EXHIBIT D

politics

Tinker, Tailor, Miner, Spy

Why the NSA's snooping is unprecedented in scale and scope.

By Shane Harris and Tim Naftali

Posted Tuesday, Jan. 3, 2006, at 6:30 AM ET

Fifty years ago, officers from the Signal Security Agency, the predecessor to the National Security Agency, visited an executive from International Telephone and Telegraph and asked for copies of all foreign government cables carried by the company. The request was a direct violation of a 1934 law that banned the interception of domestic communications, but Attorney General Tom Clark backed it. Initially reluctant, ITT relented when told that its competitor, Western Union, had already agreed to supply this information. As James Bamford relates in his book *The Puzzle Palace*, the government told ITT it "would not desire to be the only non-cooperative company on the project." Codenamed Shamrock, the effort to collect cables sent through U.S.-controlled telegraph lines ultimately involved all the American telecom giants of the era, captured private as well as government cables, and lasted nearly 30 years. Like other illegal Cold War domestic snooping programs —such as the FBI's wiretaps without warrants and the CIA's mail-opening operations—it collapsed under the weight of public reaction to the abuses of executive power revealed by Vietnam and Watergate.

Today's generation of telecom leaders is similarly involved in the current controversy over spying by the NSA. The *New York Times* reported in December that since 9/11, leading telecommunications companies "have been storing information on calling patterns and giving it to the federal government to aid in tracking possible terrorists." Citing current and former government and corporate officials, the *Times* reported that the companies have granted the NSA access to their all-important switches, the hubs through which colossal volumes of voice calls and data transmissions move every second. A former telecom executive told us that efforts to obtain call details go back to early 2001, predating the 9/11 attacks and the president's now celebrated secret executive order. The source, who asked not to be identified so as not to out his former company, reports that the NSA approached U.S. carriers and asked for their cooperation in a "data-mining" operation, which might eventually cull "millions" of individual calls and e-mails.

Like the pressure applied to ITT a half-century ago, our source says the government was insistent, arguing that his competitors had already shown their patriotism by signing on. The NSA would not comment on the issue, saying that, "We do not discuss details of actual or alleged operational issues."

The magnitude of the current collection effort is unprecedented and indeed marks a shift in how the NSA spies in the United States. The current program seems to involve a remarkable level of cooperation with private companies and extraordinarily expansive data-mining of questionable legality. Before Bush authorized the NSA to expand its domestic snooping program after 9/11 in the secret executive order, the agency had to stay clear of the "protected communications" of American citizens or resident aliens unless supplied by a judge with a warrant. The program President Bush authorized reportedly allows the NSA to mine huge sets of domestic data for suspicious patterns, regardless of whether the source of the data is an American citizen or resident. The NSA needs the help of private companies to do this because commercial broadband now carries so many communications. In an earlier age, the NSA could pick up the bulk of what it needed by tapping into satellite or microwave transmissions. "Now," as the agency noted in a transition document prepared for the incoming Bush administration in December 2000, "communications are mostly digital, carry billions of bits of data, and contain voice, data and multimedia. They are dynamically routed, globally networked and pass over traditional communications means such as microwave or satellite less and less."

The agency used to search the transmissions it monitors for key words, such as names and phone numbers, which are supplied by other intelligence agencies that want to track certain individuals. But now the NSA appears to be vacuuming up all data, generally without a particular phone line, name, or

e-mail address as a target. Reportedly, the agency is analyzing the length of a call, the time it was placed, and the origin and destination of electronic transmissions. Those details would be crucial in mining the data for patterns—according to the officials the *Times* cited, the goal of the NSA's eavesdropping system.

Pattern-based searches are most useful when run against huge sets of data. Many calls and messages must be analyzed to determine which ones are benign and which deserve more attention. With large data sets, pattern-based searching can create more nuanced pictures of the connections among people, places, and messages. Deputy Director of National Intelligence Michael Hayden, who until this year was the NSA director, recently hinted that the NSA's eavesdropping program is not just looking for transmissions from specific individuals. It has a "subtly softer trigger" that initiates monitoring without exactly knowing in advance what specific transmissions to look for. Presumably, this trigger is a suspicious pattern. But officials have not actually described any triggers, raising the question of whether the NSA has been authorized to go on such fishing expeditions.

The government experimented with large-scale pattern-based searches under the auspices of the Defense Department's Total Information Awareness program in 2002. The aim was to sift though government intelligence data, and also privately held information, for telltale signs of the planning of a terrorist attack. TIA was ridiculed as Orwellian. But at least the program tried to create new technologies to protect personal information. Adm. John Poindexter, TIA's creator, believed in the potential intelligence benefits of data-mining broadband communications, but he was also well aware of the potential for excess. "We need a much more systematic approach" to data-mining and privacy protection, Poindexter said at a 2002 conference in Anaheim, Calif., sponsored by the Defense Advanced Research Projects Agency.

Poindexter envisioned a "privacy appliance," a device that would strip any identifiers from the information—such as names or addresses—so that government miners could see only patterns. Then if there was reason to believe that the information belonged to a group that was planning an attack, the government could seek a warrant and disable the privacy control for that specific data. TIA funded research on a privacy appliance at the Palo Alto Research Center, a subsidiary of Xerox Corp. "The idea is that this device, cryptographically protected to prevent tampering, would ensure that no one could abuse private information without an immutable digital record of their misdeeds," according to a 2003 government report to Congress about TIA. "The details of the operation of the appliance would be available to the public."

The NSA's domestic eavesdropping program, however, appears to have none of these safeguards. When Congress killed TIA's funding in 2003, it effectively ended research into privacy-protection technology. According to former officials associated with TIA, after the program was canceled, elements of it were transferred into the classified intelligence budget. But these did not include research on privacy protection.

In January, Congress plans to hold hearings into the legality of the Bush administration's eavesdropping program. Lawmakers will want to know why, if the NSA cannot do its job while remaining within the legal bounds established in the 1970s, the Bush administration did not address that problem in the context of the Patriot Act. Congress might also ask why in the rush to begin data-mining, the NSA has abandoned the privacy controls planned for the TIA. As Adm. Poindexter himself noted in his resignation letter from the program in 2003, "it would be no good to solve the security problem and give up the privacy and civil liberties that make our country great."

Shane Harris, a staff correspondent for National Journal*, writes on intelligence and homeland security. Tim Naftali, the director of the Presidential Recordings Program at the University of Virginia's Miller Center of Public Affairs, is the author of* Blind Spot: the Secret History of American Counterterrorism.

Article URL: http://www.slate.com/id/2133564/
