Testimony of Morton H. Halperin

Before

The Senate Committee on the Judiciary

October 31, 2007

Mr. Chairman,

It is a great pleasure for me to appear once again before this distinguished committee to discuss the latest effort to modify FISA so that it continues to protect both our security and our liberty. This committee has found a way to protect both in the past and I am confident that it can do so again with the cooperation of those concerned about civil liberties and those charged with defending our security.

To assist in that effort, I want to propose a way of thinking about the structure of FISA and review the history of how the two major sets of issues raised by FISA have been treated.

The two major questions are: (1) What electronic communications should the government be able to acquire using procedures different from those mandated for criminal investigations; and (2) what procedures should be put in place so that all concerned groups can know clearly what the rules are and have confidence that the rules are being followed? In making some suggestions for what should be in the legislation I will focus on the second set of questions.

Pre-FISA Procedures

It is important to begin by recalling the pre-FISA world and to understand the pressures which led two administrations, large bi-partisan groups in both Houses of the Congress, and many civil libertarians to support the enactment of FISA.

In the period before FISA was enacted in 1978 there were essentially no legislated rules and only the most rudimentary procedures in the Executive branch establishing standards for when communications could be acquired. We now know that the FBI conducted surveillance of targets such as the Soviet Ambassador, Martin Luther King, Jr., steel company executives, journalists and government officials, including, I should add in the spirit of full disclosure, me when I worked in the Nixon Administration and then as a private citizen. The National Security Agency also acquired copies of telegrams entering and leaving the United States relating to anti-war activists.

The Justice Department did have formal procedures for the Attorney General to approve a warrantless surveillance, but often more informal procedures would be used—perhaps a decision by the Director of the FBI on his own or a request from a White House official to the Director.

Government communication with the telephone company – at the time, AT&T was the only one -- could not have been more casual. A designated official of the FBI called a designated official of AT&T and passed on a phone number. Within minutes all of the calls from that number were being routed to the local FBI field office and monitored. The fruits of the surveillance were routed to the officials who requested the surveillance.

The viability of this system came to an end with the Watergate scandals and the resulting revelations of the improper actions of the intelligence community. At the time, there were many leaks or reports of improper surveillance. Government officials were not certain about which surveillance activities were legal and what behavior might subject them to civil or criminal penalties. Many lawsuits were being filed and the legality of the surveillances were being challenged in criminal cases. The phone company was being sued and was beginning to demand clarity as to what its obligations were.

(All this should sound very familiar)

Enactment of FISA

The Ford Administration came to the conclusion that it was time to subject this set of activities to the rule of law. Intelligence professionals objected: they were reluctant to submit to formal rules and especially to the requirement that they get prior judicial approval before they could act, unless there was an emergency. They feared that the resulting rules might prevent them from acting as necessary. Civil libertarians were concerned that the rules might authorize surveillance that went beyond the Fourth Amendment or was open to abuse. They feared the court would be a rubber stamp and that the oversight would not be sufficient.

In the end, after multi-hearings in this and other committees, Congress was able to craft a bill that has stood the test of time. The legislation answered both questions – who could be surveilled and with what safeguards – with great clarity and in a way that struck, in my view, the right balance.

It provided that communications of foreign powers or agents of a foreign power could be acquired in the United States for the purpose of collecting foreign intelligence information. No surveillance was permitted of those without connections to foreign powers, including people suspected of leaking information. The basic procedure required approval by the Attorney General

and then approval of the FISA court, with periodic re-approvals and supervision by the Court to determine that the rules were being followed. There were also standards for a few limited situations when a surveillance could be started or conducted without a court order. These were carefully delimitated and involved emergencies, leased lines, and the Congress declaring war.

AT&T received the clarity that it sought and deserved. The rule, spelled out clearly in several places in the legislation and well understood by all, was this: If AT&T received a copy of a warrant or a certification under the statute, it was required to cooperate. If it did not receive authorization by means outlined in the statute, it was to refuse to cooperate and was to be subjected to state and federal civil and criminal penalties for unlawful acquisition of electronic communications.

Let me say a further word about the certification option since it seems to be a source of some misunderstanding and therefore needs, I will suggest, to be clarified in the current legislation.

Everyone involved in the drafting understood that there was a need to provide great clarity and simplicity to the phone company. The simplest rule would have mandated that the phone company act only with a warrant. However, there clearly were situations where speed or exigency did not permit time for a warrant and a few cases where it was agreed that a warrant should not be necessary. For those cases, the statute provided that the telephone company should cooperate if it received a certification from the Attorney General. However, it was clear from the legislation (or should have been) that the Attorney General could provide a certification only if the specific requirements of FISA had been met and he needed to assure the company that those statutory requirements had been met.

