WebMemo
Published by The Heritage Foundation
No. 1847
March 12, 2008

# FISA Modernization Is Not About "Warrantless Wiretapping"

*Andrew M. Grossman*

No phrase has done more to confuse the public and distort informed debate over foreign surveillance than "warrantless wiretapping." The accusation that the federal government is listening in on Americans' domestic telephone conversations without any legal authority or any judicial oversight has been an article of faith among those who oppose modernization of the Foreign Intelligence Surveillance Act (FISA).

Though the government's foreign intelligence programs are clouded in secrecy (and rightly so), publicly available information, statutory text, and recent comments by government officials provide strong indications that FISA modernization, by making permanent the authorities of the now-expired Protect America Act (PAA), has nothing at all to do with domestic wiretapping and has only an incidental relation to Americans' communications. Now that Congress is again considering restoring FISA to its originally intended scope of coverage by extending the authorities in the PAA, it is important to understand how the government uses these authorities.

**Electronic Surveillance and Minimization.** As a statutory matter, all domestic wiretapping requires judicial oversight.[1] Under the mandates of FISA, there is no such thing as "warrantless wiretapping" within the United States. A FISA application is more complex, lengthier, and more time-consuming to obtain than an analogous warrant application, which in many cases may run to no more than two or three pages:[2] Each application requires, by one account, "approximately 200 person-hours of government attorneys' and other intelligence officials' time."[3] To equate wiretaps pursuant to FISA orders or surveillance conducted pursuant to the PAA with "warrantless wiretapping" simply misleads the public and misinforms debate.

But it is perhaps because of the complexity of surveillance, both operationally and with respect to legal requirements, that the public debate over FISA and the Protect America Act authorities has been "dumbed down" to the simple but irrelevant phrase "warrantless wiretapping." Due to necessary secrecy and the complexity of the subject matter, it is difficult to explain, however, exactly what kind of surveillance activities is part of the current legislative proposals. Yet public information does allow informed discussion of the issue.

The Protect America Act was intended to correct a controversial FISA Court decision seeking to extend that court's power to control foreign surveillance that was never intended to be covered under FISA and never had been. That decision has not been made public, however, so commentators have been unable to state with great certainty what types of surveillance it concerned. A recent statement by an Administration official provides an answer to this question. Buried in a *Washington Post* report was this important disclosure:

This paper, in its entirety, can be found at:
*www.heritage.org/Research/LegalIssues/wm1847.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

> [I]n response to a question at the meeting by David Kris, a former federal prosecutor and a FISA expert, [Assistant Attorney General for National Security Kenneth] Wainstein said FISA's current strictures did not cover strictly foreign wire and radio communications, even if acquired in the United States. The real concern, he said, is primarily e-mail, because "essentially you don't know where the recipient is going to be" and so you would not know in advance whether the communication is entirely outside the United States.[4]

The FISA process—application to the FISA Court for an order to conduct surveillance and then surveillance pursuant to that order—covers communications that originate or terminate in the United States but not communications that are wholly foreign. Where the present difficulties seem to have arisen is the domain of electronic communications—such as Internet traffic—that might pass through the United States.

For example, an Iraqi national in Iraq may seek to access a Web site that is hosted in Iran. Due to the complexities of modern communications networks, that request may actually pass through United States–based network en route to Iran. The problem is that everything—all traffic, whether domestic or foreign in nature—passes through the same pipe. So if the intelligence services are going to intercept wholly foreign electronic communications of this nature, their only option is to tap into the stream of all traffic.[5]

The intelligence acquisition process, however, does not end there. It is in sorting through that traffic that the crucial and often misunderstood (or simply ignored) process of "minimization"[6] comes into play. Minimization is the process by which an intelligence agency applies a filter to the stream of all traffic to exclude and discard any traffic that is domestic in nature while flagging and keeping for analysis traffic that is foreign and of intelligence value.[7] In this way, the agency can exclude domestic communications that pass through its equipment merely incidentally to its foreign surveillance operations.

