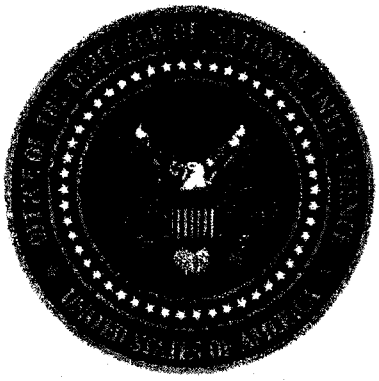
Modernizing the Foreign Intelligence Surveillance Act

Statement for the Record

Senate Select Committee on Intelligence

May 1, 2007



J. Michael McConnell
Director of National Intelligence

Information as of
May 1, 2007

SENATE SELECT COMMITTEE ON INTELLIGENCE
FISA MODERNIZATION

UNCLASSIFIED
STATEMENT FOR THE RECORD

INTRODUCTION

Good morning Chairman Rockefeller, Vice Chairman Bond, and Members of the Committee.

I am pleased to be here today in my role as the head of the Intelligence Community (IC) to express my strong support for the legislation that will modernize the Foreign Intelligence Surveillance Act of 1978 (FISA).

Since 1978, FISA has served as the foundation to conduct electronic surveillance of foreign powers and agents of foreign powers in the United States. My goal in appearing today is to share with you the critically important role that FISA plays in protecting the nation's security, and how I believe the proposed legislation will improve that role, while continuing to protect the privacy rights of Americans.

The proposed legislation to amend FISA has several key characteristics:

- It makes the statute technology-neutral. It seeks to bring FISA up to date with the changes in communications technology that have taken place since 1978;
- It seeks to restore FISA to its original focus on protecting the privacy interests of persons in the United States;
- It enhances the Government's authority to secure assistance by private entities, which is vital to the IC's intelligence efforts;

- And, it makes changes that will streamline the FISA process so that the IC can use FISA as a tool to gather foreign intelligence information more quickly and efficiently.

As the Committee is aware, I have spent the majority of my professional life in the IC. In that capacity, I have been both a collector and a consumer, of intelligence information. I had the honor of serving as Director of the National Security Agency (NSA) from 1992 to 1996. In that position, I was fully aware of how FISA serves a critical function in enabling the collection of foreign intelligence information.

In my first eight weeks on the job as the new Director of National Intelligence, I immediately can see the results of FISA-authorized collection activity. I cannot overstate how instrumental FISA has been in helping the IC protect the nation from terrorist attacks since September 11, 2001.

Some of the specifics that support my testimony cannot be discussed in open session. This is because certain information about our capabilities could cause us to lose capability. I look forward to elaborating further on all aspects of the issues in a closed, classified setting.

I can, however, make a summary level comment about the current FISA legislation. Since the law was drafted in a period preceding today's global information technology transformation and does not address today's global systems in today's terms, the community is significantly burdened in capturing overseas communications of foreign terrorists planning to conduct attacks inside the United States. We must make the requested changes to protect our citizens and the nation.

TODAY'S NATIONAL SECURITY THREATS

Because I believe that the proposed legislation will advance our ability to protect the national security, I would like to take a few minutes to discuss some of the current threats. The most obvious is the continued threat from international terrorists. Despite the fact that we are in the sixth year following the attacks of September 11, 2001, and despite the steady progress we have made in dismantling the al Qaeda organization, significant threats from al Qaeda, other terrorist organizations aligned with it, and its sympathizers remain.

Today, America confronts a greater diversity of threats and challenges to attack inside our borders than ever before. As a result, the nation requires more from our IC than ever before.

I served as the Director of NSA at a time when the IC was first adapting to the new threats brought about by the end of the Cold War. Moreover, these new threats are enhanced by dramatic, global advances in telecommunications, transportation, technology, and new

centers of economic growth.

Although the aspects of Globalization are not themselves a threat, they facilitate terrorism, heighten the danger and spread of the proliferation of Weapons of Mass Destruction (WMD), and contribute to regional instability and reconfigurations of power and influence — especially through increasing competition for energy.

