Hearing Before the United States Senate Committee on the Judiciary

Re: "FISA Amendments: How to Protect Americans' Security and Privacy and Preserve the Rule of Law and Government Accountability."

October 31, 2007

Prepared Statement of Patrick F. Philbin, former Associate Deputy Attorney General, U.S. Department of Justice.

Chairman Leahy, Ranking Member Specter, and Members of the Committee, I appreciate the opportunity to address the matters before the Committee today. I gained experience with issues related to the Foreign Intelligence Surveillance Act and the importance of electronic surveillance as an intelligence tool during my service at the Department of Justice from 2001 to 2005. My duties both as a Deputy Assistant Attorney General in the Office of Legal Counsel and, subsequently, as an Associate Deputy Attorney General involved providing advice on issues related to FISA and the use of electronic surveillance in intelligence and counterterrorism activities. Since my return to the private sector, I have continued to pay close attention to developments in this area, such as recent judicial decisions imposing heightened burdens on the U.S. government with regard to the monitoring of communications from foreign sources, and the filing of multiple lawsuits seeking to hold private telecommunications carriers liable for providing assistance to the government in its surveillance activities.

Electronic surveillance is an important tool both for preventing terrorist attacks and for rooting out espionage. At the same time, it is an intrusive technique that, if not properly constrained and controlled, can threaten the privacy and liberties of American citizens. Ensuring that electronic surveillance remains an agile and adaptable tool for the intelligence community in a world of ever-evolving technology while at the same time protecting American liberties is the challenge that Congress faces in amending FISA.

In my testimony, I wish to make three main points:

First, I want to express support for the provisions in the Bill that will allow the Executive to target the communications of persons reasonably believed to be overseas without first going to the FISA court. These provisions are consistent with FISA's original purpose and are necessary to ensure that FISA does not fall out of step with changing technology. They provide a medium-term solution to the problems that motivated Congress's enactment of a short-term fix in the Protect America Act earlier this year.

Second, I want to express my support for the provisions in Senate Bill 2248 that would grant immunity to telecommunications carriers against lawsuits based on the carriers' alleged participation in the "Terrorist Surveillance Program" authorized by the President. In essence, those lawsuits seek to hold carriers liable to the tune of billions of dollars for their patriotic decision to cooperate with U.S. government operations that Executive Branch officials had determined to be lawful and necessary. Whether or not those determinations by Executive Branch officials were correct in every instance is not a matter that should be addressed through private lawsuits against the carriers. To the contrary, allowing such lawsuits to proceed would be fundamentally unfair to carriers who are alleged to have cooperated in reliance on representations from the Executive Branch that their activities were lawful. Worse, it would provide a perverse incentive that would threaten to deter future cooperation with the government in times of emergency.

Third, however, I also want to note one provision of the bill that I consider unwise -- the provision that would create a wholly new requirement for the government to obtain an order from the FISA court before monitoring communications of U.S. citizens who are overseas. When government officials have sufficient basis to believe that U.S. citizens overseas are

engaging in espionage or terrorist activities, they should be able to act expeditiously in conducting necessary surveillance, and should not be required to go before the FISA court. Historically, such surveillance powers have been exercised for limited purposes and, as far as I am aware, there has been no suggestion of any abuse warranting this change in the law. Accordingly, I believe there is no need to expand the FISA Court's jurisdiction and to constrain the capabilities of the Executive in this way.

I. S. 2248 Appropriately Provides That No Individualized Order Need Be Sought for Surveillance of Foreign Targets Reasonably Believed To Be Outside the United States

One of the central features in the pending legislation lies in provisions that allow the Attorney General and the Director of National Intelligence to authorize the targeting for surveillance purposes of foreign terrorists and other foreign intelligence targets reasonably believed to be located outside the United States, without obtaining individualized court orders from the Foreign Intelligence Surveillance Court. The Protect America Act was a short-term fix to address this same issue. In my view, given changes in technology, a longer-term solution to make the application of FISA less dependent on the medium used to carry a communication (such as wire vs. radio waves), and more directly tied to the location of the target, is definitely warranted, and this provision is a good start.