Minimization can be incredibly complex, and its details are extremely sensitive. Determining whether a single packet on the Internet (the basic unit of communication) that is in some ways almost indistinguishable from any other packets is foreign in nature (and so not subject to the FISA process) is an extremely difficult problem, requiring sophisticated algorithms and assumptions based on historical network activity. This approach is necessarily imperfect, but it is required by the task: Given the quantity of Internet communications, individual determination is impossible and

1. *See* 50 U.S.C. §§ 1804, 1805.
2. *See, e.g.,* Commonwealth of Virginia, Affidavit for Search Warrant, at www.roanoke.com/clicks/default.aspx?url=/news/0417search_warrant.pdf (a standard Virginia search warrant application form that is one page long), and http://www.heritage.org/Research/HomelandDefense/wm1666.cfm ("Each FISA application requires approximately 200 person-hours of government attorneys' and other intelligence officials' time for each telephone number intercepted.").
3. *See* Robert Alt, Todd F. Gaziano, and Brian Walsh, *The Intelligence Community Needs Clear—and Permanent—FISA Reform*, Jan. 25, 2008, at http://www.heritage.org/Research/HomelandSecurity/wm1782.cfm.
4. Ellen Nakashima and Paul Kane, *Wiretap Compromise in the Works*, WASHINGTON POST, March 4, 2008, at A3.
5. This simple observation, as well as the analysis that follows, is entirely consistent with the report of AT&T "whistleblower" Mark Klein, who alleges that AT&T has built "'secret rooms' hidden deep in the bowels of its central offices in various cities, housing gear for a government spy operation." Also consistent is Klein's claim that "These installations enable the government to look at every individual message on the Internet…." His conclusion, however, that the government is using these facilities to "analyze exactly what people are doing" ("people" presumably meaning average Americans) is not supported by the factual evidence he presents or by any public sources. Mark Klein, AT&T'S IMPLEMENTATION OF NSA SPYING ON AMERICAN CITIZENS 2, Dec. 31, 2005, at http://blog.wired.com/27BStroke6/att_klein_wired.pdf.
6. As used in this paper, "minimization" includes both "targeting" and "minimization" as those terms are used in the statutory text and legislative proposals. Under all proposals, the procedures for both must be submitted to the FISA Court, and both serve to limit raw "surveillance" to permissible "acquisitions," which are then used for intelligence purposes. Functionally, as concerns the programs discussed in this paper, the two are identical.
7. *See* 50 U.S.C. § 1801 (h).



The Heritage Foundation LEADERSHIP FOR AMERICA

would, anyway, be inappropriately intrusive for the bulk of domestic communications.

The Protect America Act restored the government's authority to keep and analyze—that is, not minimize—communications that it reasonably believes are foreign without advance authorization by the FISA Court.[8] It did, however, require the government to regularly submit its minimization procedures to the court and allowed that court to reject them if they are "clearly erroneous."[9] This procedure acts to ensure that the government is not seeking to circumvent FISA requirements for domestic communications.

A reasonableness standard, as implemented through automatic application of minimization algorithms to computer traffic, gives the government the minimum authority it needs to conduct such surveillance effectively without sacrificing the flexibility it needs to improve its algorithms constantly to address new threats. There is some concern, for example, that expiration of the PAA has already caused military intelligence agencies to reject some changes in their electronic surveillance operations, to the possible detriment of battlefield intelligence in Iraq. This is the kind of intelligence gap that could be expected by forcing the government to obtain advance authorization from the FISA Court—an onerous process—for these kinds of operations.

Unfortunately, some privacy extremists and the conspiracy-minded seem to doubt the goodwill of those involved in minimization efforts and military intelligence gathering generally. They boldly assert that the leaders of U.S. intelligence agencies like the National Security Agency (NSA) are intent on listening in on Americans' personal telephone calls and intercepting their e-mails to detect garden-variety crimes and for other purposes. That fear, however, is not supported by any evidence.

Further, this risk would exist under any surveillance regime, including a FISA process that covered all foreign intelligence activities or even standard warrant procedures. Those who are willing to violate surveillance laws would presumably violate any other law that requires FISA Court review or other warrant.

The public record, in fact, indicates that the opposite problem is a greater concern: Intelligence agencies have demonstrated such concern for operating within legal limits that they have limited surveillance when they were not required by law to do so, to the detriment of national security.[10] Intelligence officials confirm privately that this "culture of caution" is pervasive. This does not square with unfounded assertions of widespread abuses or claims that minimization and other privacy-enhancing procedures are deliberately applied in ways that skirt statutory protections.

