

## **Domestic Communications Surveillance: Right Decision, Wrong Rules**

**James A. Lewis**

Defer for a moment the discussion of whether a Presidential edict was the right method for authorizing the National Security Agency (NSA) to engage in domestic communications surveillance. The means of authorization and the decision not to use the special court (known as FISA) established to oversee and authorize such activities is and should be a subject for scrutiny and debate. Why NSA was authorized is another matter. NSA's technical and analytical capabilities differ significantly from those found at the FBI, and making use of these capabilities for domestic surveillance gives the U.S. an advantage in the defense against terrorist attacks.

The FBI methods for communications surveillance can be generally described as falling into two classes. 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 to the target, 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 methods can loosely 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 communications, particularly international communications. A July 2001 interview in the Washington Post with NSA's then-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 collected remotely and covertly. Nations have done so since the dawn of electronic communications and the U.S. is only one of several nations that engage in this activity. Fiber optic communications, which use light to carry communications rather than electrical signals, pose a special challenge, but can still be collected.

The broad collection of communications by an intelligence agency, in one sense, could be seen as a greater encroachment into personal privacy because unlike wiretapping, it is not based on any particular suspicion. But there is a difference between what NSA collects and what it listens to: the agency uses advanced algorithms and computing capabilities to sort traffic and only a few thousand of the many millions of messages collected are ever heard or seen by a human.

FBI's focus in communications interception is shaped by its law enforcement mission and it is oriented towards domestic activities and individuals. NSA's focus is international and on networks. FBI does not have the ability to engage in mass collection of signals, nor does it have the capabilities needed to sort millions of messages in a wide variety of formats and languages in order to identify those few pieces of traffic that could be of interest.

The differing treatment of foreign and domestic traffic in NSA's 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. It is likely that the technology used by NSA has not been changed to target Americans; rather, it is the rules that have been changed to release names and messages 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 would not appear. Instead, the intercept would read "[US Person]." The name had been collected, but was excluded from use or analysis. Obtaining this US person's name was very difficult, rarely done, and required an overwhelmingly strong demonstration of criminal or espionage activity. One of the reasons the President cited in justifying his action was that NSA had collected communications from some 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 have 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 more sophisticated forms of traffic analysis can indicate when there are participants who are unknown. This kind of analysis uses statistical and modeling techniques that have been refined through years of experience. The intelligence community, beginning in the 1990s, has put considerable effort into developing analytical and decision support software, but these tools are not much used by the FBI. Counterespionage services originally developed techniques for network analysis by monitoring mail flows. By tracking the patterns of correspondence of a known spy or terrorist, the service could determine the number of nodes in a network, the identity of other participants, distinguish between participants and social acquaintances, and identify leaders.<sup>1</sup>

NSA has a large pool of analysts and linguists familiar with these and other signals intelligence analytical 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 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 labeled 'foreign' and 'domestic' that were created when the threats to security came mainly from hostile states. FISA may have unintentionally contributed to the 'stove-piping' of information, by dividing collected

---

<sup>1</sup> The CIA began a program in the 1950s, also warrantless, to monitor international mail between U.S. citizens and the Soviet Union, based in the Post Offices in New York and a few other port cities. The program did not end until 1973. It is worth noting that the 1975 Presidential Commission that reviewed the CIA mail intercept program recommended that future domestic communications interception programs or activities that "otherwise would require a warrant if conducted by law enforcement agencies" should be performed by the FBI, not the intelligence community.

signals into 'foreign' and 'domestic,' each subject to different rules, in a way that no longer fits the technology or the operations of our opponents.

The U.S. gains an important opportunity each time it captures cellphones and laptops from terrorists in Afghanistan, Iraq and elsewhere. These devices contain valuable information that can be used to identify other jihadis. Of the two agencies, NSA is best placed to exploit this information. This exploitation probably includes traffic analysis based on observing patterns of communications (determining who is in contact with 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 terrorist attacks in the United States, and a failure to take advantage of NSA capabilities to exploit this captured information fully could create a kind of de facto sanctuary for terrorists.