The pending legislation provides a medium-term solution to this problem. Among other relevant provisions, Section 701 generally removes from the definition of "electronic surveillance," to which FISA's procedures would otherwise apply, surveillance activities targeted at a person "reasonably believed to be located outside the United States." Accordingly, for the majority of surveillance activities targeted at persons outside the United States, there would be no requirement to obtain an individualized court order.

This is consistent with the original intent of FISA that warrants not be required for interception of foreign communications. In 1978, when Congress enacted FISA, foreign communications and even international communications were usually collected and monitored through interception of radio and microwave transmissions, for which no warrant was necessary. Now, those same communications are often routed through fiber-optic cables that regularly pass through the United States. This technological change should not make a difference to the legal constraints our laws place on collection. Just as it was in 1978, the underlying principle now should be that where the government is targeting foreign terrorists and foreign intelligence targets, it should be able to proceed more expeditiously than when it targets persons within our country's borders. The Bill as drafted is generally consistent with this principle and makes a needed change for the efficient use of electronic surveillance as an intelligence tool.

II. S. 2248's Provision of Immunity for Telecommunications Carriers Is Fair and Critically Promotes the National Security Interests of the United States

I also support the provisions in S. 2248 providing immunity for telecommunications carriers who allegedly participated in what has become known publicly as the "Terrorist Surveillance Program" and for other alleged intelligence activities involving electronic surveillance. These carriers have been sued in over forty lawsuits seeking hundreds of billions of dollars in damages. The pending actions are currently consolidated in the Northern District of California in *In re National Security Agency Telecommunications Records Litigation*, MDL No. 06-1791. Of course, the extent to which carriers actually did or did not participate in such a "Terrorist Surveillance Program" remains classified. The fact remains, however, that the carriers are facing years of expensive litigation and claims for potentially ruinous damages based upon allegations that they did nothing more than furnish assistance requested by the government,

authorized by the President, reviewed for legality at the highest levels of the Executive Branch, and represented to the carriers to be lawful.

Title II of the pending legislation would address this problem by allowing the Attorney General to step in and obtain the dismissal of these lawsuits. Under Section 202, a civil action challenging a telecommunication carrier's assistance in a government intelligence activity must be dismissed if the Attorney General certifies to the pertinent court either that the carrier did not provide the alleged assistance, or that the allegations of the lawsuit concern an intelligence activity (i) authorized by the President between September 11, 2001 and January 17, 2007, (ii) designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, against the United States, and (iii) described in a written request to the carrier from the Attorney General or a high-ranking intelligence official indicating that the intelligence activity was authorized by the President and had been determined to be lawful. There are several reasons why it is sound policy to retain this provision in the pending legislation.

First, protecting carriers who allegedly responded to the government's call for assistance in the wake of the devastating attacks of September 11, 2001 and during the continuing threat of further attacks is simply the right thing to do. Determining the single right thing to do has always been my touchstone for decision making, and I believe it provides the correct answer here. The allegations here are that, in the wake of the devastating attacks of 9/11, corporations were asked to assist the intelligence community based on a program authorized by the President himself and based on assurances that the program had been determined to be lawful at the highest levels of the Executive Branch. Under those circumstances, the corporations should be entitled to rely on those representations and accept the determinations of the Government as to the legality of their actions. They should not be penalized for responding patriotically in a time

of crisis and relying on the Government's own assessment of the legality of their actions. Having obtained assurance from the Government that their conduct is lawful, they should not be forced to defend themselves against protracted litigation by persons whose primary grievance lies with the Government.

