The new FISA compromise: it’s worse than you think

With the Senate set to vote on FISA amendments this week, Ars examines the …

by **Timothy B. Lee** - July 7 2008, 11:30pm CDT

Telco immunity is the icing, not the cake

Last month, the House of Representatives passed the FISA Amendments Act of 2008, Congress's latest response to President Bush's demands for expanded eavesdropping authority. The Democratic leadership, seemingly intent on avoiding real debate on the proposal, scheduled the final vote just a day after the bill was introduced in the House. Touted by Democratic leaders as a "compromise," it was supported almost unanimously by House Republicans and opposed by a majority of Democrats.

The 114-page bill was pushed through the House so quickly that there was no real time to debate its many complex provisions. This may explain why the telecom immunity provision has received so much attention in the media: it is much easier to explain to readers not familiar with the intricacies of surveillance law than the other provisions. But as important as the immunity issue is, the legislation also makes many prospective changes to surveillance law that will profoundly impact our privacy rights for years to come.

Specifically, the new legislation dramatically expands the government's ability to wiretap without meaningful judicial oversight, by redefining "oversight" so that the feds can drag their feet on getting authorization almost indefinitely. It also gives the feds unprecedented new latitude in selecting eavesdropping targets, latitude that could be used to collect information on non-terrorist-related activities like P2P copyright infringement and online gambling. In short, the FISA Amendments Act of 2008 opens up loopholes so large that the feds could drive a truck loaded down with purloined civil liberties through it. So the telecom immunity stuff is just the smoke; let's take a look at the fire.

The importance of judicial scrutiny

The most fundamental question in the FISA debate is whether judicial oversight will be required when the government spies on international communications originating on American soil. FISA has never limited spying on purely foreign communications, but under current law, the government must obtain court approval to tap a phone line or fiber optic cable in the United States, even if the other end of the communication is abroad. An application for a FISA warrant must specify the person or organization being targeted and present evidence that the target is an "agent of a foreign power," such as the Chinese government or Al Qaeda.

The Bush administration has chafed at these restrictions, insisting that the president has the inherent authority to eavesdrop on suspected terrorists without court oversight. Director of National Intelligence Mike McConnell argues that that the FISA process is so cumbersome that it impedes the intelligence community's efforts to spy on terrorists.

Civil libertarians disagree, noting that FISA sets a lower bar for approving surveillance than the process for obtaining ordinary criminal warrants. And in emergency cases, FISA allows the government to begin spying immediately and seek a warrant after the fact. Most importantly, civil liberties groups emphasize that without judicial oversight, there is no way to know if the government is respecting any limits that Congress establishes.

Consider, for example, the case of National Security Letters, administrative subpoenas that the Patriot Act allows the FBI to issue without court oversight. Last year a government audit last year foundhundreds of cases in which the FBI had issued NSLs without following even the permissive rules of the Patriot Act. Civil libertarians warn that similar corner-cutting is inevitable if the NSA is allowed to choose eavesdropping targets without judicial scrutiny.

No individual warrants for international calls

When it comes to judicial oversight of domestic-to-foreign calls, the legislation the House passed last month is an unambiguous victory for the White House and a defeat for civil libertarians. The legislation establishes a new procedure whereby the Attorney General and the Director of National Intelligence can sign off on "authorizations" of surveillance programs "targeting people reasonably believed to be located outside the United States." The government is required to submit a "certification" to the FISA court describing the surveillance plan and the "minimization" procedures that will be used to avoid intercepting too many communications of American citizens. However, the government is not required to "identify the specific facilities, places, premises, or property" at which the eavesdropping will occur. The specific eavesdropping targets will be at the NSA's discretion and unreviewed by a judge. Moreover, the judge's review of the government's "certification" is much more limited than the scrutiny now given to FISA applications. The judge is permitted only to confirm that the certification "contains all the required elements," that the targeting procedures are "reasonably designed" to target foreigners, and that minimization procedures have been established.

Crucially, there appears to be no limit to the breadth of "authorizations" the government might issue. So, for example, a single "authorization" might cover the interception of all international traffic passing through AT&T's San Francisco facility, with complex software algorithms deciding which communications are retained for the examination of human analysts. Without a list of specific targets, and without a background in computer programming, a judge is unlikely to be able to evaluate whether such software is properly "targeted" at foreigners.

The House legislation also drastically extends the timeline for reviewing surveillance activities, potentially allowing the government to commence eavesdropping and then drag out judicial review for months. Under existing law, the government must obtain judicial approval within 72 hours of the start of emergency wiretapping. In contrast, the judicial review of "certifications" can stretch out as long as four months. After beginning eavesdropping, the government has a week to submit its "certification" to the FISA court, which has 30 days to review the application. If the judge finds problems with the certification, the government can continue eavesdropping for another 30 days before it is required to comply with the order. And the government can buy *still more* time by filing an appeal to the FISA Court of Review. The appeals court may take as long as 60 days to make its decision, and the government will often be allowed to continue eavesdropping throughout the process of judicial review. This means that in many cases, the government will have completed its spying activities long before the courts reach a decision on its legality.

No "targeting" Americans

The legislation does provide modestly enhanced protections for Americans living overseas. The "authorizations" described in the previous section are only available when they "target" those who are not American citizens or legal residents. When the target of an eavesdropping program is an American, the government must satisfy more stringent requirements, including the traditional requirement that the target is an "agent of a foreign power." The surveillance also must cease within seven days if judicial approval for it is not forthcoming.