Experience under FISA

From the time that FISA went into effect until President Bush authorized a warrantless surveillance program which violated its rules, FISA was extraordinarily successful. There was not a single leak of a FISA program or surveillance. According to the testimony of successive government officials, many more communications were intercepted and used by the intelligence community under FISA than had been the case before its enactment. There were no suggestions of abuse and government officials and private companies participated in the program with no doubts and no fear of incurring penalties. There were few, if any, civil suits, and in criminal cases the courts almost uniformly upheld the statute.

Operating Outside of FISA

All that changed to the detriment of both our liberty and our security when the Administration decided to act outside of FISA rather than seeking amendments to the statute. Since the authorization of the warrantless surveillance program, there have been leaks to the press and lawsuits filed. Government officials have doubted whether the programs they have been asked to implement were legal. Private companies are under siege and in doubt about their legal obligations. Programs have been terminated or altered because they were viewed as illegal by government officials or the FISA court. Senior White House officials even visited an ailing Attorney General in his hospital room to ask him in vain to authorize a warrantless surveillance program.

Restoring FISA

To protect our security and our liberty we must restore the FISA process. It is a welcome sign of progress that the Administration asked for new legislation and seems to be ready to conduct all of its surveillance pursuant to the new law enacted by the Congress. However, the administration continues to attack those with a different view as unpatriotic or political and fails to explain why the language it proposes is necessary or even what it means. This is true of the Act passed in haste in August and, I regret to say, it is true of some of the language of the bill reported by the Senate Special Committee on Intelligence (SSCI).

This committee has the opportunity, which I urge you to seize, to return to the traditions of FISA and to report out a bill that restores the trust of the American people and protects both our security and our liberty by providing clear rules.

As I said at the outset, FISA legislation involves two major questions. First, under what circumstances may the government acquire electronic surveillance and second, what are the rules for how it can acquire those communications.

On the first question, the major change proposed by the administration and reflected in both the SSCI and House bills is to permit the acquisition from a wire in the United States of communications by targeting a person overseas without a particularized court order based on probable cause even if this involves intercepting conversations and communications of persons in the United States. There is an on-going debate about whether this change is necessary and constitutional. I propose to leave that discussion to others and to focus my remaining remarks on the procedures and rules for monitoring compliance, assuming that the committee will authorize the new surveillance program.

The SSCI bill, in my view, falls short of providing the clarity and the effective oversight that is necessary to protect our security and our liberty and to secure the trust of the American people. Let me focus on four major concerns:

1. The statement in Section 701 that "Nothing in the definition of electronic surveillance under section 101 (f) shall be construed to encompass surveillance that is targeted in accordance with this title at a person reasonably believed to be located outside the United States."

2. The failure to require that a court order must be obtained in advance of any surveillance under this new authority (except in emergencies), to provide that service providers must receive the court order before they can cooperate, and to permit effective court oversight of the surveillance process.

3. The failure to provide for effective procedures and oversight to insure that the government may not use this procedure when it is in fact seeking to acquire the communications of a U.S. person or a person in the United States.

4. The failure to eliminate the ambiguity in the statute so as to make it clear that the procedures in FISA are the sole means to conduct electronic surveillance for intelligence purposes and that private companies must cooperate if they receive a court order or a certification specifically authorized by this statute and must not cooperate in any other circumstance.

Section 701

With all due respect to the drafters of Section 701 of the proposed legislation (who continue to be anonymous), it can only be described as Alice in Wonderland. It says that the language in FISA, which defines "electronic surveillance," means not what it clearly says, but what the current bill says that it says. Later, in two places the reported bill says that electronic surveillance has the meaning from FISA and that the change in the definition should be ignored Moreover, no reason to write the bill this way is presented in the Committee Report or elsewhere that I am aware of, or by the administration. The intended purpose can be accomplished by much more explicit language as I will discuss.

The FISA definition of electronic surveillance includes the following:

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States.

Section 701 of the bill reported by SSCI reads as follows:

"Limitation on the Definition of Electronic Surveillance."
"Nothing in the definition of electronic surveillance under section 101 (f) shall be construed to encompass surveillance that is targeted in accordance with this title at a person reasonably believed to be located outside the United States."

In other words, even though the plain language of 101 (f) (2) covers all acquisitions from wire in the United States if either person is in the United States, the language in the reported bill asserts that it does not cover such an interception if it is directed at a person outside the United States. This is clearly a change in the definition and not a "limitation" on the definition as the SSCI bill labels it or a "clarification" of the definition as the Protect America Act (PAA) headed it.

Having said that words do not mean what they clearly do mean, the bill in two other sections says, "never mind." That is, as the Committee Report puts it, the bill "negates that limitation for the matters covered by those sections" that deal with the use of the information in criminal trials and exclusivity. However, there is no such "negation" of the "limitation" for the sections of FISA that establish criminal and civil penalties. Thus, the only result of this convoluted language might be to negate the possibility of civil or criminal penalties for illegal acquisition of this information. There is no reason to believe that this was the Committee's intent.

