

Chicago Tribune

Phone giants mum on spying In past, industry has cooperated with U.S.

By Jon Van

Tribune staff reporter

Published December 29, 2005

In the days following revelations that the Bush administration ordered the National Security Agency to spy on domestic telephone and Internet communications without a court order, one involved party has remained silent.

The nation's telephone giants--which control the data pipelines--have neither commented on nor denied their reported participation, nor have they reacted to the charge that they may have been complicit in violating privacy rights.

But historically the telecom companies have cooperated with the government on wholesale wiretapping, and the Bush administration's anti-terrorism programs appear to be no exception.

Without commenting directly on a classified topic, industry officials--when asked--suggested that they would not stand in the way of a request for help.

"Our members have worked for years with law enforcement with an objective to preserve lawfully authorized surveillance," said Tom Amontree, a spokesman for the US Telecom Association, the industry group representing most phone companies. "We have no comment on national security matters."

Added Eric Rabe, a spokesman for Verizon Communications Inc., one of the nation's phone giants: "We typically make law enforcement agencies get a court order. Our default is to cooperate, but we don't feel we should appropriate customer information lightly. We try to make sure what we do is in compliance with the law."

During the Cold War, telecom organizations freely cooperated with government agencies regarding national security, and there seemed to be little worry about whether the requests were accompanied by court orders, one expert said.

"In the 1960s, I worked for an international telex and telegram carrier in their Washington office," said Bob Atkinson, policy research director of the Columbia Institute for Tele-Information. "Every day a government agent stopped by to pick up copies of all telegrams that were sent overseas.

"I asked about it once and was told we'd been making copies available to the government since World War II.

"I think the practice only ended when people stopped sending telegrams."

Chicago Tribune

The Bush administration has been responding to critics since Saturday's disclosure that it directed the NSA to comb through huge volumes of telephone and Internet communications without first seeking court orders. The New York Times reported that since Sept. 11, 2001, unidentified American telecom companies have helped the government gain "backdoor access" to streams of communications flowing into and out of the U.S. in the search for terrorism suspects.

A Bush spokesman, Trent Duffy, called the current use of wiretaps without the usual court authorization limited.

Rabe, of Verizon, said it's true that phone companies have always been willing to help government inquiries, though times have changed.

In the Cold War era when there was great concern about Communists, "probably a lot of things went on," Rabe said, "but today we're more circumspect."

Last year when agents of the U.S. music industry asked Verizon for information about its Internet subscribers, the phone giant refused and went to court to protect its customers' privacy.

He noted that no telecom companies have been named in disclosures about NSA eavesdropping and declined to say if Verizon cooperates with that program. Bob Dwyer, a spokesman for AT&T Inc., another phone giant, said, "We don't comment on national security issues."

The question of what the telecom companies can help find is difficult to answer because of the highly classified nature of the work. But experts say the computer technology that enables eavesdropping on a national scale may well generate enough data to overwhelm human agents.

"Their idea of finding a needle in a haystack seems to involve getting more hay," said David Isenberg, a fellow at the Berkman Center for Internet and Society at Harvard University.

Isenberg said people who wish to evade government eavesdropping probably can do so by encrypting their communications.

For example, calls made using Internet telephony from the European-based Skype service are all encrypted, Isenberg said.

While government agencies might decrypt targeted communications, it's not possible to do this with the vast amounts of information apparently targeted by the NSA, he said.

The decentralized nature of the Internet and the multiplicity of ways to communicate further complicate the task of wholesale eavesdropping, said Daniel Berninger, a communications analyst with Tier 1 Research.

Chicago Tribune

By focusing on traffic that leaves the country, government agents can tap into optical fiber lines that are buried on the oceans and on radio signals bounced off satellites in space, Berninger said.

This provides some identifiable "choke points" where communications enter and leave the country, he said, providing an easier task than trying to randomly monitor domestic traffic that flows on the Internet in all directions around the country, he said.

Tapping into modern communications lines will yield billions of packets of voice and data all mixed together that is the electronic version of getting the slivers of paper that come out of a shredder, Berninger said.

While there is equipment available to put the signals back together as e-mail, voice conversations, downloaded music and the like, "once you add encryption to the mix, the game's over," said Berninger.

The technique used to monitor vast amounts of communications is data mining, and sophisticated software programs are regularly used by private businesses as well as government agencies.

Looking at data such as which phone numbers are called from which numbers can provide a lot of useful information, said Paul Bradley, a consultant with Apollo Data Technologies LLC, a Chicago-based data mining software firm.

"A lot of research has been done into social networking," said Bradley. "When you use free instant messaging, the provider looks at who chats with whom to reconstruct social networks. They collect a ton of information. I'm sure government agencies do that."

SPSS Inc., a Chicago-based software pioneer in data mining, provides programs to aid the Army in spotting hackers who are attempting to invade its computer systems and to help Homeland Security protect the nation's borders.

Such software could determine when people use aliases by comparing several different conversations and the patterns of name use within each, said Bill Haffey, technical director of SPSS' public sector products.

The system could even be programmed to send an agent an e-mail or call his cell phone to inform him once it discovers aliases that interest him, he said. Even if a security agency couldn't break an encryption used for messages, just noting the pattern of encryption could provide useful information, Haffey said.

"There's no magic in any of this," said Jack Noonan, SPSS chief executive. "Everything we do with technology, you could do with humans. But sifting through billions of records could take all the humans in the world, taking years.

"With this technology, you can do it quickly enough to make a difference."

- - -

Chicago Tribune

Tapping in by land, by sea and from space

One question arising from the recent revelation that the National Security Agency monitored phone calls by U.S. citizens without court approval is whether phone companies worked with the agency to monitor calls. Some ways the NSA might have tapped into communications:

With help from phone companies:

TELEPHONE SWITCHES

One of the easiest ways to monitor phone conversations is to attach a wiretapping device to a telephone switch, which is what phone companies use to route calls. Calls can then be directly recorded and reviewed.

Without help from phone companies:

TRANSOCEANIC CABLES

Large fiber-optic cables laid across the ocean floor from the U.S. to other countries require a light signal carrying a voice message to be amplified along the way. To do this, the light signal is converted to an electronic digital signal, amplified and then converted back into a light signal. During this conversion, a U.S. ship could use special instruments to read the signal, yielding the messages within.

SATELLITES

- Many communication signals travel across land by being relayed from stations and towers. Because of the Earth's curvature, these signals may not all reach the relay station and can end up in space, where government satellites can pick them up.
- Signals from overseas, beamed toward the U.S. from communications satellites, can be intercepted by large dishes used by the government.

Sources: GlobalSecurity.org, Electronic Privacy Information Center

Chicago Tribune

jvan@tribune.com