Granting immunity to the telecommunications carriers here is consistent with the immunity that the common law has long recognized for private citizens who respond to a call for assistance from a public officer in the course of his duty. The salutary purpose of such a rule is to recognize that private persons should be encouraged to offer assistance to a public officer in a crisis and should not be held accountable if it later turns out that the public officer made a mistake. The rule ensures, in the words of Justice Cardozo, that "the citizenry may be called upon to enforce the justice of the State, not faintly and with lagging steps, but honestly and bravely and with whatever implements and facilities are convenient and at hand." *Babbington v. Yellow Taxi Corp.*, 250 N.Y. 14, 17 (1928).

Smith v. Nixon, 606 F.2d 1183 (D.C. Cir. 1979), is illustrative of the way courts have dealt with such matters. In that case the United States Court of Appeals for the District of Columbia Circuit upheld the dismissal of a telephone company from a case that challenged the wiretapping of a home telephone. While suggesting that the wiretap itself might have been illegal, the Court of Appeals held that the company still could not be held liable because it "did not initiate the surveillance, and it was assured by the highest Executive officials in this nation that the action was legal." *Id.* at 1191. Similar principles surely apply here, especially given the limited nature of the immunity contemplated in the bill, which would apply only where carriers were told that a program was authorized by the President and determined to be lawful.

In light of existing precedent regarding qualified immunity, some might argue that there is no need for Congress to enact a specific provision providing immunity to telecommunications carriers here. But this argument overlooks the point that even litigating questions of qualified immunity can prove burdensome; and there is also a real possibility that courts would misapply qualified immunity doctrines and rule against the carriers. Even if the telecommunications carriers ultimately prevail, moreover, the specter of protracted litigation over such questions could serve to deter future cooperation with government officials in times of emergency. The pending legislation thus wisely provides for dismissal after the filing of a duly executed government certification.

Second, immunity is appropriate because allowing the suits to proceed would risk leaking sensitive national security information. As the suits progress, they will inevitably risk disclosure of intelligence sources and methods that will damage the national security of the United States in the midst of its ongoing struggle with al Qaeda. The assertion of state secrets privilege is not a cure-all for protecting national security information, as some decisions in the suits have already shown. The longer the suits proceed, the more details concerning the ways the intelligence community may seek information from the Nation's telecommunications infrastructure will leak. Our enemies are far from stupid; as such information trickles out, they will adapt their communications security to thwart our surveillance measures, and valuable intelligence will be lost.

Third, failing to provide immunity to the carriers here would also discourage both communications companies and other private sector corporations from providing assistance in the context of future emergencies, thus damaging the national security of the United States and potentially putting American lives at risk. In the continuing struggle with Al Qaeda, one of our

Nation's greatest strategic assets is its private sector and the information that sector has available to it. Particularly in this war with a shadowy enemy, intelligence is vital for success. If immunity is not provided, however, it is likely that, in the future, private sector corporations will prove much more reluctant to provide assistance swiftly and willingly, and critical time in obtaining information will be lost. I agree fully with the conclusion in the report accompanying the bill from the Select Committee on Intelligence: "The possible reduction in intelligence that might result from this delay is simply unacceptable for the safety of our Nation." S. Rep. 110-209, at 11.

Finally, I disagree with the suggestions made by some that the private lawsuits against carriers can force the carriers to serve a gatekeeper role to second-guess and provide, in essence, oversight on the intelligence-gathering decisions of the Executive. I believe that approach is misguided. As a general matter, telecommunications carriers are simply not well-positioned to second-guess government decisions regarding the propriety or legality of intelligence activities. I know from experience that the legal questions involved in such matters are highly specialized, extremely difficult, often involve difficult constitutional questions of separation of powers and are not readily susceptible for analysis by lawyers at a company whose primary concern is providing communications service to the public. We should not adopt policies that give private corporations incentives to demand detailed information from the Executive and in essence to conduct their own mini-investigations into the propriety of intelligence operations the government wishes to conduct. As explained above, such incentives would be at cross-purposes with the government's need for expedition.

