Restrictions on Domestic Spying](#)

(December 16, 2005)

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.

**Readers' Opinions**[Forum: National Security](#)

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 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.

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 warrants 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 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."

*Barclay Walsh contributed research for this article.*

**Correction:** Dec. 28, 2005, Wednesday:

*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.*

[More Articles in Washington >](#)

#### RELATED ARTICLES

[Big Brother Is Tracking You. Without a Warrant.](#) (May 18, 2003)

[THREATS AND RESPONSES: PRIVACY: Going Electronic, Denver Reveals Long-Term Surveillance](#) (December 21, 2002)

[TRACES OF TERROR: CIVIL LIBERTIES: Echo of F.B.I. Abuses In Queries on New Role](#) (June 13, 2002)

[AFTER THE ATTACKS: CIVIL LIBERTIES: Some Foresee A Sea Change In Attitudes On Freedoms](#) (September 15, 2001)

#### RELATED SEARCHES

[Surveillance of Citizens By Government](#) | [United States Politics and Government](#) | [Terrorism](#) |

#### INSIDE NYTIMES.COM



Blog

[The](#)



[Charles Taylor's Rise and Fall](#)

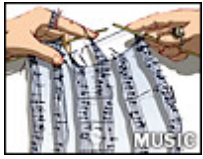


[The Ghost in the Baghdad Museum](#)



[Making of a Toddler Supergroup](#)

[Caucus](#)



[Digital Composer](#)



Kate Phillips and The Times's politics staff on the latest news from Washington and around the nation.

# 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](#)



#### ↓ Radio Address

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

#### ↓ Radio Interviews

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

# EXHIBIT C

Everyone can file Federal Taxes **FREE.**

Start Now!

**TaxACT.**



[NYTimes.com](#)

Go to a Section

Welcome, [mhof1218](#) - [Member Center](#) - [Log Out](#)

SEARCH

NYT Since 1981

Search

# Spy Agency Mined Vast Data Trove, Officials Report

By [ERIC LICHTBLAU](#) and JAMES RISEN

Published: December 24, 2005

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.

## Related

[Bush Lets U.S. Spy on Callers Without Courts](#) (December 16, 2005)

[Daschle Says Congress Never Authorized Program](#)

[Alito Wrote on Wiretaps](#)

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

- [E-Mail This](#)
- [Printer-Friendly](#)
- [Reprints](#)
- [Save Article](#)



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

Advertisement

**Buy stocks for \$4**



- No Minimums
- No Inactivity Fees
- Invest Any Amount

[Click here >](#)

**ING DIRECT** | **shareBUILDER**

## Most E-Mailed Articles The New York Times

Past 24 Hours | [Past 7 Days](#)

1. [1 in 100 U.S. Adults Behind Bars, New Study Says](#)
2. [Findings: The Advantages of Closing a Few Doors](#)
3. [Gail Collins: Hillary, Buckeye Girl](#)
4. [Facing Default, Some Walk Out on New Homes](#)
5. [Blood Thinner Might Be Tied to More Deaths](#)

[Go to Complete List](#)

## ADVERTISEMENTS

All the news that's fit to personalize.

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.

[More Articles in Washington >](#)

#### RELATED ARTICLES

[Spying Program Snared U.S. Calls](#) (December 21, 2005)

[Bush Again Defends Spy Program](#) (January 2, 2006)

[Defense Lawyers in Terror Cases Plan Challenges Over Spy Efforts](#) (December 28, 2005)

[DOMESTIC SURVEILLANCE: THE WHITE HOUSE: Defending Spy Program, Administration Cites Law](#) (December 23, 2005)

[DOMESTIC SURVEILLANCE: CONGRESSIONAL LEADERS: Among Those Told of Program, Few Objected](#) (December 23, 2005)

#### RELATED SEARCHES

[National Security Agency](#) | [Terrorism](#) | [Bush, George W](#) | [Privacy](#) |

#### INSIDE NYTIMES.COM



[Charles Taylor's Rise and Fall](#)



[The Ghost in the Baghdad Museum](#)



[Making of a Toddler Supergroup](#)

[Blog](#)

[The Caucus](#)



Kate Phillips and The Times's politics staff on the latest news from Washington and around the nation.