Globalization also exposes the United States to complex counterintelligence challenges. Our comparative advantage in some areas of technical intelligence, where we have been dominant in the past, is being eroded. Several non-state actors, including international terrorist groups, conduct intelligence activities as effectively as capable state intelligence services. Al Qaeda, and those aligned with and inspired by al Qaeda, continue to actively plot terrorist attacks against the United States, our interests and allies.

A significant number of states also conduct economic espionage. China and Russia's foreign intelligence services are among the most aggressive in collecting against sensitive and protected U.S. systems, facilities, and development projects approaching Cold War levels.

FISA NEEDS TO BE TECHNOLOGY-NEUTRAL

In today's threat environment, the FISA legislation is not agile enough to handle the country's intelligence needs. Enacted nearly thirty years ago, it has not kept pace with 21st Century developments in communications technology. As a result, FISA frequently requires judicial authorization to collect the communications of non-U.S., i.e., foreign persons, located outside the United States. Currently, FISA forces a detailed examination of four questions:

Who is the target of the communications?
Where is the target located?
How do we intercept the communications?
Where do we intercept the communications?

This analysis clogs the FISA process with matters that have little to do with protecting privacy rights of persons inside the United States. Modernizing the FISA would greatly improve the FISA process and relieve the massive amounts of analytic resources currently being used to craft FISA applications.

FISA was enacted before cell phones, before e-mail, and before the Internet was a tool used by hundreds of millions of people worldwide every day. When the law was passed in 1978, almost all local calls were on a wire and almost all long-haul communications were in the air, known as "wireless" communications. Therefore, FISA was written to distinguish between collection on a wire and collection out of the air.

Now, in an age of modern telecommunications, the situation is completely reversed; most long-haul communications are on a wire and local calls are in the air. Think of using your cell phone for mobile communications.

Communications technology has evolved in ways that have had unforeseen consequences under FISA. Technological changes have brought within FISA's scope communications that the IC believes the 1978 Congress did not intend to be covered. In short, communications currently fall under FISA that were originally excluded from the Act.

The solution is to make the FISA technology-neutral. Just as the Congress in 1978 could not anticipate today's technology, we cannot know what changes technology may bring in the next thirty years. Our job is to make the country as safe as possible by providing the highest quality intelligence available. There is no reason to tie the nation's security to a snapshot of outdated technology.

Communications that, in 1978, would have been transmitted via radio or satellite, are transmitted principally via fiber optic cables. While Congress in 1978 specifically excluded from FISA's scope radio and satellite communications, certain fiber optic cable transmissions currently fall under FISA's definition of electronic surveillance. Congress' intent on this issue is clearly stated in the legislative history:

"the legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States."

Similarly, FISA places a premium on the location of the collection. Legislators in 1978 could not have been expected to predict an integrated global communications grid that makes geography an increasingly irrelevant factor. Today a single communication can transit the world even if the two people communicating are only a few miles apart.

And yet, simply because our law has not kept pace with our technology, communications intended to be excluded from FISA, are included. This has real consequences to our men and women in the IC working to protect the nation from foreign threats.

FOREIGN INTELLIGENCE COLLECTION UNDER FISA

Today, IC agencies may apply, with the approval of the Attorney General and the certification of other high level officials, for court orders to collect foreign intelligence information under FISA. Under the existing FISA statute, the IC is often required to make a showing of probable cause, a notion derived from the Fourth Amendment, in order to target for surveillance the communications of

a foreign person overseas.

Frequently, although not always, that person's communications are with another foreign person overseas. In such cases, the current statutory requirement to obtain a court order, based on a showing of probable cause, slows, and in some cases prevents altogether, the Government's efforts to conduct surveillance of communications it believes are significant to the national security.

This is a point worth emphasizing, because I think many Americans would be surprised at what the current law requires. To state the case plainly: there are circumstances under which when the Government seeks to monitor, for purposes of protecting the nation from terrorist attack, the communications of **foreign** persons, who are physically located in **foreign** countries, the Government is required under FISA to obtain a court order to authorize this collection. We find ourselves in this position because the language in the FISA statute, crafted in 1978, simply has not kept pace with the revolution in communications technology.

