The New York Times
nytimes.com

December 16, 2007

Wider Spying Fuels Aid Plan for Telecom Industry

By ERIC LICHTBLAU, JAMES RISEN and SCOTT SHANE

This article is by Eric Lichtblau, James Risen and Scott Shane.

WASHINGTON — For months, the Bush administration has waged a high-profile campaign, including personal lobbying by President Bush and closed-door briefings by top officials, to persuade Congress to pass legislation protecting companies from lawsuits for aiding the National Security Agency's warrantless eavesdropping program.

But the battle is really about something much bigger. At stake is the federal government's extensive but uneasy partnership with industry to conduct a wide range of secret surveillance operations in fighting terrorism and crime.

The N.S.A.'s reliance on telecommunications companies is broader and deeper than ever before, according to government and industry officials, yet that alliance is strained by legal worries and the fear of public exposure.

To detect narcotics trafficking, for example, the government has been collecting the phone records of thousands of Americans and others inside the United States who call people in Latin America, according to several government officials who spoke on the condition of anonymity because the program remains classified. But in 2004, one major phone carrier balked at turning over its customers' records. Worried about possible privacy violations or public relations problems, company executives declined to help the operation, which has not been previously disclosed.

In a separate N.S.A. project, executives at a Denver phone carrier, Qwest, refused in early 2001 to give the agency access to their most localized communications switches, which primarily carry domestic calls, according to people aware of the request, which has not been previously reported. They say the arrangement could have permitted neighborhood-by-neighborhood surveillance of phone traffic without a court order, which alarmed them.

The federal government's reliance on private industry has been driven by changes in technology. Two decades ago, telephone calls and other communications traveled mostly through the air, relayed along microwave towers or bounced off satellites. The N.S.A. could vacuum up phone, fax and data traffic merely by erecting its own satellite dishes. But the fiber optics revolution has sent more and more international communications by land and undersea cable, forcing the agency to

seek company cooperation to get access.

After the disclosure two years ago that the N.S.A. was eavesdropping on the international communications of terrorism suspects inside the United States without warrants, more than 40 lawsuits were filed against the government and phone carriers. As a result, skittish companies and their lawyers have been demanding stricter safeguards before they provide access to the government and, in some cases, are refusing outright to cooperate, officials said.

“It’s a very frayed and strained relationship right now, and that’s not a good thing for the country in terms of keeping all of us safe,” said an industry official who believes that immunity is critical for the phone carriers. “This episode has caused companies to change their conduct in a variety of ways.”

With a vote in the Senate on the issue expected as early as Monday, the Bush administration has intensified its efforts to win retroactive immunity for companies cooperating with counterterrorism operations.

“The intelligence community cannot go it alone,” Mike McConnell, the director of national intelligence, wrote in a New York Times Op-Ed article Monday urging Congress to pass the immunity provision. “Those in the private sector who stand by us in times of national security emergencies deserve thanks, not lawsuits.”

Attorney General Michael B. Mukasey echoed that theme in an op-ed article of his own in The Los Angeles Times on Wednesday, saying private companies would be reluctant to provide their “full-hearted help” if they were not given legal protections.

The government’s dependence on the phone industry, driven by the changes in technology and the Bush administration’s desire to expand surveillance capabilities inside the United States, has grown significantly since the Sept. 11 attacks. The N.S.A., though, wanted to extend its reach even earlier. In December 2000, agency officials wrote a transition report to the incoming Bush administration, saying the agency must become a “powerful, permanent presence” on the commercial communications network, a goal that they acknowledged would raise legal and privacy issues.

While the N.S.A. operates under restrictions on domestic spying, the companies have broader concerns — customers’ demands for privacy and shareholders’ worries about bad publicity.

In the drug-trafficking operation, the N.S.A. has been helping the Drug Enforcement Administration in collecting the phone records showing patterns of calls between the United States, Latin America and other drug-producing regions. The program dates to the 1990s, according to several government officials, but it appears to have expanded in recent years.

Officials say the government has not listened to the communications, but has instead used phone numbers and e-mail addresses to analyze links between people in the United States and overseas. Senior Justice Department officials in the Bush and Clinton administrations signed off on the operation, which uses broad administrative subpoenas but does not require court approval to demand the records.

