



Friday, May 19, 2006

Furor aside, privacy of phone records is not a protected right

For aggrieved customers and privacy advocates, FCC regulations—not the U.S. Constitution—may offer the best hope for protecting phone records, say lawyers

By Philippa Maister, Staff Reporter

Whatever the truth turns out to be with regard to allegations that telephone companies turned over the phone records of millions of customers to the National Security Agency, it is a glaring reminder that there is no constitutional right to privacy, according to John P. Hutchins, a partner at Troutman Sanders and an expert in privacy and data security.

"This should be of concern to businesses as well," says Peter C. Canfield, a partner in Dow, Lohnes & Albertson's Atlanta office. "What they communicate and to whom may well become the subject of government inquiry."

A story in the May 11 issue of *USA Today* cited "people with direct knowledge of the arrangement" who accused the NSA of "secretly collecting the phone call records of tens of millions of Americans," using data provided under contractual agreements by AT&T, BellSouth Corp. and Verizon Communications.

BellSouth and Verizon have denied the allegations, which raise a host of legal issues including constitutional and privacy concerns, as well as potential violations of Federal Communications Commission regulations. The issue is a thorny one for businesses: Who owns the data that is collected on customers?

While the allegations against the phone companies have created outrage among some customers and privacy advocates, Hutchins said they shouldn't expect much support from the U.S. Constitution.

Hutchins said the Fourth Amendment's protection against unreasonable searches and seizures without a warrant would not restrain the NSA's actions because the amendment is intended to protect against searches for evidence in criminal cases.

The First Amendment's guarantee of free speech also would not apply because the NSA situation does not involve the government's ability to impede an individual's ability to make a statement, he said.

"The most interesting issue for me in this case is that it really points out there is no constitutional right to privacy—even though there is a widespread belief in this country that one exists," Hutchins said. "The right to privacy has been judicially interpreted in various contexts, such as *Roe v. Wade*, from 'the penumbra of rights' included in the Bill of Rights. That is largely misunderstood by the American public."

Hutchins cited a string of violations of the privacy of personal records that occurred last year, beginning with misuse of Alpharetta-based ChoicePoint's database by bogus customers.

"The government and private business are out there all the time gathering all kinds of data about us that most Americans think they have the right to keep private, but the right to privacy is actually pretty limited," he said. "There are restrictions, but they are by and large a result of legislative action."

Canfield agrees that First and Fourth Amendment rights are unlikely to come into play. He said the contractual relationship between a phone company and a subscriber may offer some redress if the company has a privacy policy that officially promises to restrict disclosure of personal information.

"For breach of contract, the issue would be what sort of relationship exists between the phone company and the subscriber regarding the use of their data," he said.

Look to FCC rules

FCC regulations offer the best hope for protecting the records of phone companies' customers, according to To-Quyen T. Truong, head of the telecommunications practice in Dow, Lohnes & Albertson's Washington office.

"Telephone companies have an obligation to protect the confidentiality of that information," Truong said. "The FCC has lots of rules on this and the circumstances under which companies can use it or disclose it. They can disclose it to provide service or to comply with a legal requirement.

"There has to be a legal process for it, such as a subpoena or a court order. Beyond that, it gets into a gray area," Truong said.

"If there is no legal requirement to provide that information—if it is just a commercial agreement—the phone company cannot do so without the customer's permission."

If the customer does not consent, the FCC can impose a fine of up to \$130,000 per violation per day and up to \$1.325 million per violation, Truong said.

Many states also regulate phone companies' activities and have the ability to impose substantial penalties, Truong said. The cases filed to date have been brought under state law.

In 2005, the Georgia Legislature passed a law that barred phone companies from releasing an individual's phone records without that person's consent "except with proper law enforcement or court order documentation, as otherwise provided by law" or as authorized by the Georgia Public Service Commission. Companies are required to certify annually to the attorney general that they have telephone record security procedures in place.

Truong said the FCC also administers the Communications Assistance for Law Enforcement Act, which requires phone companies to cooperate with law enforcement authorities' electronic surveillance activities under specified rules. However, too little is known about the NSA's arrangements with phone companies to determine whether this Act was triggered, she said.

FCC Commissioner Michael J. Copps has called for an FCC investigation of whether the phone companies violated Section 222 or any other provisions of federal law. "We need to be certain that the companies over which the FCC has public interest oversight have not gone—or been asked to go—to a place where they should not be," he said.

Merger questions

If true, the allegations against the phone companies could come back to haunt them when the FCC and Department of Justice rule on the proposed merger of AT&T and BellSouth, Truong said.

"It would not be surprising for interested parties to raise that issue in the merger review," she said. "The review is supposed to assess whether the merger would be in the public interest. Whether these allegations would result in any FCC action on the issue is an open question."

Within hours of the story breaking, two New Jersey lawyers filed a suit against President Bush, the NSA and Verizon alleging violations of the Telecommunications Act, which regulates phone companies. BellSouth has been targeted with similar suits.

Mustaque Ahamad, director of the Georgia Tech Information Security Center and a professor in the College of Computing, said traffic analysis—the technical term for the NSA's alleged program—is fairly simple. However, tracking the calls of all customers of the three telephone companies, while feasible, is no trivial project, he said.

Ahamad said traffic analysis can be used to reveal and analyze social networks. "Usually there's a sort of clustering of a group of people who talk among themselves," he said. "They are looking at who you talk to directly, and who those people in turn talk to.

"The danger is that if someone else gets their hands on this data, there's a potential for abuse by someone else trying to make a commercial profit, perhaps illegally," Ahamad said.

DISCOVER MORE

Here's a link to more information on protecting the privacy of your phone records:

- Federal Communications Commission Consumer Advisory:
<http://www.fcc.gov/cgb/consumerfacts/phoneaboutyou.html>

Staff Reporter *Philippa Maister* can be reached at pmaister@alm.com.