Language in a bill that says the legislation should not be "construed" in a certain way is useful if the language of the legislation is ambiguous or if there is a fear that the Executive branch or the courts might construe the language to imply something that was not intended. For example, in retrospect it would have been useful for Congress to have said in the Authorization to Use Military Force (AUMF) that it should not be" construed" as amending FISA. However, when the intent is to change the law it should be done in a straightforward way so there can be no ambiguity as to what was intended. This is especially important when we are dealing with civil liberties.

This result can be achieved simply by striking Section 701 and changing Section 703 (g) (2) (A) (vi) -- which sets out the requirements for the certification to be given to the FISA court – to read, " the surveillance is targeted at persons reasonably believed to be located outside the United States."

I urge the committee to ask the administration how their understanding of what the statute required would change if the legislation was amended in this way.

The Role of the FISA Court

The SSCI bill has important provisions which begin to re-establish an appropriate role for the FISA court, but much more needs to be done if the court is to be able to play its essential role in providing assurance to service providers and to the public that the rules established by the Congress are being followed.

The government should be required to go the FISA court first and to get approval from the court before it begins surveillance, except in an emergency situation. By definition, if there is no emergency, there is time to go to the court and there is no reason to allow the executive branch to begin a surveillance without first having court approval. Requiring as a matter of routine that court approval must come first will assure that the executive branch gives the matter the full consideration that it deserves before starting a surveillance which will lead to the acquisition of many conversations and communications of persons in the United States and Americans abroad. Moreover, requiring the executive to go to the court before beginning a surveillance would enable Congress to require that the service providers cooperate only if they have a court order or a certification in an emergency.

I cannot imagine any public policy argument to the contrary once one concedes that the court needs to play a role and there is an exception for emergencies with ample time limits. The SSCI Committee Report does not provide any rationale and I have not seen any from the Administration except the general statement that they do not want to be burdened. That is clearly not a sufficient reason in a constitutional democracy.

One consequence of the failure of the bill to require prior judicial authorization is that it also fails to empower the court to cut off surveillance that is illegal under the statute. Under proposed Section 703(j)(5)(B) the government can repeatedly submit new guidelines to the court every 30 days, and the court cannot order the surveillance to stop because the government can elect to continue it while it adjusts its procedures repeatedly.

Second, the legislation needs to make clear that the FISA court has continuing supervisory authority to insure that the surveillance is being conducted consistent with the statute. The court's authority to seek additional information and to order changes in the surveillance activity should not be left in doubt. The court should be able to supervise the minimization procedures and whatever procedures there are to insure that the communications of persons in the United States and Americans anywhere are not inappropriately acquired.

Let me turn to that issue.

Communications of Persons in the United States

If Congress extends beyond the period of the PAA the authority to acquire wire communications in the United States without individual warrants, it must take additional steps to insure that the communications of persons in the United States are not inappropriately acquired or disseminated beyond the NSA collection process.

There are, I think, two major concerns. One is abuse. There is legitimate concern that this vast power will be used to acquire communications of innocent Americans and used for political purposes. I see no suggestion that this has been done since 9/11, but the history of past abuses suggests that Congress needs to keep this concern in mind as it grants substantial additional powers to the Executive branch.

The second concern is how to deal with the conversations of U.S. persons and persons in the United States. At one end of the spectrum is an interception that is truly incidental and is not disseminated in a way that reveals the identity of the American. At the other end of the spectrum would be the intentional targeting of a person known to be in the United States. The bill does very little to deal with the vast space in between.

It is not easy to come up with an effective standard for when a regular FISA warrant should be required. That is the strongest reason, in my view, to have a much shorter sunset time for this new grant of authority. Congress must be in a position in a short time to assess how this balance is working and to determine if additional safeguards are needed.

There are several additional steps that I urge the committee to take to deal with this serious concern.

First, I urge you to adopt the provision included in the House bill which requires that guidelines be adopted and approved by the FISA court that "will be used to ensure that an application is filed under section 104, if otherwise required by this Act, when a significant purpose of an acquisition is to acquire the communications of a specific person reasonably believed to be located in the United States."

In other words, if the intelligence community wants to acquire the communications of a specific person in the United States, it must get a standard FISA warrant based on probable cause that one of the communicants is a foreign power or the agent of a foreign power. This seems to be a reasonable operational definition of when the acquisition of communications is no longer incidental. I am not aware of any specific response from the intelligence community to this language and urge the committee to seek an evaluation of its impact on the proposed program.