At the same time, there must be some mechanism for addressing concerns raised about the program at issue. Some have raised questions about the underlying legitimacy of the

surveillance program in which various telecommunications carriers allegedly participated, and about the legal reasoning of the government officials involved in establishing and overseeing that program. As the Committee is likely aware, I am intimately familiar with the legal analysis conducted within the Executive Branch of the intelligence program in question and with debates about that analysis, both within the Executive Branch and in Congress. I can understand that what has leaked about the program might lead reasonable people to want further probing into the legal bases for the program. And ensuring that all intelligence activities do strictly adhere to the law is an imperative. But the question of liability for telecommunications carriers is logically and legally entirely distinct from that debate and should be decided wholly apart from it. The mechanism for addressing legal concerns about the intelligence programs is through rigorous oversight within the Executive Branch -- which, I might add, does actually work -- and through a joint effort between the Executive and Congress to ensure appropriate oversight. The Executive and Congress are the branches constitutionally charged with responsibility in these fields, and they should appropriately address questions about intelligence activities, not leave those matters vital for national security to be sorted out in private lawsuits.

The mechanism that is least suited for addressing concerns about the Executive Branch's legal decisions, and least likely to produce outcomes that rationally address the national security imperatives of the Nation, is private lawsuits conducted in public forums seeking to obtain money damages from private entities who were not responsible for the intelligence-gathering decisions made by the Executive Branch.

III. S. Bill 2248 Should Be Amended To Remove the Requirement That a Warrant Be Obtained To Conduct Surveillance of U.S. Citizens Overseas

There is one respect, however, in which S. Bill 2248 departs from historical practice and from the underlying principles motivating the passage of FISA in 1978. Significantly,

subsection 703(c)(2) of the bill requires the government to obtain a warrant from the FISA Court in order to conduct surveillance of a U.S. citizen who is reasonably believed to be *outside the United States*. To obtain such a warrant the Attorney General must submit to the FISA Court an application setting forth facts demonstrating that there is probable cause that the target of the surveillance is an agent of a foreign power or terrorist organization. This is a new requirement, introduced in the Select Committee on Intelligence by way of an amendment to the original bill, and it would expand the FISA Court's jurisdiction in ways that have not before been tested.

In my view this requirement is inconsistent with our historical practice and unwarranted. As for history, under Executive Order 12333, which President Reagan signed in 1981, the Attorney General was permitted to authorize surveillance of U.S. citizens both within the United States and overseas upon a finding of probable cause to believe that the person in question is an agent of a foreign power. Such determinations have been handled outside of the FISA framework and without resort to the FISA Court. This system has worked well in allowing us to move flexibly and expeditiously to collect valuable intelligence on U.S. citizens who unfortunately choose to align themselves with foreign powers or terrorists. This system is consistent with the President's independent authority to conduct intelligence activities in the course of conducting United States foreign policy and acting to counter foreign threats. *See, e.g., In re Sealed Case*, 310 F.3d 717, 742 (Foreign Intel. Surveillance Ct. of Review 2002) (describing the inherent authority of the President of the United States to gather foreign intelligence information).

At the same time, there has been no demonstration that the power to conduct limited surveillance of U.S. citizens overseas without resort to the FISA Court has led to abuse. Attorneys General have exercised their powers under Executive Order 12333 with judgment and

discretion. They have not targeted ordinary tourists or businesspeople engaged in routine overseas travel; instead, this authority has been used sparingly and appropriately. In light of the limited purposes for which surveillance of U.S. citizens overseas is conducted, coupled with the lack of evidence of abuse, there is no reason to impair the flexibility of highly sensitive intelligence and counterterrorism investigations by adopting a warrant requirement in this context. Nor is a warrant required by the Fourth Amendment. The touchstone of the Fourth Amendment is reasonableness. And it has long been held that in foreign intelligence investigations, the President may order warrantless searches consistent with the Fourth Amendment. That result can only apply more strongly to searches overseas. Accordingly, I recommend that the Senate amend the bill to remove this provision.

* * *

Thank you, Mr. Chairman, for the opportunity to address the Committee. I would be happy to address any questions the Committee may have.