At least one major phone carrier — whose identity could not be confirmed — refused to cooperate, citing concerns in 2004 that the subpoenas were overly broad, government and industry officials said. The executives also worried that if the program were exposed, the company would face a public-relations backlash.

The D.E.A. declined to comment on the call-tracing program, except to say that it "exercises its legal authority" to issue administrative subpoenas. The N.S.A. also declined to comment on it.

In a separate program, N.S.A. officials met with the Qwest executives in February 2001 and asked for more access to their phone system for surveillance operations, according to people familiar with the episode. The company declined, expressing concerns that the request was illegal without a court order.

While Qwest's refusal was disclosed two months ago in court papers, the details of the N.S.A.'s request were not. The agency, those knowledgeable about the incident said, wanted to install monitoring equipment on Qwest's "Class 5" switching facilities, which transmit the most localized calls. Limited international traffic also passes through the switches.

A government official said the N.S.A. intended to single out only foreigners on Qwest's network, and added that the agency believed Joseph Nacchio, then the chief executive of Qwest, and other company officials misunderstood the agency's proposal. Bob Toevs, a Qwest spokesman, said the company did not comment on matters of national security.

Other N.S.A. initiatives have stirred concerns among phone company workers. A lawsuit was filed in federal court in New Jersey challenging the agency's wiretapping operations. It claims that in February 2001, just days before agency officials met with Qwest officials, the N.S.A. met with AT&T officials to discuss replicating a network center in Bedminster, N.J., to give the agency access to all the global phone and e-mail traffic that ran through it.

The accusations rely in large part on the assertions of a former engineer on the project. The engineer, who spoke on the condition of anonymity, said in an interview that he participated in numerous discussions with N.S.A. officials about the proposal. The officials, he said, discussed ways to duplicate the Bedminster system in Maryland so the agency "could listen in" with unfettered access to communications that it believed had intelligence value and store them for

later review. There was no discussion of limiting the monitoring to international communications, he said.

“At some point,” he said, “I started feeling something isn’t right.”

Two other AT&T employees who worked on the proposal discounted his claims, saying in interviews that the project had simply sought to improve the N.S.A.’s internal communications systems and was never designed to allow the agency access to outside communications. Michael Coe, a company spokesman, said: “AT&T is fully committed to protecting our customers’ privacy. We do not comment on matters of national security.”

But lawyers for the plaintiffs say that if the suit were allowed to proceed, internal AT&T documents would verify the engineer’s account.

“What he saw,” said Bruce Afran, a New Jersey lawyer representing the plaintiffs along with Carl Mayer, “was decisive evidence that within two weeks of taking office, the Bush administration was planning a comprehensive effort of spying on Americans’ phone usage.”

The same lawsuit accuses Verizon of setting up a dedicated fiber optic line from New Jersey to Quantico, Va., home to a large military base, allowing government officials to gain access to all communications flowing through the carrier’s operations center. In an interview, a former consultant who worked on internal security said he had tried numerous times to install safeguards on the line to prevent hacking on the system, as he was doing for other lines at the operations center, but his ideas were rejected by a senior security official.

The facts behind a class-action lawsuit in San Francisco are also shrouded in government secrecy. The case relies on disclosures by a former AT&T employee, Mark Klein, who says he stumbled upon a secret room at an company facility in San Francisco that was reserved for the N.S.A. Company documents he obtained and other former AT&T employees have lent some support to his claim that the facility gave the agency access to a range of domestic and international Internet traffic.

The telecommunications companies that gave the government access are pushing hard for legal protection from Congress. As part of a broader plan to restructure the N.S.A.’s wiretapping authority, the Senate Intelligence Committee agreed to give immunity to the telecommunications companies, but the Judiciary Committee refused to do so. The White House has threatened to veto any plan that left out immunity, as the House bill does.

“Congress shouldn’t grant amnesty to companies that broke the law by conspiring to illegally spy on Americans” said Kate Martin, director of the Center for National Security Studies in Washington.

But Bobby R. Inman, a retired admiral and former N.S.A. director who has publicly criticized the agency's domestic eavesdropping program, says he still supports immunity for the companies that cooperated.

"The responsibility ought to be on the government, not on the companies that are trying to help with national security requirements," Admiral Inman said. If the companies decided to stop cooperating, he added, "it would have a huge impact on both the timeliness and availability of critical intelligence."