Eavesdropping Leaps Into 21st Century

By MATTHEW FORDAHL, AP Technology Writer

Sun Jan 22, 11:46 PM ET

SAN JOSE, Calif. - In the past, intercepting communications meant just that — copying a telegram mid-route, steaming open an envelope or attaching alligator clips to the copper wires that connected every telephone in the world.

But the old ways of communicating are heading into the sunset like the Pony Express and being replaced by phone calls, instant messages, e-mail and more that are converted into digital data before they gallop across the Internet and other advanced networks.

This constant interchange of massive amounts of data, converging into speeding bitstreams on common pipes, is both a blessing and a curse for eavesdroppers.

It's easier than ever to access wholesale feeds of data. But such work is also more controversial than traditional wiretapping, as seen in objections to post-9/11 warrantless domestic surveillance and to regulatory moves to require networks to be tap-friendly.

Critics question whether safeguards put in place a quarter century ago following FBI wiretapping misconduct are strong enough to prevent abuse in the 21st century. Others fear the information superhighway is turning out to be a fast path to mass surveillance.

"The thing that really should worry people is that once the capability is there, people will abuse it," said Jennifer Granick, executive director of Stanford University's Center for Internet and Society. "The opportunity for abuse is so much greater, because so much more of our private information is transmitted over the network."

Always a hot topic, the debate over wiretapping is further fueled today not only by the knowledge of what's possible but also by a dearth of details of what's actually happening.

What makes the White House surveillance program — acknowledged after The New
New York Times disclosed it in December — a cause of such concern is that it skirts existing laws and employs techniques resembling a wide-mouthed vacuum before the fine-toothed combs can be wielded.

It's being performed by the ultra-secret National Security Agency, which is believed to have the most advanced information vacuuming technology available. The NSA did not return telephone calls seeking comment on its methods.

The agency's efforts are reported to enjoy the cooperation of telecommunications companies, which run the major backbones and junctions where data — phone calls and Internet traffic — is exchanged between carriers' networks. Those companies have refused to confirm or deny to The Associated Press whether they've cooperated with the program, which the White House says began in 2002 with the aim of preventing terrorist attacks.

But they could be helping in a number of ways to provide information on who's talking to whom, when, how long the communication lasts and, ultimately, the content itself. Under the laws bypassed by the Bush administration, warrants for wiretaps require some evidence of wrongdoing.

Given the huge amount of data that traverses networks, it's likely that one element of the program involves analyzing traffic to single out anyone who communicates with people in suspicious locations. Data accumulated for phone billing could be one of the sources.

Modern networks can yield such information not just for phone calls but also for any other type of communication that passes through. When the data is converted to packets, as in the Internet, each one contains a header with the origin and destination. Even without support from a carrier, the NSA could be sniffing communication as it traverses the airwaves or passes through the millions of miles of fiber optic cable that are buried underground or beneath oceans.

The technical problem is in the fire hose of information involved, said Mark Rasch, a former Justice Department computer crimes prosecutor.

"The idea that the NSA could be sitting on every call going internationally, listening in on every possible language, for the words al-Qaida, 'terrorist' or 'bombs' is just fallacy," he said. "Computers capable of doing that simply don't exist and hopefully never will."

But the technology does exist to quickly read just the destination or origin information.

That sort of monitoring, if done on a wide scale, creates thorny moral, ethical and legal problems because those channels are much more likely to contain the chatter of innocents than the machinations of terrorists. And it raises the question of how that traffic is used.

"The thing about traffic analysis is you can mine that to any depth you want," said Bruce Schneier, chief technology officer of Counterpane Internet Security Inc.

In domestic criminal cases, law enforcement officials who want simply to know who is talking to whom — excluding content — need only tell a court it's important to a case. But that low burden of proof was established with the belief that only one line would be monitored.
When such surveillance is done on all outbound international calls, the law is not clear.

"I would say the Fourth Amendment (guaranteeing protection against unreasonable searches) is the Fourth Amendment, and the fact that you're invading the privacy of millions as opposed to dozens should make it worse, not better," said Rasch, who is now chief security counsel at Solutionary Inc., a security risk management firm.

It's believed that once the traffic analysis identifies "people of interest," they are then targeted for further surveillance and, possibly, full-content monitoring. Then, the NSA could simply mirror the data going to or coming from a target. It could even set up a parallel phone company or its own Internet Service Provider that would be invisible to its targets, Rasch said.

Critics note that the White House could easily have used the secret court created by the 1978 Foreign Intelligence Surveillance Act to get approval for such wiretaps, but chose instead to bypass it.

As it is, the FISA court has been criticized for rubber stamping requests.

"During the Clinton years, we were fighting that kangaroo court — they never said no," Schneier said. "Here we are now wishing for the little oversight that the court had."

The NSA surveillance also raises questions about wiretapping in investigations unrelated to national security.

Responding to complaints by law enforcers that such digital communications as Internet telephony can stymie their eavesdropping, the FCC decided last year decided that the 1994 Communications Assistance for Law Enforcement Act should be extended next year to apply to some broadband Internet access providers and Voice over Internet Protocol (VoIP) companies.

CALEA compels those companies to proactively build out that capability, and network equipment vendors are starting to building surveillance tools into their gear in anticipation of compliance.

Some companies, such as VeriSign Inc. and NeuStar Inc., offer an all-in-one service for carriers and service providers, which some federal agencies have argued will actually enhance privacy for people not under investigation.

But critics say that rather than laying the groundwork for privacy, new regulations will more likely enable greater misuse.

"There's no question in my mind that once we make the networks less secure because of CALEA, we will exploit that lack of security to intercept communications under every legal authority asserted by the government," Rasch said.