CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

CRITICAL QUESTIONS

Domestic Surveillance, FISA, and Terrorism

James Lewis
November 7, 2007

The Bush administration entered office with the intent of restoring, in its view, executive branch authorities and presidential prerogatives. The attacks of September 11 and the wars in Afghanistan and Iraq reinforced the notion that the president's constitutional authority as commander in chief provided sweeping powers that were sufficient to authorize a range of actions for defense. Among these actions was the authorization of a program in which the National Security Agency (NSA), the U.S. agency responsible for collecting communications intelligence, would begin surveillance of the electronic communications of U.S. citizens and residents without first obtaining an approval (in the form of a warrant) from the special court established precisely for this purpose.

That court, the Foreign Intelligence Surveillance Court (FISC), was created as part of reforms made in the 1970s in response to perceived excesses of U.S. intelligence agencies. Before passage of the Foreign Intelligence Surveillance Act (FISA), the president had broad scope to conduct intelligence operations without congressional or court oversight. Vietnam, the Watergate scandal, and revelations of the frequent misuse of domestic surveillance dating back to the 1950s made this untrammeled presidential authority seem unwise. In 1978, Congress established new congressional committees for intelligence oversight and, under FISA, created rules for domestic surveillance and the FISC to authorize such surveillance under a warrant and oversee it.

During the intervening decades, critics charged that FISA had become somewhat sclerotic. The National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) was told that "the process for getting FISA packages approved at Federal Bureau of Investigation (FBI) Headquarters and the Department of Justice was incredibly lengthy and inefficient." The 9/11 Commission concluded that errors in processing FISA surveillance requests likely contributed to the success of the 9/11 attacks. Some of FISA's 9/11 shortcomings may have been the result of timidity and misinterpretation of the law by officials at various agencies, but this failure does not detract from the need to rethink FISA—the technological and political assumptions of the 1970s do not fit the post–9/11 world.

Congress wrote FISA to focus on the surveillance of the employees and agents of foreign states rather than unknown members of informal religious groups. In addition, FISA was modeled on the communications technologies of a simpler age. Communications now rely on globally connected networks based on packet switching (in which messages are broken into small, discrete pieces, sent over many different routes, and then reassembled into a single message, rather than the single, end-to-end connections of the 1970s). FISA has been amended to better fit new technologies, but it needs reconceptualization rather than patchwork fixes.

The perception of FISA's inefficiency and the desire to restore executive branch authorities combined to transform an emergency request for warrantless surveillance immediately after the 9/11 attacks into a permanent program authorized by the president alone. The presidential surveillance program began to unravel, however, shortly after it became public knowledge in December 2005. We are told that the program is essential for defense against terrorism, and this is probably true. Simply ending it and going back to the practices of the 1990s would put the United States at risk. On the other hand, assertions that presidential authority alone is sufficient for authorization and oversight of domestic surveillance do not withstand scrutiny. In January 2007, facing a range of legal and legislative challenges, the administration agreed to put the NSA domestic surveillance program under FISA court oversight. In May 2007, the court lived up to its critics' fears when, according to the director of national intelligence, one of its judges issued an order that made collection under the program more difficult. To remedy this, Congress passed a six-month stop-gap authorization (the "Protect America Act") in August 2007. The act, however, does not address a number of crucial issues. Congress needs to rewrite FISA so that it better meets the security challenges that the United States faces today.

The features of an improved FISA would include the ability to differentiate between activities that need high evidentiary standards and those that do not and between activities that require a warrant and those that can be authorized in some other way. FISA needs to accommodate programmatic surveillance, in which patterns in Internet or telephone traffic point to suspicious activity. There have been steps to adjust FISA to current communications technologies, but more needs to be done.

FISA needs to allow some surveillance activities without a warrant or at least without the greater evidentiary requirements needed for conventional warrants. FISA needs to distinguish between activities (such as actually listening to a conversation) that absolutely require a warrant and those activities that can be conducted under some other authorization. FISA needs clear procedures that allow the president or attorney general to begin surveillance immediately in the case of an emergency and continue it for some time. From Congress, FISA activities need better oversight; from this or subsequent administrations, FISA needs better management so that the processes for getting a warrant application before the court do not become so cumbersome that they damage security.

Q1: Should all surveillance require a warrant?

