

NSA utilizing 'social network analysis' in surveillance

By *BRIAN BERGSTEIN - AP Technology Writer - 05/12/06*

BOSTON — If the National Security Agency is indeed amassing a colossal database of Americans' phone records, one way to use all that information is in "social network analysis," a data-mining method that aims to expose previously invisible connections among people.

Social network analysis has gained prominence in business and intelligence circles under the belief that it can yield extraordinary insights, such as the fact that people in disparate organizations have common acquaintances. Companies can buy social networking software to help determine who has the best connections for a particular sales pitch.

So it did not surprise many security analysts to learn Thursday from USA Today that the NSA is applying the technology to billions of phone records.

"Who you're talking to often matters much more than what you're saying," said Bruce Schneier, a computer security expert and author of "Beyond Fear: Thinking Sensibly About Security in an Uncertain World."

The NSA declined to comment. But several experts said it seemed likely the agency would want to assemble a picture from more than just landline phone records. Other forms of communication, including cell phone calls, e-mails and instant messages, likely are trackable targets as well, at least on international networks if not inside the U.S.

To be sure, monitoring newer communications services is probably harder than getting billing records from landline phones. USA Today reported that the NSA has collected call logs from the three largest U.S. phone companies, BellSouth Corp., AT&T Inc. and Verizon Communications Inc.

That level of cooperation confirmed the fears of many privacy analysts, who pointed out that AT&T is already being sued in federal court in San Francisco for allegedly giving the NSA access to contents of its phone and Internet networks. The charges are based on documents from a former AT&T technician.

It remains unclear whether other communications providers have been asked for their call logs or billing records.

Verizon Wireless spokesman Jeffrey Nelson definitively said his company was "not involved in this situation." His counterparts at Cingular — an AT&T/BellSouth joint venture — and Sprint Nextel Corp. were less explicit and did not deny any participation.

Even without cell phone carriers' help, of course, calls between wireless subscribers and Verizon, AT&T and BellSouth landlines presumably would be captured.

Among Internet service providers, representatives for AOL LLC said the company complies with individual government subpoenas and court orders but does not have a blanket program for broader sharing of customer data. Microsoft Corp. had "never engaged in the type of activity referenced in these articles," according to a statement from Scott Charney, its vice president for trustworthy computing. Google Inc. spokesman Steve Langdon said his company does not participate, either.

Yahoo Inc. officials say they comply with subpoenas, but refused to elaborate, saying they cannot comment on specific government interactions.

Even without full inside help, the NSA has proven itself adept at capturing communications or at least analyzing traffic information. The Echelon program, for example, is known to have tapped into satellite, microwave and fiber-optic phone links — including undersea cables — in order to gain insights into what the rest of the world was talking about.

The Internet does present new challenges for snoops, which has led federal authorities to seek an expansion of a key surveillance law so that it applies to new kinds of Web services.

But even now authorities can tap into data feeds. There is a relatively small number of major Internet backbones and data junctions where networks hand information off to each other.

And while e-mail, Internet calls and other data packets splinter and take varying routes across networks, each packet has a header identifying its source and destination. It's not obvious what the packet is part of — whether an e-mail, a Web page or an Internet phone call — but it still contains the equivalent of a phone billing record: who's talking to whom.

“It's not trivial to analyze all the material, but it's trivial to get to the material,” said Barry Steinhardt, director of the technology and liberty program at the American Civil Liberties Union.

Even Skype, the popular Internet phone service that encrypts its calls — which presumably prevents sweeping monitoring of their content — is believed to be vulnerable to who's-calling-whom traffic analysis.

Still, while the government clearly can parlay industry cooperation and technical firepower to grab lots of communications, there's bound to be a limit.

For example, tiny, free voice-over-Internet services likely don't bother to maintain the kinds of call logs that Verizon, BellSouth and AT&T apparently handed over, said Jeff Pulver, an authority on the technology.

Also, social network analysis would appear to be powerless against criminals and terrorists who rely on a multitude of cell phones, payphones, calling cards and Internet cafes.

And then there are more creative ways of getting off the grid. The Madrid train bombings case has revealed that the plotters communicated by sharing one e-mail account and saving messages to each other as drafts that didn't traverse the Internet like regular mail messages would.

Privacy activists worry that the government is likely to try to overcome these surveillance gaps by making more use of the information it does have — by cross-referencing phone or other records with commercially harvested data.

One effort in that direction, the Pentagon's infamous Total Information Awareness program, was technically shuttered by Congress, but the government still can access copious data from the private sector.

Even if the NSA's surveillance went no further than the NSA's access to phone billing records, it clearly would raise hackles.