4 of 4 DOCUMENTS

USA TODAY

May 11, 2006 Thursday
FINAL EDITION

SECTION: NEWS; Pg. 1A

LENGTH: 2654 words

HEADLINE: NSA has massive database of Americans' phone calls;
3 telecoms help government collect billions of domestic records

BYLINE: Leslie Cauley

BODY:

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.

"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 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 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 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 $1.325million per violation. The FCC has no hard definition of "violation." In practice, that means a single "violation" could cover one customer or 1million.

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

GRAPHIC: PHOTO, B/W,Ron Edmonds,AP

LOAD-DATE: May 11, 2006