

Foreign Intelligence and Surveillance Act Fact Sheet
Colonel Teddy Bitner, US Army (Retired)

Bottom Line Up Front: The 1978 Foreign Intelligence and Surveillance Act (FISA) needs immediate revision to ensure national security while protecting US citizens' Fourth Amendment rights. Delay in revising or terminating the Act may result in critical failures to detect or prevent terrorist actions against citizens of the United States or our interests abroad.

Background:

Congress enacted the FISA law in 1978 in reaction to President Nixon's unconstitutional surveillance of American citizens. The purpose of the law was to limit a President's ability to surveil American citizens by providing for the requirement for a court order before a wiretap could be installed. Consequently, the law established four categories for which warrants must first be obtained before electronic surveillance could be used:

- (a) those involving a particular, known American citizen or permanent resident alien *who is in the United States* and has intentionally been targeted for monitoring, no matter whether the interception takes place inside or outside the United States;
- (b) those involving someone *inside the United States*, even if that person has not been intentionally targeted, if the interception occurs within the United States;
- (c) those in which all parties to the communication are located *within the United States*; and
- (d) those rare contacts which are neither radio nor wire communications, "in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes."

Obviously, none of the above categories involve foreign-to-foreign communications. However, in 2007, a FISA court judge ruled that since foreign-to-foreign communications are routed through the United States (but not terminating in the US), the US government is then required to obtain a court order before it can listen to overseas terrorist communications. The ruling means that, for example, it is illegal for the NSA or CIA to monitor terrorist communications originating in Pakistan and terminating in Germany that is routed through a switch or server located in the US (which includes virtually all international communications world-wide). This ruling temporarily shut down monitoring of overseas terrorist communications and put telecommunications companies which cooperated with the US Government (believing that FISA did not cover overseas communications as detailed in the legislative language above) at risk of lawsuit or prosecution.

In August 2007, Congress passed legislation that provided temporary relief to the FISA requirements for six months, in order to provide time to put together new legislation to amend FISA. The six months ended in February with the Senate passing a revised statute, while the House refused to compromise on a provision that would protect telecommunication companies,

who believed they were operating within the framework of the law prior to the FISA court ruling from lawsuits or prosecution.

As it now stands, CIA and NSA are required to seek probable-cause judicial warrants to surveil terrorists in Iraq, Afghanistan, and elsewhere around the globe. The burden imposed by this ruling brings tens of thousands of enemy communications under FISA's arduous legal procedures, all of which benefits Osama bin Laden and his associates, treating them as if they were US citizens, protected under the Fourth Amendment. In essence, this ruling shuts down intelligence collection on overseas terrorists. .

While the requirement may seem reasonable on the surface, in fact, obtaining a FISA court ruling on a wiretap is a long and arduous process. A classic example is the case of Coleen Rowley, the FBI agent who attempted to obtain a FISA warrant to review the contents of Zacarias Moussaoui's computer. "(She) ran up against a number roadblocks in her effort to secure a FISA warrant in the case of Zacarias Moussaoui, the al Qaeda operative who had taken flight training in preparation for the hijackings. Investigators wanted to study the contents of Moussaoui's laptop computer, but the FBI bureaucracy involved in applying for a FISA warrant was stifling, and there were real questions about whether investigators could meet the FISA court's probable-cause standard for granting a warrant. FBI agents became so frustrated that they considered flying Moussaoui to France, where his computer could be examined. But then the attacks (of September 11, 2001) came, and it was too late."¹

Position

Congress should modify FISA to clarify the US Government's ability to monitor communications originating and terminating overseas, regardless of how the communications are routed. The legislation should also provide immunity for telecommunications companies that cooperated with the US Government prior to the FISA court decision, believing under the plain language of FISA, that their participation in counter-terrorist surveillance efforts were perfectly legal.

¹ Byron York, "Why Bush Approved the Wiretaps", December 19, 2005, *National Review Online*, accessed February 22, 2008.