

Communications Surveillance Foreign and Domestic: Right Decision, Wrong Rules December 2005

Why would the President order the National Security Agency (NSA) to collect information on Americans connected to terrorism without first obtaining the approval of the special court (known as FISA) established to oversee and authorize such activities? This question really has two parts, why NSA, and why without FISA approval. This essay will look at aspects that may help explain what the President got from NSA that he could not get from FBI. NSA has different technical and analytical capabilities than the FBI and it makes sense to give it a greater role in homeland security (defer for a moment the discussion of whether a Presidential edict was the right way to give them this role).

The FBI uses two general methods for communications surveillance. The first is to physically place a device on or near a target's phone or computer. This requires physical access to an individual target's home or office. The second method is to monitor a target's traffic on a communications network at the switch or server. This does not require physical access, but it does require the cooperation of a service provider. In both cases, the collection process is focused on a suspect individual, as is appropriate for law enforcement activities. Both of these can be described as wiretaps.

NSA also has the capability to emplace devices on an individual target's communications equipment, but as part of its larger signals intelligence mission, it can engage in mass collection of certain kinds of communications, particularly international communications. A July 2001 interview in the Washington Post with NSA's Director mentioned "the agency's constellation of spy satellites and its giant listening stations on five continents ...vacuuming communications out of the ether." This collection does not require the cooperation of service providers. All electronic equipment emits some kind of signal. These signals can be detected and collected remotely and covertly. Nations have done so since the dawn of the radio age a century ago. Fiber optic communications, which use light to carry communications rather than electrical signals, pose a special challenge, but can also be collected. Mass collection, in one sense, is a greater encroachment into personal privacy because unlike wiretapping, it is not based on any particular suspicion.

FBI's focus is domestic and on individuals. NSA's focus is international and on networks. FBI does not have the ability to engage in mass collection, nor does it have the analytical capabilities to sort millions of messages in a variety of formats and languages in order to identify those few pieces of traffic that could be of interest for U.S. security.

The distinction between foreign and domestic in the mass collection of international communications is created by policy and law, not by technology. NSA collects international signals. This means that it collects both the foreign and the domestic end of a signal. The technology has not been changed to target Americans; the rules have been changed to release names already collected. Before September 11, when NSA reported on the interception of an international call between a foreign target and an American, the intercept would give the foreign target's name but the name of the American could not appear. Instead, the intercept would read "[US Person]." The name had been collected, but obtaining this name was very difficult, rarely done, and required an overwhelmingly strong and lengthy demonstration of criminal or espionage activity. One of the reasons the

President cited in justifying his action was that NSA had collected communications from two of the September 11 terrorists before the attack, but did not process these communications as they involved a US Person.

NSA is uniquely placed to monitor networks that had both foreign and domestic participants. FBI does not have this foreign monitoring capability. Nor does FBI have the analytical capability to analyze networks. This is more than simple link-analysis. The most important difference is that link analyses connects known participants, while traffic analysis can indicate when there participants who are unknown. Traffic analysis uses statistical and modeling techniques that have been refined with years of experience. Counterespionage services originally developed techniques for network analysis by monitoring mail. By tracking the correspondence of a known spy or terrorist, the service could determine the size of a network, the identity of other participants, distinguish between participants and social acquaintances, and identify leaders (the U.S. had a program to monitor international mail going to the Soviet Bloc, based in the New York and a few other port cities, that did not end until 1973).

NSA has a large pool of analysts and linguists familiar with these and other signals intelligence techniques. It has numerous engineers, mathematicians and computer scientists experienced in monitoring communications and in dealing with the challenges created by new technologies. It has knowledge of foreign terrorist activities and, as part of its mass collection activities, it collects information involving U.S. persons, although this information was not used in the past. FBI, as a domestic law enforcement agency, had none of these capabilities. Most Americans would not want to give a domestic law enforcement agency the capability for mass monitoring of internal communications as this is completely alien to the Constitution's approach to law enforcement and citizens rights.

NSA, with its analytical and linguistic capabilities, with its greater technical resources, and with its ability to collect both domestic and foreign communications, offers unique advantages in a conflict with an opponent like Al Qaeda. Al Qaeda is a loose, informal collection of jihadi cells sprawled across continents and borders. Its members (participants might be a more accurate term) are citizens or residents of many countries, including of the countries they intend to attack. They are sophisticated and use the rights and protections afforded to citizens in the West to shield their activities. Al Qaeda and other jihadist groups do not fit into the neat boxes of foreign and domestic created when the threats to security came mainly from hostile states.

The U.S. has an important opportunity with the contact information found in the cellphones and laptops it captured from terrorists in Afghanistan, Iraq and elsewhere. Of the two agencies, NSA was best placed to exploit this information. This exploitation probably included both traffic analysis based on watching patters of communications (determining who was a member of a terrorist network) and, once a terrorist had been identified, interception and analysis of the content of those communications. Breaking the distinction between foreign and domestic intelligence is crucial for preventing future attacks, and a failure to take advantage of NSA to exploit this captured information fully could create a kind of de facto sanctuary for terrorists.

The FBI could also have sought to monitor international calls by asking service providers for their cooperation. The problem would not have been with either secrecy - phone companies are already capable of keeping wiretaps a secret – or with timeliness – monitoring can begin very quickly. The problem would have been that most telephone companies or other service providers would have been very reluctant to cooperate based on a Presidentially-endorsed request from the FBI rather than a warrant or a court order. Their own lawyers would have strongly advised them against such cooperation. An FBI request to a phone company would not have provided the broad coverage of NSA’s mass collection activities, nor would it have allowed the use of NSA’s analytical capabilities, experience and skills.

An argument could even be made that there are advantages to using NSA rather than the FBI. NSA does not have arrest and enforcement powers. It can identify terrorists, but it cannot take action against them. It must pass this information to law enforcement, which operates under a different and more extensive set of constraints (assuming that these have not also been waived by executive order).

A new role for NSA brings real advantages. The more difficult issue is how to create this new role. A July 2002 CSIS article on what the U.S. needed to do to respond to terrorism recommended the following:

One crucial change may be to reconsider the rules and laws that apply to the National Security Agency, which is responsible for the technical collection of “signals intelligence.” NSA does not collect information on American persons. Changing the rules, among them the Foreign Intelligence Surveillance Act (FISA) to allow NSA to collect information on Americans involved with terrorism could be a crucial part of any new defense.

The emphasis is on reconsideration of rules and laws. This reconsideration could have involved testing FISA, to see if there were surveillance actions that would be rejected. Since its passage, FISA has been misinterpreted and applied in an increasingly restrictive manner (procedures that minimized acquisition efforts, for example, hampered some collection techniques) and damaged counterterrorism efforts. But it is hard to believe that there was a FISA judge in 2002 who have denied action against someone connected to Bin Laden or other jihadis. If this had occurred, it would have greatly strengthened the case for the President’s action.

Even if the FISA process had not been tested and found wanting, it is difficult to believe that an Administration request to modify legislation to allow the use of NSA would have been refused. There were several opportunities to ask Congress to change the applicable laws and it is likely that Congress would have concurred (after some useful debate) if the Administration had sought additional changes to FISA in the Patriot Act or new authorities in the Intelligence Reform and Terrorist Prevention Act. But none of these things was done. Why this is so requires a different and more troubling discussion.