FISA was never intended to apply to foreign communications, and this fundamental legal principle—reflective of the President's inherent constitutional authority—should not be sacrificed because of changes in the details of the technical implementation of communications networks. The authorities that expired with the PAA simply restored FISA, for a limited time before it expired, to its originally intended scope, giving the government appropriate discretion and flexibility to carry out its responsibility to protect the nation from foreign threats while safeguarding America's freedoms and liberties.

**Why Immunity Matters.** In the context of the kind of surveillance activities described above, immunity for telecom operators and others who have facilitated the surveillance is not a side issue but an essential part of the program. Despite their reputation for high-tech innovation, government entities like the NSA cannot conduct this kind of electronic surveillance on their own. These activities require both the

8. S. 1927, 110th Cong. § 2 (2007).
9. *Id.*
10. Nat'l Comm'n on Terrorist Attacks Upon the United States, FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 79 (July 2004); Dep't of Justice, FINAL REPORT OF THE ATTORNEY GENERAL'S REVIEW TEAM ON THE HANDLING OF THE LOS ALAMOS NATIONAL LABORATORY INVESTIGATION 714 (May 2000); U.S. Senate Select Comm. on Intelligence & U.S. House Permanent Select Comm. on Intelligence, JOINT INQUIRY INTO INTELLIGENCE COMMUNITY ACTIVITIES BEFORE AND AFTER THE TERRORIST ATTACKS OF SEPTEMBER 11, 2001, S. REP. No. 107-351 & H.R. REP. No. 107-792, at 386 (2002).

cooperation and the expertise of network providers—the same telecommunications and other companies that are now facing 38 or more lawsuits in response to just this sort of collaboration with the government. Legal liability will chill future cooperation.

The surveillance activities described above are legal, but proving both the substance of these activities and their legality would require the disclosure of sensitive information relating directly to core mechanisms of surveillance, such as exactly what network traffic is routed through government devices, what minimization procedures are employed, and what cooperative acts the cooperating telecommunications providers performed.

Answering any of these inquiries would likely expose the methods of surveillance, enabling foreign individuals and entities plotting against the United States and its allies to evade detection by altering their patterns of communication. Disclosure of this sort would seriously undermine important surveillance programs to the direct detriment of national security.

It is for this reason that the government has understandably invoked the state secrets privilege to prevent telecommunications providers from disclosing in court the legal documents provided by the government analyzing the legality of their cooperation. Without these documents, however, the providers have no easy means of proving their good-faith compliance with the law. Thus, without immunity, they are subject to massive legal liabilities and litigation expenses for cooperating with surveillance programs that they were assured and reasonably believed to be within the bounds of the law.

This issue extends beyond telecommunications providers to encompass other suppliers of software and equipment that the government needs to conduct surveillance activities. Representatives of these companies privately acknowledge that Congress's actions on retroactive immunity will determine how much they invest in developing surveillance and data-analysis systems for government use.

Without immunity, legal, effective, and privacy-protecting surveillance programs will be stymied by lack of cooperation, lack of expertise, and lack of technological capabilities. Properly understood, these intelligence programs depend on immunity from politically driven civil lawsuits that threaten to undermine their very bases. Immunity is not a handout but a key part of the program and a requirement to incentivize the private sector to engage in necessary research and development to protect the country into the future.

**Conclusion.** The authorities granted by the Protect America Act do not concern "warrantless wiretapping" and do not alter the general requirement that the government go through an intensive authorization process—more demanding than standard criminal warrant procedures—to obtain permission from a judicial body to listen in on domestic communications. Nothing in the law or the public record rebuts this fact.

As can best be ascertained from the public record, these authorities are used not to conduct wiretaps but to sort through and analyze electronic communications that are foreign in nature and flow through U.S. networks. If more individuals on both sides of the FISA debate were to acknowledge this fact, the result would be a better informed public and more productive discussion and debate.

*—Andrew M. Grossman is Senior Legal Policy Analyst in the Center for Legal and Judicial Studies at The Heritage Foundation.*