Testimony of

Mr. James X. Dempsey

July 26, 2006

Statement of James X. Dempsey
Policy Director
Center for Democracy and Technology
before the
Senate Judiciary Committee

"Modernization of the Foreign Intelligence Surveillance Act"

July 26, 2006

Chairman Specter, Ranking Member Leahy, Members of the Committee, thank you for the opportunity to testify today.

Is "Modernization" Another Way of Saying Warrantless Searches and a Blank Check for the President?

Undoubtedly, it is appropriate to consider from time to time whether the Foreign Intelligence Surveillance Act should be amended to respond to the changing threats facing our nation or advances in technology. However, FISA has been modernized already several times since 9/11, most notably in the recently reauthorized PATRIOT Act, and providers of digital communications services in the US have for some years been modifying their network to accommodate government surveillance.

The Chairman's bill as it stands today is not a modernizing bill. Rather, it would turn back the clock to an era of unchecked Presidential power, warrantless domestic surveillance, and constitutional uncertainty.

We commend Chairman Specter for his tireless leadership in seeking to ensure judicial review of this President's warrantless surveillance program. From the outset, the Chairman has criticized the Administration's disregard for FISA's express requirements. He has vigorously sought more information about the program, and he has held repeated hearings. The Chairman has worked across the aisle to draft legislation with Senator Feinstein. Now, through intense negotiations, the Chairman has secured the promise of the President to submit his current program to court review. With profound respect, we must conclude that the price the Chairman paid for that simple concession is far too high.

FISA, a Complex but Proven Statute, Should Be Amended Only with Great Caution and Only on the Basis of a Public Showing of Need

Prior to this hearing, the Administration has made no showing on the public record that FISA is in need of further amendment, with the sole exception of the Attorney General's explanation of problems involving FISA's emergency exception, problems due in part to the paperwork burdens created by the Executive Branch and perpetuated by this Administration.

Perhaps at this hearing, the Administration's witnesses will describe further specific defects in FISA. If they do, we will endeavor to respond to them in our oral remarks, but, surely, any issues the Administration raises at this hearing will require further careful study. Certainly, if the Administration identifies any problems at this hearing (on Wednesday), it is too soon to expect that suitable responses to them can be drafted and understood by the next day (Thursday), when this Committee may again take up FISA-related legislation, or even by next week.

Congress can best modernize FISA - if it needs modernizing -- only after further hearings, building on public testimony by the Administration. Updating FISA in a way that is Constitutional and responsive to the Administration's needs will require an iterative process of in-depth analysis (some of it necessarily classified) and public dialogue.

The threat of terrorism demands such a careful response. Of course, the government must have strong powers, including the authority to carry out various forms of electronic surveillance. However, not only to protect constitutional rights but also to ensure effective application of those powers, government surveillance must be focused. That focus can best be achieved through a system of checks and balances, implemented through executive, legislative and judicial review.

Any modernization of FISA should be open not only to ways in which the Act may unduly burden intelligence gathering but also to ways in which its controls need to be tightened in light of modern realities. The standards of the surveillance laws, weak in some key respects before 9/11, have been eroded by the PATRIOT Act, by Executive Branch actions, and most dramatically by the evolution of technology, which has made more and more personal information readily accessible to the government. A number of steps - none of them in current proposals -- could be taken to improve FISA compliance, accountability, oversight and transparency.

The Chairman's New Legislation Would Not Modernize FISA - It Would Turn Back the Clock to an Era of Warrantless Domestic Surveillance

Since last December, the President, the Attorney General, and other senior Administration officials have stated that the President's program of warrantless wiretapping is narrowly focused on international calls of suspected terrorists, that the program is used in circumstances where immediate monitoring is necessary for some short period of time, that domestic calls are not covered, and that in every case there is reasonable ground (or "probable cause") to believe that the target is associated with al Qaeda. The Administration has repeatedly assured lawmakers and the public that it is not engaged in a program of "domestic surveillance."

Chairman Specter has negotiated with the Administration a bill that would turn back the clock, not only by repealing FISA's exclusivity provision but also by authorizing a domestic program far broader - and far more intrusive on the privacy of American citizens -- than the one the President and Attorney General have described.

Section 4 - The Chairman's Bill Would Not Guarantee Judicial Review of Future Surveillance Programs Affecting Americans

The President has promised that he will submit his warrantless surveillance program for FISA court review if the Chairman's bill is enacted. With the highest respect for the Chairman, this is a small if not meaningless concession.