The FBI could have sought to monitor international calls by asking service providers for their cooperation. The problem with giving FBI this task would not have been with secrecy - phone companies are already capable of keeping wiretaps a secret - or with timeliness - monitoring can begin very quickly. The problems would have been that telephone companies or other service providers would most likely 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. Additionally, FBI request to a phone company would not have provided the borderless scope of NSA's collection activities, nor would it have allowed the use of NSA's analytical capabilities, experience and skills.

The decision to use NSA highlights a fundamental problem the U.S. has had to face since September 11. Despite the passage of both the Homeland Security Act and the Intelligence Reform and Terrorist Prevention Act, the U.S. has failed to devise a system for satisfactorily conducting domestic intelligence operations. Both laws created new agencies. Both laws provided new authorities. But both the authorities and agencies created by the new laws are inadequate for the task of domestic intelligence. In particular, few would believe that Homeland Security, the new agency Congress created, could or should be responsible for domestic intelligence.

Congress and the Administration could not resolve the domestic intelligence issue. It is an uncomfortable problem. A long series of precedents show that Americans do not like the idea of domestic intelligence operations, and that they have good reason for this dislike. While there was some discussion of creating an U.S. equivalent of MI5 (the British domestic intelligence agency), the idea did not advance very far. Creating an U.S. MI5 would have been too radical a departure from the bureaucratic and legal norms built up around intelligence, counterterrorism and law enforcement. A new agency charged with domestic surveillance would have created serious risks to civil liberties. Addressing the issues of how to confront terrorists who operate with equal ease inside and out of the United States would have required a long and difficult debate. The daunting thicket of legal complexities that surrounds intelligence activities deterred those who wanted quick passage of legislation.

The debate over 'data mining' may have helped to complicate the issue. By suggesting that counter-terrorism required the collection and analysis of massive amounts of information on routine activities by all Americans (credit cards, travel, internet searches), data mining made domestic surveillance seem to hold unmanageable risk. In fact, any program that monitors all Americans is unnecessary and unproductive for counterterrorism. This sort of program would

create unmanageable risks for civil liberties and reduce the efficiency of counter-terror efforts by generating mounds of worthless information. A more focused surveillance program that uses information collected by foreign intelligence programs to identify persons of interest for domestic surveillance would be more effective in identifying terrorists and disrupting their operations. If this targeted surveillance is what NSA is doing, it has helped counter-terrorism efforts, but the surveillance necessary for this sort of targeted approach may not always be based on information that meets the current standards required by the FISA process.

The provisional solution to the domestic intelligence problem was to announce that the FBI would take on the domestic intelligence role. But it will take years to create a new intelligence capability at the FBI, to recruit analysts and linguists, to create organizational structures for reporting and to develop a culture and orientation of intelligence rather than law enforcement among agents. If the Administration had relied on this fledgling FBI capability, a weak DHS and the strictures of FISA, the U.S. would have been more vulnerable to the new kind of opponent it faces today. Instead, the administration appears to have decided (and to have briefed Congressional leaders from both parties on its decision) to involve NSA in domestic collection. The administration's argument – that the President had the authority and that adequate oversight was provided – will be severely tested in the upcoming Congressional hearings.

The upcoming hearings may not address the more difficult questions – to what extent do we need improved domestic intelligence capabilities for effective counterterrorism and what limitations, authorities and oversight are required for any new program. The answer to these questions is neither a return to the FISA status quo nor assertions of executive authority, although these are likely to be offered up by the contending parties.

Effective counterterrorism needs a reconsideration of rules and laws that apply to intelligence. This reconsideration could have involved testing FISA, to see if there were necessary surveillance actions that the court, operating under its old rules, would reject. Since its passage, FISA has been applied in an increasingly restrictive manner (procedures that minimized acquisition efforts, for example, hampered some collection techniques). This is not surprising. A bureaucracy dominated by lawyers has a tendency for creeping legalism and caution. 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 a FISA request had made and been denied, it would have greatly strengthened the case for the President's action, but there is no indication that such a denial occurred.

Even if the FISA process had not been tested and found wanting, it is also difficult to believe that an Administration request to modify legislation to allow the use of NSA would have been refused by congress. 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 were done. Why this is so requires a different and more troubling discussion.