This section is a modest restriction on the government's prior eavesdropping powers. Traditionally, FISA did not govern purely overseas eavesdropping activities, even if they targeted American citizens. Under the new legislation, the government will need court approval to "target" Americans overseas, even when the surveillance is conducted overseas.

However, as a practical matter, this enhancement of Americans' privacy rights may prove extremely limited. The government may not "target" Americans under the broad "authorizations" discussed in the previous section, and in some cases the government may discard information obtained about Americans as part of the required

"minimization" procedures, but the government would retain significant latitude to decide which information it retains. The paradoxical consequence is that broader wiretapping orders may be approved more easily than narrower ones. For example, the government could not unilaterally "authorize" the "targeting" of a particular San Francisco resident's international communications. However, it could "authorize" a dragnet surveillance program that intercepted the international communications of all San Francisco residents under the pretext that it was "targeting" any foreign terrorists who might happen to communicate with San Francisco residents.

This is particularly troubling when we remember that in 2002, the Foreign Intelligence Surveillance Court of Review held that FISA does not prohibit coordination between foreign intelligence gathering and domestic law enforcement. That suggests that the FBI could ask the NSA to tailor its filters to intercept evidence of Internet gambling, copyright infringement, or other ordinary crimes. The Americans whose communications were turned over could not be the "target" of the surveillance, but the House legislation requires only that foreign intelligence gathering be "a significant purpose" of eavesdropping programs. If a terrorist surveillance program also catches American citizens who are gambling or infringing copyright law, that's even better!

Other provisions

As has been widely reported, the legislation would grant broad, retroactive immunity to firms that participated in the president's warrantless surveillance program. The bar for granting immunity is extremely low: to receive immunity, the firm must merely demonstrate that it had received a letter from the government stating that the program was lawful. Since we already know that the program participants received such letters, there is no practical difference between this standard and blanket immunity.

The legislation expands the list of people who can be spied on to include those engaged in "the international proliferation of weapons of mass destruction." And curiously, it has an extremely broad definition of "weapons of mass destruction." It includes not only nuclear, chemical, and biological weapons, but also "any explosive, incendiary, or poison gas that is designed, intended, or has the capability to cause a mass casualty incident." As Wired's Jason Sigger points out, this is significantly broader than the traditional definition. The legislation mandates that the Inspectors General of each agency involved in FISA surveillance prepare reports to Congress detailing the nature and extent of post-September 11 surveillance activities.

Democratic leaders have made much of a provision designating FISA (along with ordinary criminal wiretapping procedures) as the "exclusive means" for intercepting electronic communications. But as a ruling last week made clear, this provision is little more than window dressing. Republican-appointed judge Vaughn R. Walker ruled last week that the 1978 FISA statute established "the exclusive means for foreign intelligence surveillance activities to be conducted." If the president ignored the exclusivity provisions of the current iteration of FISA, it's not clear what is accomplished by adding another one.

Compromise or capitulation?

Democratic leaders have worked hard to portray the legislation as a compromise, but close examination of its provisions suggests that it is an unvarnished victory for President Bush and his allies in Congress. The legislation eliminates meaningful judicial oversight of eavesdropping between Americans citizen and foreigners located overseas and effectively legalizes dragnet surveillance of domestic-to-foreign traffic. It stretches out the judicial review process so much that the government will in many cases be able to complete its surveillance activities before the courts finish deciding on its legality. And Democratic leaders have capitulated on the immunity question, agreeing to language that would almost certainly lead to retroactive immunity for lawbreaking telecom companies.

Many supporters of Barack Obama were dismayed last month when he announced that he would support the legislation. Indeed, more than 20,000 have joined a group on his campaign website urging him to reject the bill; the group is now the largest on his website. But thus far, Obama has maintained his support for the bill.

Last week, an Obama surrogate insisted that "with FISA expiring," the bill was the best Democrats could hope to get. The only problem is that FISA *isn't* expiring. It was enacted in 1978 and is not scheduled to sunset. The Protect America Act did expire in March, but given that the Bush administration managed to prevent terrorist attacks under FISA for almost six years until last summer's passage of the Protect America Act, it's hard to be too alarmed about living under FISA again for the final six months of Pres. Bush's term.

The Democrats' capitulation is particularly puzzling because, as we've pointed out before, the Democrats' firm stance on FISA this Spring turned out to be a political asset, not a liability. When House Democrats called Pres. Bush's bluff and allowed the Protect America Act to expire in March, it got a wave of positive coverage from the media, which pointed out that the PAA's expiration would have little effect on the government's ability to spy on terrorists. Now that Democratic leaders are switching sides yet again, we've seen the re-emergence of unflattering coverage focusing on the Democrats' weakness on national security issues and lack of party unity. Protecting civil liberties ought to be a matter of principle, but even if Democratic leaders are unmoved by civil liberties concerns, one might have expected them to stand up to the White House based on purely political motivations.

Civil libertarians' last stand against expanded government surveillance will occur in the Senate, in a vote that is expected to occur this week. So far, the determined opposition of a small group of Senators led by Chris Dodd and Russ Feingold has managed to stall the legislation for a couple of weeks. Dodd has signaled that he will continue using every weapon at his disposal to stop the legislation. But with Democratic leaders lining up in support of the bill, Dodd and Feingold face an uphill battle.

http://arstechnica.com/tech-policy/2008/07/fisa-compromise/