First, it is not clear that any legislation is necessary to get the President's program reviewed, since the program is already the subject of 30 pending cases. In the lead case, the district court last week turned aside a government effort to dismiss the case and is headed towards consideration of the merits.

Second, the Chairman's bill does not bind this President to submit for judicial review future programs nor does it require future Presidents to submit their programs for court review - programs that may be substantially different from this President's program.

Third, the definitions used in the Chairman's bill might fail to give the FISA court jurisdiction to review the President's program:

? The President has said that his program only allows short term monitoring, but the Chairman's bill applies only to programs of long term monitoring.
? The Attorney General has said that in every case, the President's program targets a specific suspected member or affiliate of al Qaeda, but the Chairman's bill applies only when it is not possible to specify who is being targeted.

Even assuming that the Chairman's bill would allow the FISA court to review the President's program, in other key ways the bill undermines judicial review by forcing transfer to the Foreign Intelligence Surveillance Court of Review (FISCR) of any case initiated by a citizen challenging a communications intelligence activity of the government. In these cases, the government would have the benefit not only of all its normal procedural grounds for seeking dismissal of a case but also of the largely ex parte and in camera processes of the FISCR, making it virtually impossible for parties challenging the government program to overcome the evidentiary burdens they would face.

Finally, the Chairman's bill imposes no consequences on the Administration should the Court refuse to approve the President's program. Unlike FISA, which states that surveillance begun without court approval must cease if the surveillance is later found to be unjustified, the Chairman's bill does not say that the government must cease programmatic activity that the court refuses to approve.

The Price Is Too High - Turning the Clock Back to an Era of Unchecked Presidential Power and Warrantless Domestic Surveillance

What did it take to get the President to agree to submit his program to judicial review? It took a radical rewrite of FISA: the authorization of a broad new category of domestic surveillance, under "programmatic" or "general search" warrants; the repeal of FISA's exclusivity provision, making the entire statute, including the Chairman's amendments, merely optional; the repeal

FISA's wartime exception, granting the President a blank check in domestic surveillance; and, in Section 9, major new exceptions to the warrant requirement for communications to which Americans are a party.

Sections 5-6 -General Warrants

Sections 5 and 6 of the Chairman's bill would authorize (but not require) the Administration to apply for, and the FISA court to grant, "general warrants," which are prohibited by two key provisions of the Fourth Amendment: particularity and probable cause.

With a general warrant, the Chairman's bill would authorize a program of domestic surveillance far broader than President Bush's program. The Attorney General has said that the President's program targets only communications with particular suspected members or affiliates of al Qaeda, only on the basis of probable cause, and only if one leg of the call is with a party overseas. The latest version of the Chairman's bill would authorize seizing the contents of purely domestic calls of American citizens without probable cause, without specific suspicion, and where the call has nothing to do with al Qaeda and not even anything to do with terrorism.

The substitute is especially broad because it allows interception intended to collect the communications not only of suspected terrorists but also a person who "is reasonably believed to have communication with or be associated with" a terror group or suspected terrorist. This means that a journalist who interviews a suspected terrorist, and doesn't even know that the person is considered a terrorist, could be subject to surveillance under this bill. Also, there is no limit on "associated with." Is one "associated with" a suspected terrorist because one goes to the same mosque? Is one "associated with" a suspected terrorist because one has roots in the same village or neighborhood? These connections may be worth checking out, but they are not adequate basis for content interception, which has always been considered one of the most intrusive forms of government invasion of privacy.

Also, the substitute does not use the Constitutional concept of probable cause. It actually does not specify the standard the court must use in determining whether the government has made the requisite showings. Instead, the substitute states that the court must find that the program is "reasonably designed" to intercept the communications of suspected terrorists or persons "reasonably believed [by whom it doesn't say] to have communication with or be associated with" suspected terrorists.

Invoking the FISA court's approval is purely optional under the substitute. Unlike the original version of the Chairman's bill, the substitute does not require the Administration to submit the President's warrantless surveillance program or any future program for judicial review.

The Chairman's bill, unlike FISA, requires either that a "significant purpose" of the program be the collection of foreign intelligence or that its purpose be to "protect against international terrorism," which means that the program can be used when its sole purpose is the collection of criminal evidence

While initial court approval of a program would be for up to 90 days, the court could renew the program for any length of time it deems reasonable.