Moreover, this Committee and the American people should be confident that the information the IC is seeking is **foreign intelligence** information. Writ large, this includes information relating to the capabilities, intentions and activities of foreign powers, organizations or person, including information on international terrorist activities. FISA was intended to permit the surveillance of foreign intelligence targets, while providing appropriate protection through court supervision to U.S. citizens and to other persons in the United States.

While debates concerning the extent of the President's constitutional powers were heated in the mid-1970s, as indeed they are today, we believe that the judgment of Congress at that time was that FISA's regime of court supervision was focused on situations where Fourth Amendment interests of persons in the United States were implicated. It is important to note that nothing in the proposed legislation changes this basic premise in the law.

Another thing that this proposed legislation does **not** do is change the law or procedures governing how NSA, or any other government agency, treats information concerning United States persons. For example, during the course of its normal business under current law, NSA will sometimes encounter information to, from or about U.S. persons. Yet this fact does not, in itself, cause the FISA to apply to NSA's overseas surveillance activities.

Instead, at all times, NSA applies procedures approved by the U.S. Attorney General to all aspects of its activities that minimize the acquisition, retention and dissemination of information concerning U.S. persons. These procedures have worked well for decades to ensure the constitutional reasonableness of NSA's surveillance

activities, and eliminate from intelligence reports incidentally acquired information concerning U.S. persons that does not constitute foreign intelligence.

Some observers may be concerned about "reverse targeting" in which the target of the electronic surveillance is really a person in the United States who is in communication with the nominal foreign intelligence target overseas. In such cases, if the real target is in the United States, FISA would require the IC —to seek approval from the FISA Court in order to undertake such electronic surveillance.

In short, the FISA's definitions of "electronic surveillance" should be amended so that it no longer matters how collection occurs (whether off a wire or from the air). If the subject of foreign intelligence surveillance is a person reasonably believed to be in the United States or if all parties to a communication are reasonably believed to be in the United States, the Government should have to go to court to obtain an order authorizing such collection. If the government seeks to acquire communications of persons outside the United States, it will continue to be conducted under the lawful authority of Executive Order 12333, as they have been for decades.

SECURING ASSISTANCE UNDER FISA

The proposed legislation reflects that it is vitally important that the Government retain a means to secure the assistance of communications providers. As Director of NSA, a private sector consultant to the IC, and now Director of National Intelligence, I understand that in order to do our job, we frequently need the sustained assistance of those outside of government to accomplish our mission.

Presently, FISA establishes a mechanism for obtaining a court order directing a communications carrier to assist the Government with the exercise of **electronic surveillance** that is subject to Court approval under FISA. However, as a result of the proposed changes to the definition of electronic surveillance, FISA does not provide a comparable mechanism with respect to authorized **communications intelligence** activities. The proposal would fill this gap by providing the Government with means to obtain the aid of a court to ensure private sector cooperation with lawful intelligence activities.

This is a critical provision that works in concert with the proposed change to the definition of "electronic surveillance." It is crucial that the government retain the ability to ensure private sector cooperation with activities that are "electronic surveillance" under current FISA, but that would no longer be if the definition were changed. It is equally critical that private entities that are alleged to have assisted the IC in preventing future attacks on the United States be insulated from liability for doing so. The draft FISA

Modernization proposal contains a provision that would accomplish this objective.

THE FISA PROCESS SHOULD BE STREAMLINED

In addition to updating the statute to accommodate new technologies, protecting the rights of people in the United States, and securing the assistance of private parties, the proposed legislation also makes needed administrative changes. These changes include:

(1) streamlining applications made to the FISA Court, and (2) extending the time period the Department of Justice has to prepare applications following Attorney General authorized emergency collection of foreign intelligence information.

The Department of Justice estimates that these process-oriented changes potentially could save thousands of attorney work hours, freeing up the Justice Department's National Security lawyers and the FISA Court to spend more of their time and energy on cases involving United States persons - - precisely the cases we want them to be spending their efforts on. And, if we combine the streamlining provisions of this bill with the technology-oriented changes proposed, the Intelligence Community will be able to focus its operational personnel where they are needed most.