A1: It is unlikely that the warrantless surveillance program involved more than listening to phone conversations, and the oft-repeated charge that NSA listened to millions of American's conversations is silly. NSA probably listened to a few conversations—after sophisticated software programs identified one phone number as linked to another number of a person potentially involved in terrorism. This can be done without listening to the conversation at all—the physical equivalent is looking at the address on an envelope but not reading the letter. Reading the electronic addresses should not require the same sort of authorization as actually listening to the conversation; conversely, a decision to go beyond looking at addresses and actually listening should never be done without a warrant. Communications surveillance is the only method that can provide a broad national or global overview of terrorist activity. It is invaluable for security. At the same time, however, it is a fishing expedition: NSA's computers look for patterns that suggest someone is interesting. If FISA extended the idea of a programmatic or umbrella warrant, in which surveillance was not focused on a specific individual or the content of their communications, with carefully defined thresholds for surveillance activities, these activities could be authorized under warrant by the court.

Q2: The Constitution says you need probable cause for searches and seizures—should this be the standard for FISA?

A2: The drafters of the Constitution wanted to restrict police powers for surveillance without approval of a court and require that this approval only be granted when there is "probable cause" that a crime has been committed. FISA used a modified version of probable cause—that the target of surveillance is probably an agent of a foreign power (including non-state groups like Hamas). Probable cause is perhaps too high a standard, however, for dealing with the clandestine, informal organizations that make up jihad, and the jihadis have exploited civil liberties protection to advance their operations. FISA would benefit if it was more flexible in its requirements for less intrusive surveillance activities. There are different evidentiary standards that could trigger less intrusive surveillance, such as "reasonable suspicion" (this is the standard used in some European democracies). A revised FISA that allowed some surveillance activities under reasonable suspicion, while restricting more intrusive measures to probable cause, could be better suited to today's conflicts. A surveillance program that monitored who talked to whom when there was a reasonable suspicion of involvement with terrorism (say that the phone number had been found on the cell phone of a terrorist captured in Iraq) but only listened to the content of those conversations under warrant might meet constitutional requirements.

Q3: How can FISA procedures be streamlined?

A3: One of the major problems with FISA is the cumbersomeness of the procedures that have grown up around it. Applications for FISA surveillance are held to very high standards of evidence and drafting that are inappropriate for counterterrorism. The attorney general creates these procedures, and legislation could encourage him to do a better job of managing the process of applying for a warrant so that it does not again become an obstacle. One way to focus attention on this administrative problem would be to require a report to the public and to Congress on how many days it takes, with no "stopping-the-clock" exceptions, for a request from the field to become an application to the court.

Q4: What is the distinction between foreign and domestic communications?

A4: The distinction between foreign and domestic communications was a linchpin of the 1978 act, but unfortunately, technology has eroded that distinction. FISA was careful to carve out intelligence collection of radio signals (an NSA mission) from court oversight. As telecommunications moved from satellites (a radio signal) to fiber optic cables (which the law defined as a wire and subject to the court), more foreign intelligence activities became subject to FISA than were originally intended. The Protect

America Act helped to fix this problem by making clear that FISA does not apply when foreign persons outside of the United States are under surveillance, even if the communication passes through (and is intercepted) domestically. FISA should be drafted to be technologically neutral and to carefully clarify that protections apply to citizens and residents of the United States, not communications that are just passing through.

Q5: Should the telephone companies be held liable (and then compensated for their liability)?

A5: Should the telephone companies be held liable for complying with a request from the attorney general or the president that was declared fully legal? The answer in part of the civil liberties community is yes, punish them. A halfway point is the idea that the telephone companies should be allowed to be sued and, if found liable and fined, compensated by the government for their punishment. Both notions are bad if the goal is the long-term security of the country. FBI and NSA need the cooperation of the companies even with a warrant. Companies will be less willing to cooperate once we set the pattern of a president swearing them to secrecy and then telling them that cooperation is legal, only to yank the rug out from under them later in court. The precedent is that if a citizen helps police officers at their request in an activity that appears legal, the citizen is not liable. We do not want a situation in which the next time there is an emergency people drag their feet out of fear of being sued.

James Lewis is a senior fellow and director of the Technology and Public Policy Program at the Center for Strategic and International Studies in Washington, D.C.