EXHIBIT F

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.

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.