Section 8 - The Repeal of FISA's Exclusivity Provision Is Significant

Section 9 of the Chairman's bill would repeal the exclusivity provisions of FISA and allow the President to choose, at his discretion, between using FISA and pursuing some other undefined and constitutionally questionable method to carry out secret surveillance of Americans. This provision would turn back the clock 30 years ago, inviting a return to the era of COINTELPRO and the intelligence-related abuses that created confusion and drove down morale inside the intelligence agencies.

Repeal of exclusivity is not meaningless, for the whole purpose of the exclusivity clause is to constrain any "inherent power" the President has to carry out electronic surveillance in the absence of Congressional action. Indeed, in 1978, this very Committee stated in its Report on FISA that, "even if the President has 'inherent' constitutional power to authorize warrantless surveillance for foreign intelligence purposes, Congress has the power to regulate the exercise of this authority by legislating a reasonable warrant procedure governing foreign intelligence surveillance."

In its recent opinion in Hamdan v. Rumsfeld, the Supreme Court majority noted, "Whether or not the President has independent power, absent congressional authorization, to convene military commissions, he may not disregard limitations that Congress has, in proper exercise of its own war powers, placed on his powers." Justice Kennedy, in his concurrence, explained why it is both constitutional and desirable for the Congress and the President to work together to devise a consensus set of rules for the exercise of national security powers and why the President is bound by those rules enacted by Congress:

This is not a case, then, where the Executive can assert some unilateral authority to fill a void left by congressional inaction. It is a case where Congress, in the proper exercise of its powers as an independent branch of government, and as part of a long tradition of legislative involvement in matters of military justice, has considered the subject of military tribunals and set limits on the President's authority. Where a statute provides the conditions for the exercise of governmental power, its requirements are the result of a deliberative and reflective process engaging both of the political branches. Respect for laws derived from the customary operation of the Executive and Legislative Branches gives some assurance of stability in time of crisis. The Constitution is best preserved by reliance on standards tested over time and insulated from the pressures of the moment. . . .

There is no doubt about it: repeal of exclusivity would restore to their full, albeit undefined scope, the President's inherent powers to conduct surveillance, turning back the clock to the era of uncertainty and abuse.

Section 9 - Total Information Awareness on Steroids?

To cinch the deal with the White House, the Chairman has added to his bill a new Section 9, which would vastly expand the scope of warrantless surveillance that never has to be submitted to a court and create a vast database of phone calls and other information reminiscent of the Total Information Awareness program, which the Administration could data mine at will, outside any judicial or congressional oversight.

Probably 30% of the meaning of FISA is buried in its definitions, especially its definition of "electronic surveillance" and "minimization procedures." Sugar-coated as "conforming amendments," the changes made by Section 9 to these two definitions, and the changes to Section 102 of FISA, would authorize large-scale warrantless surveillance of American citizens and the indefinite retention of citizens' communications for future datamining.

The "cut and bite" amendments of Section 9 are very hard to parse, but so far, we have identified the following remarkable provisions:

? The bill makes major changes to FISA's definition of electronic surveillance. Under FISA, if the collection of information fits within the definition of "electronic surveillance," it requires a court order or must fall under one of FISA's exceptions. If the collection of information is outside the definition of electronic surveillance, then it is not covered by the Act, and can be carried on without a warrant. Therefore, narrowing the definition of electronic surveillance places more activity outside the oversight of the Act. Section 9 makes major changes to the definition of electronic surveillance, permitting the NSA's vacuum cleaners to be turned on any international calls involving US citizens.

? In what may be the most far-reaching provision, Section 9 amends section 102 of FISA (50 USC 1802) to allow the "Attorney General" to authorize warrantless surveillance if it is "solely directed at the acquisition of the communications of a foreign power or agent of a foreign power." Under this amendment, so long as the surveillance is "directed at" a foreign power or non-US person suspected of being an agent of a foreign power, the government can intercept the purely domestic calls of US citizens without court order.

? Under the bill, if he chooses, the Attorney General can designate anyone - his secretary, the janitor, an official of the department of Defense, a local police officer, as "Attorney General", thereby authorized to approve warrantless surveillance under section 102, to issue certifications to communications companies and others, and to carry out all the other duties assigned to the Attorney General under the Act.

