WebMemo
Published by The Heritage Foundation
No. 1782
January 25, 2008

The Intelligence Community Needs Clear—and *Permanent*—FISA Reform

Robert Alt, Todd Gaziano, and Brian W. Walsh

The Senate is on the verge of passing legislation to extend the important intelligence surveillance authorities of the Protect America Act, passed six months ago. Those authorities, set to expire on February 1, allow the intelligence services to conduct surveillance of communications between persons located outside of the United States when the communications happen to pass through domestic networks. Without this fix, approving such intercepts of solely international communicants would become an even lengthier and more onerous process—one never intended even by the Congress that passed the Foreign Intelligence Surveillance Act (FISA)—to the great detriment of national security.

In addition, the Senate legislation grants retroactive immunity to telecom providers that, in good faith, worked with the government in its surveillance programs, a fair and crucial step to encourage future cooperation on security matters. As one astute commentator has explained, "The telecoms know the technology better than anyone else. If we are going to keep a step ahead of the people trying to kill us, the intelligence community needs the top experts in the tent helping us—help you can't expect to get if you create a climate where they have to fear they will be sued for providing it."[1] For now, however, the House has rejected that measure, though negotiations with the Administration continue.

The war on terrorism is not a brief skirmish but a long war, and the tools needed to wage it should therefore not be hobbled by artificial expiration dates imposed for political advantage. According to some reports, current FISA legislation may be saddled with a one-month expiration date. This would be counterproductive. Continuity of intelligence operations requires continuity of authorities, not constantly shifting sunsets and a fluid legal structure. Congress should expand and make permanent the FISA reforms in the Protect America Act and grant retroactive immunity to telecom companies that have done their part to strengthen national security. These steps are necessary to avoid hobbling America's wartime intelligence-gathering abilities.

Need for Modernization. The House passed the Protect America Act of 2007 (PAA) on August 4, 2007, and the President signed it into law the next day. Despite the disclaimers by Members of Congress who want to create a more restrictive regime for gathering intelligence on terrorists, the PAA passed because it had bipartisan support and because Director of National Intelligence (DNI) Mike McConnell spoke personally with approximately 260 Members. He explained why the PAA was necessary to remedy the damage caused by an unprecedented and seemingly erroneous decision by the Foreign Intelligence Surveillance Court in May 2007.[2] The decision opened an intelligence gap by effectively requiring the federal government, for the first time ever, to obtain a FISA warrant for

This paper, in its entirety, can be found at:
www.heritage.org/Research/HomelandSecurity/wm1782.cfm

Produced by the Center for Legal and Judicial Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

any surveillance of persons located overseas if their electronic communications (e.g., emails, cell-phone calls, and text messages) might possibly be routed through the United States.

Because significant advances in technology that change how calls and packets of data are routed have occurred since the passage of FISA in 1978, and because most of the world's largest telecommunications and Internet service providers are located in the United States, this would have required a FISA warrant for surveillance of potentially every person located overseas. No one could know in advance whether any communication by a person located outside the United States might end up being routed through the United States. DNI McConnell disclosed that thousands of individuals overseas are being monitored for terrorist activities. Obtaining approval for each intercept would be nearly impossible.

Each FISA application requires approximately 200 person-hours of government attorneys' and other intelligence officials' time for each telephone number intercepted. Only about 100 persons are being monitored in the United States, but this alone requires the equivalent of full-time service of ten government attorneys or other intelligence officials just to prepare the FISA applications.[3] Thousands of persons outside of the United States are being monitored for terrorism-related activities. For every thousand, 100 government officials would have to spend a year working fulltime to prepare all of the FISA applications. As former National Security Administration General Counsel Robert L. Dietz noted in congressional testimony concerning revising FISA: "My concern is analyst time. And the issue that most concerns us is counterterrorism experts and analysts do not grow on trees. And every time I've got five or 10 or 15 or 20 counterterrorism experts working FISA factual issues, that's time when they're not trying to stop the enemies of the United States."[4] This is not the formula for a nimble and effective international intelligence regime.

Furthermore, a series of repeated "sunsets" does not provide the intelligence community with the clarity, certainty, or tools necessary to perform their vital work. Investigations that are vital to national security on January 31 will also be vital on February 2. Simply extending the bill for 30 more days does not provide intelligence gatherers with the kind of guidance and consistency requisite to perform the kind of long-term, strategic intelligence collection that the war on terrorism requires.

Members of Congress who now publicly express regret about their vote to enact the Protect America Act should trust their original instincts rather than be swayed by unfounded hypothetical harms or the potential for partisan gain. A bipartisan majority recognized last August that if Congress failed to act, it would expose tens of thousands of Americans to a heightened risk of injury and death at the hands of terrorists. Unfortunately, the sky-is-falling rhetoric of privacy absolutists seems to have swayed some Members since.

Conclusion. The Protect America Act wisely exempted intelligence gathering targeted at persons not on U.S. soil. This makes perfect sense because constitutional protections were never intended to extend to intelligence gathering for national security purposes to persons located outside of the United States. It relies on the same minimization procedures that have always applied to reduce the intru-

1. Andrew C. McCarthy, *FISA Deal on the Horizon*, at *www.defenddemocracy.org//in_the_media/in_the_media_show.htm?doc_id=555915*.
2. Although this secret court decision was never released, it seems erroneous based on news reports citing officials who have reviewed it. The conclusions these officials have drawn from their review are the only available public source for evaluating the decision's merits, and the decision thus may have had the effect of chilling more intelligence gathering conduct than its holding necessarily required.
3. This estimate assumes that a workweek is at least 40 hours and that each government attorney or other intelligence official spends all of his or her time working on nothing other than FISA applications.
4. *Hearing on Legislative Proposals To Update the Foreign Intelligence Surveillance Act (FISA) Before the Subcommittee on Crime, Terrorism, and Homeland Security of the House Judiciary Committee*, 109th Cong. (2006) (statement of Robert L. Dietz, General Counsel of the National Security Agency), available at *www.fas.org/irp/congress/2006_hr/fisa4.html*.

The Heritage Foundation LEADERSHIP FOR AMERICA

sion on the privacy interests of Americans who (whether wittingly or unwittingly) communicate with suspected terrorists or other enemy soldiers.

The Protect America Act is not perfect, though. In particular, it fails to grant the President authority to carry out elements of the so-called Terrorist Surveillance Program (TSP), under which the executive purportedly intercepted communications between suspects overseas and individuals in the United States. While the Protect America Act does correct the FISA Court's apparent error of requiring FISA warrants for communications that originate and terminate outside the United States, a more comprehensive bill—one which takes into account legitimate intelligence requirements, the traditional Fourth Amendment status of foreign intelligence searches, and the President's constitutional authority to conduct these searches—would express congressional acquiescence and authorization for programs like the TSP, as well.

The Protect America Act also wisely extended prospective immunity to communications providers that have worked with U.S. intelligence services to facilitate intelligence gathering for national security. With 40 or more civil lawsuits already filed against these providers for their cooperation, Congress should take the logical, fair step and provide retroactive immunity as well.

Congress should make the Protect America Act permanent and enhance its provisions to provide retroactive and permanent liability protection to American businesses that cooperate with reasonable intelligence requests. To do otherwise looks like political gamesmanship—and the stakes are too high to play games with national security.

—Robert Alt is Deputy Director of, Todd Gaziano is the Director of, and Brian W. Walsh is Senior Legal Research Fellow in, the Center for Legal and Judicial Studies at The Heritage Foundation.