FISA WILL CONTINUE TO PROTECT CIVIL LIBERTIES

When discussing whether significant changes to FISA are appropriate, it is always appropriate to thoughtfully consider FISA's history. Indeed, the catalysts for FISA's enactment were abuses of electronic surveillance that were brought to light. The revelations of the Church and Pike committees resulted in new rules for U.S. intelligence agencies, rules meant to inhibit abuses while preserving our intelligence capabilities. I want to emphasize to this Committee, and to the American people, that none of the changes being proposed are intended to, nor will have the effect of, disrupting the foundation of credibility and legitimacy that FISA established.

Instead, we will continue to conduct our foreign intelligence collection activities under robust oversight that arose out of the Church and Pike investigations and the enactment of FISA. Following the adoption of FISA, a wide-ranging, new intelligence oversight structure was built into U.S. law. A series of laws and Executive Orders established oversight procedures and substantive limitations on intelligence activities. After FISA, the House and Senate each established intelligence oversight committees. Oversight mechanisms were established within the Department of Justice and within each intelligence agency – including a system of inspectors general.

More recently, additional protections have been implemented community-wide. The Privacy and Civil Liberties Oversight Board

was established by the Intelligence Reform and Terrorism Prevention Act of 2004. The Board advises the President and other senior executive branch officials to ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of all laws, regulations, and executive branch policies related to efforts to protect the Nation against terrorism. Unlike in the 1970s, the IC today operates within detailed, constitutionally-based, substantive, and procedural limits under the watchful eyes of Congress, numerous institutions within the Executive Branch, and, through FISA, the judiciary.

With this robust oversight structure in place, it also is important to ensure that the IC is more effective in collecting and processing information to protect Americans from terrorism are other threats to the security of the United States. FISA must be updated to meet the new challenges faced by the IC.

The Congressional Joint Inquiry Commission into IC Activities Before and After the Terrorist Attacks of September 11, 2001, recognized that there were systemic problems with FISA implementation. For example, the Commission noted that "there were gaps in NSA's coverage of foreign communications and FBI's coverage of domestic communications." As a result of these and other reviews of the FISA process, the Department of Justice and IC have continually sought ways to improve.

The proposed changes to FISA address the problems noted by the Commission. At the same time, a concerted effort was made in our proposal to balance the country's need for foreign intelligence information with the need to protect core individual civil rights.

CONCLUSION

This proposed legislation seeks to accomplish several goals:

- First, the changes proposed are intended to make FISA technology-neutral, so that as communications technology develops - - which it absolutely will - - the language of the statute does not become obsolete.

- Second, this proposal is not intended to change privacy protections for Americans. In particular, this proposal makes no changes to the findings required to determine that a U.S. person is acting as an agent of a foreign power. The proposal returns the FISA to its original intent of protecting the privacy of persons in the United States.

- Third, the proposed legislation enhances the Government's ability to obtain vital assistance of private entities.

- And fourth, the proposed legislation allows the Government to make some administrative changes to the way FISA

applications are processed. As Congress has noted in its reviews of FISA process, streamlining the FISA process makes for better government.

This Committee should have confidence that we understand that amending FISA is a major proposal. We must get it right. This proposal is being made thoughtfully, and after extensive coordination for over a year.

Finally, I would like to state clearly my belief that bipartisan support for bringing FISA into the 21st Century is essential. Over the course of the last year, those working on this proposal have appeared at hearings before Congress, and have consulted with Congressional staff regarding provisions of this bill. This consultation will continue. We look to the Congress to partner in protecting the nation. I ask for your support in modernizing FISA so that it will continue to serve the nation for years to come.

As I stated before this Committee in my confirmation hearing earlier this year, the first responsibility of intelligence is to achieve understanding and to provide warning. As the new head of the nation's IC, it is not only my desire, but my duty, to encourage changes to policies and procedures, and where needed, legislation, to improve our ability to provide warning of terrorist activity and other threats to our security.

I look forward to answering the Committee's questions regarding this important proposal to bring FISA into the 21st Century.