[Digital](#)  
[Composer](#)

[Copyright 2006 The New York Times Company](#) | [Home](#) | [Privacy Policy](#) | [Search](#) | [Corrections](#) | [XML](#) | [Help](#) | [Contact Us](#) | [Work for Us](#) | [Site Map](#) | [Back to Top](#) |

---



# EXHIBIT D

Advertisement

**Openair** A new outlook on adventure

Open Air Magazine available inside USA TODAY on March 7th

Click here for more information

USA TODAY usatoday.com

USA TODAY Classifieds: [cars.com](#) | [careerbuilder.com](#) | [Marketplace](#) | [Real estate](#)

- Home
- News
- Travel
- Money
- Sports
- Life
- Tech
- Weather

## Washington/Politics

▪ [E-MAIL THIS](#) ▪ [PRINT THIS](#) ▪ [SAVE THIS](#) ▪ [MOST POPULAR](#) ▪ [SUBSCRIBE](#) ▪ [REPRINTS & PERMISSIONS](#)

Posted 2/5/2006 11:26 PM Updated 2/6/2006 12:12 AM

### 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,

Advertisement

© Best Buy 2006

All the best brands, all in one place. We'll help find the best one for you.

COMPARE NOW

BEST BRANDS. BEST HELP.™ **BEST BUY**

#### Related Advertising Links

What's This?

##### Hot Stock Alert - GFET

Green Energy, Cellulose Ethanol. Growth Stock... [www.GulfEthanolCorp.com](http://www.GulfEthanolCorp.com)

##### Hot Stock Alert - TMDI

Telemedicine Medical Technology & Mini Medical... [www.Telemedicus.com](http://www.Telemedicus.com)

#### E-Mail Newsletters

Sign up to receive our free **Daily Briefing e-newsletter** and get the top news of the day in your inbox.

E-mail:

Select one:  HTML  Text

#### Breaking News E-Mail Alerts

- [Get breaking news in your inbox as it happens](#)

powered by **YAHOO!**

#### Wash/Politics

- [Washington home](#)
- [Washington briefs](#)
- [Government guide](#)

#### Health&Behavior

- [H&B home](#)
- [Medical resources](#)
- [Health information](#)

#### Opinion

- [Opinion home](#)
- [Columnists](#)
- [Cartoons](#)

#### More News

- [Top news briefs](#)
- [Nation briefs](#)
- [World briefs](#)
- [States](#)
- [Lotteries](#)
- [By the numbers](#)
- [Special reports](#)
- [Day in pictures](#)
- [Snapshots](#)
- [Offbeat](#)
- [Video](#)
- [Talk Today](#)
- [Marketplace](#)
- [Real estate](#)
- [Arcade](#)
- [Newspaper](#)
- [Classifieds](#)

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 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.

Sponsored Links

**Hot Stock Alert - TMDI**

Telemedicine Medical Technology & Mini Medical Clinics. Growth Stock.

[www.Telemedicus.com](http://www.Telemedicus.com)

**Hot Stock Alert - GFET**

Green Energy, Cellulose Ethanol. Growth Stock Investment.

[www.GulfEthanolCorp.com](http://www.GulfEthanolCorp.com)

**Do You Know Your Credit Score?**

The average U.S. credit score is up to 692. See yours for \$0.

[www.freecreditreport.com](http://www.freecreditreport.com)

[Get listed here](#)

**Newspaper Home Delivery - Subscribe Today**

Advertisement



---

USATODAY.com partners: [USA WEEKEND](#) • [Sports Weekly](#) • [Education](#) • [Space.com](#)

[Home](#) • [Travel](#) • [News](#) • [Money](#) • [Sports](#) • [Life](#) • [Tech](#) • [Weather](#)

Resources: [Mobile news](#) • [Site map](#) • [FAQ](#) • [Contact us](#) • [E-mail news](#)  
[Jobs with us](#) • [Internships](#) • [Terms of service](#) • [Privacy policy/Your California Privacy Right](#)  
[Media kit](#) • [Media Lounge](#) • [Press room](#) • [Electronic print edition](#) • [Reprints and Permissions](#)

[Add USATODAY.com RSS feeds](#) 

The Nation's Homepage

Copyright 2008 USA TODAY, a division of [Gannett Co. Inc.](#)