CATO AT LIBERTY

AUGUST 21, 2012 5:11PM

What the Manual by DOJ's Top Intelligence Lawyer Says About the FISA Amendments Act

By JULIAN SANCHEZ

To a casual observer, debates about national security spying can seem like a hopeless game of he-said/she-said. Government officials and congressional surveillance hawks characterize the authorities provided by measures like the FISA Amendments Act of 2008 in one way, while paranoid civil libertarians like me tell a more unsettling story. Who can say who's right?

Fortunately, there is an authoritative unclassified source that explains what the law means: the revised 2012 edition of *National Security Investigations and Prosecutions* by David S. Kris (who headed the Justice Department's National Security Division from 2009–2011) and J. Douglas Wilson. As the definitive (unclassified) treatise on what foreign intelligence surveillance law says, means, and permits, it's the same resource you'd expect the government attorneys who apply for surveillance authority to consult for guidance on what the law does and doesn't allow spy agencies to do. Let's see what it says about the scope of surveillance authorized by the FAA:

> [The FAA's] certification provision states that the government under Section 1881a is "not required to identify the specific facilities, places premises, or property at which an acquisition … will be directed or conducted." This is a significant grant of authority, because it allows for authorized acquisition—surveillance or a search—directed at any facility or location. For example, an authorization targeting "al Qaeda"—which is a non-U.S. person located abroad—could allow the government to wiretap any telephone that it believes will yield information from or about al Qaeda, either because the telephone is registered to a person whom the government believes is affiliated with al Qaeda, or because the government believes that the person communicates with others who are affiliated with al Qaeda, regardless of the location of the telephone. Unless the FISC attempts to address the issue under the rubric of minimization, no judge will contemporaneously review the government's choice of facilities or places at which to direct acquisition. [….] Review of the certification is limited to the question "whether [it] contains all the required elements"; the FISC does not look behind the government's assertion's. Thus, for example, the FISC could not second-guess the government's foreign intelligence purpose of conducting the acquisition, as long as the certification in fact asserts such a purpose.

Got that? The requirement that surveillance have a foreign "target" is satisfied if the general purpose of a wiretap program is to gather information *about* a foreign *group* like al Qaeda, and it employs procedures designed for that purpose. It does *not* mean that the particular phone numbers or e-mail accounts or other "facilities" targeted for surveillance have to belong to a foreigner: those could very well belong to an American citizen located within the United States, and no court or judge is required to approve or review the choice of which individuals to tap.

Kris and Wilson elaborate in a discussion of surveillance under the Protect America Act, the stopgap legislation that preceded the FAA, explaining how the language of the law could be exploited to conduct what most of us would think of as domestic surveillance despite the nominal requirement of a "foreign" target:

> The concern was that the government could be said to "direct" surveillance at the entity abroad, but still monitor communications on a facility used (or used exclusively) by an individual U.S. person in this country. Indeed, **the government in the recent past had taken the position that surveillance of a U.S. person's home and mobile telephones was "directed at" al Qaeda, not at the U.S. person himself. Applied to the PAA, this logic seemed to allow surveillance of Americans' telephones and e-mail accounts, inside the United States, without adherence to traditional FISA, as long as the government could persuade itself that the surveillance was indeed "directed" at al Qaeda or another foreign power that was reasonably believed to be abroad.** When confronted with these concerns the government explicitly equated the PAA's "directed at" standard with FISA's "targeting" standard, meaning that acquisition was "directed" at an entity when the government was trying to acquire information from or about that entity.
>
> More importantly for present purposes, the government's equation of the "targeting" and "directed at" standards meant that **concerns raised about the PAA applied equally to the FAA**, which (as discussed above) authorizes acquisition "targeting" a "person" reasonably believed to be abroad, and explicitly adopts traditional FISA's broad definition of the term "person." **The concern was that the government could use Section 1881a for an acquisition "targeting" al Qaeda, but "directed" at a facility or place used (or used exclusively) by John Smith, a U.S. person located in the United States, for Smith's domestic communications.** [Emphasis added.]

As Kris and Wilson note, Congress ultimately added a further limitation designed to allay such concerns, but it did *not* do so by prohibiting any flagging of Americans' e-mail accounts or phone lines for interception and recording without a warrant. *That is still allowed*—though "minimization procedures" are then supposed to limit the retention and use of such information.

What Congress prohibited instead was the use of FAA surveillance to "intentionally acquire any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States." But as Kris and Wilson point out, this restriction "is imperfect because location is difficult to determine in the modern world of communications, and the restriction applies only when the government 'knows' that the communication is domestic."

So to review: under the FAA, a court approves general procedures for surveillance "targeting" a foreign group. But the court does not approve or (necessarily) review any intelligence agency's own discretionary determination about which specific people's e-mail addresses, phone lines, or online accounts should be flagged for interception in order to gather information about that foreign group. The government's past arguments indicate that it believes it may spy on the accounts or phones of individual American citizens located in the United States under an authorization to gather information *about* a foreign "target." All the law requires is that they not *intentionally* record the American's calls and e-mails when they are are *known in advance* to be to or from another American.

Remember: this isn't my interpretation of the law. This isn't speculation from someone at the American Civil Liberties Union or the Electronic Frontier Foundation about how the government *might* try to read the statute. This a legal reference text written by the lawyer who, until quite recently, ran the show at DOJ when it came to FISA surveillance. The next time you hear a member of Congress declare that the FAA has nothing to do with eavesdropping on Americans, ask yourself who is more likely to have an accurate understanding of what the law really says.

Topics: Foreign Policy and National Security, Law and Civil Liberties

Tags: Al Qaeda, department of justice, doj, FAA, FISA, protect america act, spying, wiretaps

This work by Cato Institute is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.

PRINTED FROM CATO.ORG