? The bill amends the definition of a non-US person agent of a foreign power to include someone who "possesses or is expected to transmit or receiving foreign intelligence while in the" US.

The Specter- Feinstein Bill Is the Correct Approach

It is important to note that Senator Feinstein is one of the members of the special Senate Intelligence Subcommittee that received classified briefings about the President's program(s). After receiving the briefings, she concluded that the appropriate legislative response would be a bill narrowly focused on the issues the Administration said caused it to circumvent FISA-namely, the need for more resources, greater speed in approving FISA applications and more flexibility to begin wiretapping in an emergency. Significantly, Senator Feinstein remained convinced after receiving classified briefings that the program(s) can and should be conducted under FISA.

The Specter-Feinstein bill responds to the Administration's public testimony to date. As we understand the Attorney General's testimony, the sole reason the administration could not use FISA was that the emergency procedure was not flexible enough. This bill addresses that issue by

providing more resources to the FISC, DOJ, FBI, and NSA and allowing the Attorney General to delegate the power to approve applications and to authorize surveillance in emergencies.

The most important aspect of this bill is its reaffirmation that FISA and Title 18 are the exclusive means by which the government can conduct electronic surveillance. The bill reinforces this by prohibiting the appropriation of funds for electronic surveillance outside of FISA or Title 18 and by stating that if Congress intends to repeal or modify FISA in future legislation, it must expressly state in the legislation its intention to do so.

Specter-Feinstein would:

? reaffirm the exclusivity provisions of FISA and Title 18;
? prohibit the appropriation of funds for any electronic surveillance conducted outside of FISA or Title 18;
? enhance congressional oversight;
? extend the FISA emergency period from 72 hours to 7 days;
? allow the Attorney General to delegate authority to approve FISA applications and to authorize emergency surveillance;
? give the FISC, DOJ, FBI and NSA the ability to hire more staff as necessary to meet the demands of the application process;
? give the Chief Justice of the United States the power to appoint additional judges to the FISC, as needed;
? mandate the development of a document management system to expedite and facilitate the FISA application process; and
? make "authorization for the use of military force" and the declaration of a "national emergency" events that trigger the FISA wartime exception.

The Administration's Testimony To Date Has Merely Reaffirmed the Enduring Value of FISA's Core Principles

FISA contains five basic principles, each of which is independent from the others, and prior to today the Administration has not made a case for altering any of them:

? Except in emergency situations, the government must obtain prior judicial approval to intercept communications inside the US.
? Congress carefully oversees surveillance activity within the US, which presumes that Congress is fully informed of all surveillance activity.
? The interception of the content of communications is focused on particular individuals suspected of being terrorists or particular physical or virtual addresses used by terrorists.
? The threshold for initiating a content interception is probable cause to believe that the target is a terrorist and that the interception will yield intelligence.
? The rules laid down publicly in statute are the exclusive means for carrying out electronic surveillance within the US.

So far, on the first question, the Administration has offered on the public record no reason for dispensing with prior judicial approval, except in emergency cases for short-term surveillance.

Other than its philosophical antipathy to Congressional oversight, the Administration has offered no substantive reason for not seeking the support and oversight of Congress.

In terms of particularized suspicion, on the record so far the Administration has consistently emphasized that all interceptions of content under the President's Terrorist Surveillance Program are based on particularized suspicion.

In terms of probable cause, the Attorney General emphasized in Congressional testimony that the Administration is adhering in the Terrorist Surveillance Program to the probable cause standard.

On the question of exclusivity, twice the Supreme Court has rejected the Administration's extreme views of executive power, and, in any case, for a variety of reasons, intelligence activities are most effectively sustained when they are carried out on the basis of a public consensus between Congress and the Executive Branch.

Despite the lack of any publicly articulated rationale, the bill the Chairman negotiated with the Administration would cast aside all five of these principles.

FISA Has Well-Served Both Civil Liberties and the National Security

FISA has well-served the nation for nearly 30 years, placing electronic surveillance inside the United States for foreign intelligence and counter-intelligence purposes on a sound legal footing. Tens of thousands of surveillance orders have been issued under FISA, and the results have been used in hundreds of criminal cases, and never once has a constitutional challenge been sustained.

