BELLSOUTH AND THE N.S.A.: SHOULD TENNESSEEANS BE WORRIED?

Monday, June 5, 2006

BELLSOUTH AND THE N.S.A.: SHOULD TENNESSEEANS BE WORRIED?

Regional carrier denies releasing phone records as civil rights groups file suits, request investigation

By Dane Baker

Despite often stringent denials from BellSouth officials, questions continue to persist about the Atlanta-based companyís involvement with a secret National Security Agency program analyzing domestic phone calls for terrorist activity.

The regional carrier, which services much of the southeast, including Tennessee, was one of four telephone companies mentioned in a May 11 USA Today report charging that three of them had turned over customer phone records to the N.S.A. without a court order. The fourth, Qwest Communications, said it was approached by N.S.A. officials and rejected the request.

The [phone record] data are used for ësocial network analysis, USA Today reported, which refers to studying how terrorist networks contact each other and how they are tied together.

The issue is how much context can be revealed from the records, said Professor Michael Berry, Interim Head of the University of Tennesseeís Computer Science department. The source and destination numbers allow one to build a graph or network of communication in time and space that could be used to track patterns of communication that might appear odd or abnormal, he said.

Unlike the other carriers said to have beenallegedly approached by the N.S.A., BellSouth does not operate its own long-distance network. Long-distance calls placed by BellSouth customers must travel at least partially on other networks, such as AT&T, who which recently agreed to acquire BellSouth.

If domestic eavesdropping includes monitoring of local calls, BellSouth would be a crucial piece of the puzzle allegedly being constructed by the N.S.A. Otherwise, its potential value to the N.S.A. is unclear, aside from carrying some long-distance traffic from customers.

For its part, BellSouth denies even being contacted by the N.S.A., let alone providing customer records.

"That is correct, we have not provided any customer records at all to the N.S.A. Through our review we can not even find where we have been contacted by the N.S.A.," said Vice President of Corporate Communications Jeff Battcher, referring to an internal investigation conducted days after the USA Today story ran.

When asked if anyone from the company had any contact with the N.S.A. during the last five years, Battcher said, "To the best of our knowledge, and after our review, the answer is no."

Yet the spotlight continues to grow more intense: Since May 11, BellSouth has been named identified in numerous lawsuits seeking damages for allegedly turning over customer records and bypassing the courts. And on May 24, the American Civil Liberties Union of Tennessee filed a formal complaint with the Tennessee Regulatory Authority, asking the body to investigate our claim and order BellSouth to end its practice of sharing our phone records. "The information provided to the government about these telecommunication customers can be easily matched with other databases to obtain the name and residence of each caller," Executive Director Hedy Weinberg wrote inthe letter to the regulatory body. "This information would enable the government to track every phone call made by every Tennessee residential customer, including the identity of the people they have called and the length of each conversation," the letter read.

Most public opinion polls show the majority of Americans don't support the N.S.A.ís domestic programs. USA Today/Gallup reported that 51% disapproved of phone records collection, while 43% approved [6% had no opinion].

In addition to the ACLU complaint, the state Regulatory Authority reported receiving three inquiries from consumers for more information on about BellSouth's involvement.

"The Consumer Services Division of the TRA will investigate the matter," said Julie Woodruff, Senior Policy Advisor to TRA Chairman Ron Jones.

BellSouth has ten working days to issue a response to the May 24 complaint, Woodruff said. The state body will then consider what action to take.

Similar complaints were filed by local ACLU chapters to utility regulatory bodies in 20 states, including Maine, where Verizon asked the state Public Utility Commission not to investigate whether it had turned over customer phone records to the N.S.A., citing the classified nature of the information. "The phone companies will say the details of the program are state secrets, but I can reiterate to you that the government has a history of over-classifying information and claiming that any information or evidence that might be embarrassing or illegal are estate secrets, said ACLU of Tennessee's Weinberg.

Among civil rights groups, the focus has shifted to filing civil lawsuits and pressuring state authorities because the federal government has refused to investigate the program.

"The classified nature of the N.S.A.ís activities makes us unable to investigate the alleged violations," said FCC Chairman Kevin Martin in a written response to U.S. Rep. Edward Markey (D-MA), who requested a formal investigation by the FCC.

The Electronic Frontier Foundation has filed a class-action suit against AT&T, based largely on revelations of former AT&T technician Mark Klein. Kleinís deposition, heavily redacted by government censors, tells of a secret room at an AT&T facility in California where equipment was being installed "to route the publicís telephone calls that transit through" the AT&T facility. Responsibility for the room was given to a "management-level technician whom the N.S.A. cleared and approved for the special job."

If proven to be true, an N.S.A. "social network analysis" program would complement other rumored domestic intelligence activities, including an eavesdropping program involving "up to 500 people at any given time" without a warrant, revealed in a mid-December account published in the The New York Times

Given the green light by a secret 2002 executive order signed by President Bush, the N.S.A. program targets international phone calls and e-mails originating inside the United States.

Ironically, the interceptions take place without the approval of secret courts like the Federal Intelligence Surveillance Court, created in the wake of similar scandals involving N.S.A. surveillance of civil rights, peace, and other activists in the 1970s.

"The FISA court it's not very difficult to get something through a FISA court. I kinda liken the FISA court to a monkey with a rubber stamp," former N.S.A. analyst-turned-whistleblower Russell Tice told the television program Democracy Now in January.

"So, you have to ask yourself the question: Why would someone want to go around the FISA court in something like this?" he said, referring to a "vacuum cleaner approach" that casts a wide surveillance net.

"And I think thatís something Congress needs to address. They need to find out exactly how this system was operated and ultimately determine whether this was indeed a very focused effort or whether this was a vacuum cleaner-type scenario," he said.

Civil liberty concerns aside, the potential effectiveness of such a phone record data mining program remains questionableóparticularly in light of recent N.S.A. failures that have reportedly cost billions but yielded little in the search for terrorist groups. [See sidebar.]

Experts also question the potential for false leads generated by data mining programs.

The "prevalence of false leads is especially pronounced when U.S. citizens or residents are surveilled," the Washington Post reported in February, quoting an anonymous intelligence official. Former N.S.A. head Gen. Michael Hayden was also quoted by the Post as saying that given the nature of these programs, analysts "have to go down some blind alleys to find the tips that pay off."