Second, the committee should provide for record keeping which will enable the court, the committees and others to more effectively monitor this process. This should include requiring that records be kept of all "unmasking" of the identities of U.S. persons from communications acquired by this program. Records should also be kept and reported regularly of the number of persons in the U.S. whose communications are disseminated as well as the number of times in which the target of the communication actually turned out to be in the United States or to be a U.S. person abroad.

I urge the Committee to consider two additional steps. First, you should consider creating a presumption, to be monitored by the FISA court, that if the NSA disseminates more than three conversations of the same U.S. person, that person has become a subject of interest to the intelligence community so that a warrant would be required to disseminate additional conversations or to intentionally acquire them. I suggest a presumption because I think the government should be able to show that for some particular reason the dissemination is appropriate.

Finally, I urge you to consider a limitation on the types of foreign intelligence information that can be disseminated from this program if it concerns a U.S. person. Since the need for this new authority arose as a result of the new demands following 9/11, there is every reason to consider limiting the new authority to collecting information related to international terrorism. If that is not done, at the very least there should be a limit on the kinds of information about Americans derived from their conversations that can be disseminated.

The appropriate divide is between information in (e) (1) as opposed to (2) of the FISA definition of foreign intelligence information. FISA established this breakdown precisely to distinguish between information about activities that were inherently illegal, such as espionage, sabotage or terrorism, as compared to the information in (2) which deals with information of interest to the intelligence community about national security or foreign policy but which includes many innocent conversations among, for example, experts on a particular country.

Exclusive Means

Let me turn finally to the question of exclusive means. Here I want to associate myself with the very thoughtful additional views of Senators Feinstein, Snowe and Hagel to the SSCI Report.

I believe, as they do, that the original FISA legislation was as clear as legislation can be. Congress intended that the means that it provided would be the exclusive means for conducting electronic surveillance for intelligence purposes. When it referred to "other statutes" it meant the criminal laws, and

when it referred to "certifications that a warrant was not required and that the statutory requirements had been met" it meant the statutory requirements of FISA and not of another statute.

Nonetheless, because both the Executive branch and, apparently, the service providers claim to have read FISA differently, Congress should take some additional steps beyond those in the SSCI bill to make clear to all concerned that Congress intends the means authorized by FISA to be the sole means to conduct this surveillance.

It is particularly important to do this if the Congress is going to grant some form of relief to the service providers for their past behavior. Indeed I think it is essential that the service providers publicly and unequivocally acknowledge that in the future they will be liable for civil and criminal penalties if they cooperate with the intelligence community outside the procedures of FISA.

Here are the additional steps that I suggest:

1. As I have already proposed, eliminate Sec. 701. This is essential to avoid any suggestion that electronic communication conducted for intelligence purposes in the United States is not covered by the exclusivity provisions or by the criminal and civil penalties.

2. At each place in FISA where Congress grants authority to conduct electronic surveillance without a court order, add a phase specifying that the certification given to a service provider must specify the specific statutory provisions being relied on and that the specific requirements of that section have been met. This will prevent the Attorney General from providing a general certification that the surveillance is lawful.

3. Add general language that the requirements of FISA can be amended only by legislation enacted after the enactment of these amendments that specifically refers to FISA and specifically amends the authority to conduct electronic surveillance. This would make impossible the kind of specious argument made by the government that the AUMF somehow amended FISA and make it unnecessary to say in every bill passed later that it should not be construed so as to authorize surveillance outside of the FISA procedures.

4. Amend the section of FISA that provides for criminal and civil penalties for cooperation outside of the FISA procedures. Here is the proposed change to 2511 (2) (a) (ii) (B) dealing with cooperation permitted without a court order:

(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by [law] a specific provision of the Foreign Intelligence Surveillance Act

, specifying the provision and stating that all statutory requirements of that specific provision have been met, and that the specified assistance is required.

This change would eliminate any possible intentional or unintentional misreading of the clear intent of the language. Service provides and government officials alike would be on notice that they can cooperate with a surveillance only if there is a court order or the government is acting pursuant to the specific requirements of a provision of FISA which authorizes surveillance without a court order, either temporarily while a warrant is obtained or under circumstances, such as the lease line exception, where the statute does not require a court order, and that the requirements of that provision have been satisfied.

Taken together and with what is already in the SSCI bill, I believe the language would provide the strongest possible assertion of exclusive means while sending a totally unambiguous message to service providers that in the future they should not come to Congress for relief if they cooperate outside the requirements of this legislation.

Conclusion

Mr. Chairman, I appreciate very much this opportunity to testify before this Committee and present views on possible amendments to FISA. At the same time I am aware that there are many other individuals and groups with a deep interest in FISA whose views are not necessarily identical to those presented in my statement. I trust the committee will consider those views as well, as it debates this critical legislation.

I would, of course, be delighted to respond to your questions or to submit any additional information for the record.