GlobalResearch
Center for Research on Globalization

National Security Department: Listening In

By Seymour M. Hersh
Global Research, May 23, 2006
The New Yorker 23 May 2006
Theme: Police State & Civil Rights

A few days before the start of the confirmation hearings for General Michael Hayden, who has been nominated by President Bush to be the head of the C.I.A., I spoke to an official of the National Security Agency who recently retired. The official joined the N.S.A. in the mid-nineteen-seventies, soon after contentious congressional hearings that redefined the relationship between national security and the public's right to privacy. The hearings, which revealed that, among other abuses, the N.S.A. had illegally intercepted telegrams to and from the United States, led to the passage of the 1978 Foreign Intelligence Surveillance Act, or FISA, to protect citizens from unlawful surveillance. "When I first came in, I heard from all my elders that 'we'll never be able to collect intelligence again,'" the former official said. "They'd whine, 'Why do we have to report to oversight committees?' " But, over the next few years, he told me, the agency did find a way to operate within the law. "We built a system that protected national security and left people able to go home at night without worrying whether what they did that day was appropriate or legal."

After the attacks of September 11, 2001, it was clear that the intelligence community needed to get more aggressive and improve its performance. The Administration, deciding on a quick fix, returned to the tactic that got intelligence agencies in trouble thirty years ago: intercepting large numbers of electronic communications made by Americans. The N.S.A.'s carefully constructed rules were set aside.

Last December, the Times reported that the N.S.A. was listening in on calls between people in the United States and people in other countries, and a few weeks ago USA Today reported that the agency was collecting information on millions of private domestic calls. A security consultant working with a major telecommunications carrier told me that his client set up a top-secret high-speed circuit between its main computer complex and Quantico, Virginia, the site of a government-intelligence computer center. This link provided direct access to the carrier's network core—the critical area of its system, where all its data are stored. "What the companies are doing is worse than turning over records," the consultant said. "They're providing total access to all the data."

"This is not about getting a cardboard box of monthly phone bills in alphabetical order," a former senior intelligence official said. The Administration's goal after September 11th was to find suspected terrorists and target them for capture or, in some cases, air strikes. "The N.S.A. is getting real-time actionable intelligence," the former official said.

The N.S.A. also programmed computers to map the connections between telephone numbers in the United States and suspect numbers abroad, sometimes focussing on a geographic area, rather than on a specific person—for example, a region of Pakistan. Such calls often triggered a process, known as "chaining," in which subsequent calls to and from the American number were monitored and linked. The way it worked, one high-level Bush

Administration intelligence official told me, was for the agency "to take the first number out to two, three, or more levels of separation, and see if one of them comes back"—if, say, someone down the chain was also calling the original, suspect number. As the chain grew longer, more and more Americans inevitably were drawn in.

FISA requires the government to get a warrant from a special court if it wants to eavesdrop on calls made or received by Americans. (It is generally legal for the government to wiretap a call if it is purely foreign.) The legal implications of chaining are less clear. Two people who worked on the N.S.A. call-tracking program told me they believed that, in its early stages, it did not violate the law. "We were not listening to an individual's conversation," a defense contractor said. "We were gathering data on the incidence of calls made to and from his phone by people associated with him and others." Similarly, the Administration intelligence official said that no warrant was needed, because "there's no personal identifier involved, other than the metadata from a call being placed."

But the point, obviously, was to identify terrorists. "After you hit something, you have to figure out what to do with it," the Administration intelligence official told me. The next step, theoretically, could have been to get a suspect's name and go to the fisa court for a warrant to listen in. One problem, however, was the volume and the ambiguity of the data that had already been generated. ("There's too many calls and not enough judges in the world," the former senior intelligence official said.) The agency would also have had to reveal how far it had gone, and how many Americans were involved. And there was a risk that the court could shut down the program.

Instead, the N.S.A. began, in some cases, to eavesdrop on callers (often using computers to listen for key words) or to investigate them using traditional police methods. A government consultant told me that tens of thousands of Americans had had their calls monitored in one way or the other. "In the old days, you needed probable cause to listen in," the consultant explained. "But you could not listen in to generate probable cause. What they're doing is a violation of the spirit of the law." One C.I.A. officer told me that the Administration, by not approaching the FISA court early on, had made it much harder to go to the court later.

The Administration intelligence official acknowledged that the implications of the program had not been fully thought out. "There's a lot that needs to be looked at," he said. "We are in a technology age. We need to tweak fisa, and we need to reconsider how we handle privacy issues."

Marc Rotenberg, the executive director of the Electronic Privacy Information Center, believes that if the White House had gone to Congress after September 11th and asked for the necessary changes in FISA "it would have got them." He told me, "The N.S.A. had a lot of latitude under FISA to get the data it needed. I think the White House purposefully ignored the law, because the President did not want to do the monitoring under FISA. There is a strong commitment inside the intelligence community to obey the law, and the community is getting dragged into the mud on this."

General Hayden, who as the head of the N.S.A. supervised the intercept program, is seen by many as a competent professional who was too quick to follow orders without asking enough questions. As one senior congressional staff aide said, "The concern is that the Administration says, 'We're going to do this,' and he does it—even if he knows better." Former Democratic Senator Bob Kerrey, who was a member of the 9/11 Commission, had a

harsher assessment. Kerrey criticized Hayden for his suggestion, after the Times exposé, that the N.S.A.'s wiretap program could have prevented the attacks of 9/11. "That's patently false and an indication that he's willing to politicize intelligence and use false information to help the President," Kerrey said.

Hayden's public confirmation hearing last week before the Senate Intelligence Committee was unlike the tough-minded House and Senate investigations of three decades ago, and added little to what is known about the wiretap program. One unexamined issue was the effectiveness of the N.S.A. program. "The vast majority of what we did with the intelligence was ill-focussed and not productive," a Pentagon consultant told me. "It's intelligence in real time, but you have to know where you're looking and what you're after."

On May 11th, President Bush, responding to the USA Today story, said, "If Al Qaeda or their associates are making calls into the United States, or out of the United States, we want to know what they are saying." That is valid, and a well-conceived, properly supervised intercept program would be an important asset. "Nobody disputes the value of the tool," the former senior intelligence official told me. "It's the unresolved tension between the operators saying, 'Here's what we can build,' and the legal people saying, 'Just because you can build it doesn't mean you can use it.' " It's a tension that the President and his advisers have not even begun to come to terms with.

Articles by: **Seymour M. Hersh**