Changing FISA in the radical ways now being proposed would jeopardize this certainty and could harm the national security. It would cast a cloud of constitutional doubt over intelligence gathering. Those in the government and the private sector who carry out electronic surveillance would no longer be assured their actions were lawful. Hesitation and second-guessing could inhibit risk-taking. In the absence of mandatory court review, internal doubts might arise more frequently about the legality of a program, but those with concerned might see no other option except to publicly leak the existence of the program in order to force its reconsideration. If the Administration did find a terrorist through surveillance under a radically different FISA, that person might escape conviction and imprisonment if the evidence against him were rejected on constitutional grounds.

FISA Has Already Been Modernized

In the PATRIOT Act and in other legislation since 9/11, Congress has already "modernized" FISA. In signing the PATRIOT Act in 2001, President Bush specifically concluded that it would modernize FISA:

We're dealing with terrorists who operate by highly sophisticated methods and technologies, some of which were not even available when our existing laws were written. The bill before me takes account of the new realities and dangers posed by modern terrorists. ... This new law that I sign today will allow surveillance of all communications used by terrorists, including e-mails,

the Internet, and cell phones. As of today, we'll be able to better meet the technological challenges posed by this proliferation of communications technology.

Four and half years later, when the PATRIOT Act's sunsetting provisions were reauthorized, the Justice Department concluded on the basis of its record that the PATRIOT Act had done its job in modernizing FISA and other laws:
The USA PATRIOT Act, enacted on October 26, 2001, has been critical in preventing another terrorist attack on the United States. It brought the federal government's ability to investigate threats to the national security into the modern era--by modifying our investigative tools to reflect modern technologies ... .

In contrast, recent proposals seem intended not to "modernize" FISA, but to cast aside fundamental Fourth Amendment protections simply because the government has too much communications information available to it for easy interception.

Public Congressional Hearings Led To Enactment of FISA, and Should be the Prerequisite for Any Major Changes

Congress can examine FISA publicly without compromising national security. Of course, some elements of the inquiry will have to be conducted in secret, with in-depth staff involvement, but once Congress has the full picture it can and should conduct public hearings with Administration witnesses taking the lead. Indeed, Congress did this successfully thirty years ago: FISA was the product of exhaustive public hearings. The debate on FISA was full and robust. There were years of fact-based hearings and extensive staff investigations into the complete facts about spying on Americans in the name of national security. Multiple committees in both Houses considered the legislation in both public and closed hearings. There was extended floor debate as well. The secrecy of electronic surveillance methods was preserved throughout.

Congress cannot determine whether or how to change FISA without a thorough understanding of what the Administration is doing domestically and why it believes the current law is inadequate. The Administration must explain to Congress why it is necessary to change the law, and Congress must satisfy itself that any recommended changes would be constitutionally permissible. As Chairman Hoekstra recently said in his letter to the President, "Congress simply should not have to play Twenty Questions to get the information that it deserves under our Constitution."

Technological Changes Improve the Government's Surveillance Capabilities and May Justify Tighter Controls

The digital revolution has been a boon to government surveillance. The proliferation of communications technologies and the increased processing power of computers have made vastly greater amounts of information available to the government. In some respects, digital communications are easier to collect, store, process and analyze than analog communications.

If FISA is ill-suited to the new technology, it is because its standards are too weak and the vacuum cleaner technology of the NSA is too powerful when aimed domestically, given the reliance of so many ordinary Americans on the Internet, its global nature, and the huge growth in

the volume of international communications traffic on the part of ordinary Americans. Given the post-9/11 loosening of regulations governing intelligence sharing, the risk of intercepting the communications of ordinary Americans and of those communications being misinterpreted by a variety of agencies as the basis for adverse action is vastly increased. This context requires more precise--not looser--standards, closer oversight, new mechanisms for minimization, and limits on retention of inadvertently intercepted communications.

Technology Can Support Particularity

It has been suggested that it is difficult or impossible for the government to isolate the communications of specific targets in networks using packet switching rather than circuit switching technology. However, partly as a result of the Communications Assistance for Law Enforcement Act of 1994 (CALEA), a number of companies are offering technology to isolate packet communications for government surveillance. One company, for example, notes that its surveillance technology for broadband Internet service providers and ISPs "is highly flexible, utilizing either passive probes or active software functionality within the network nodes to filter out traffic of interest." Cisco recently released its "Service Independent Intercept Architecture," which uses existing network elements and offers an "integrated approach that limits the intercept activity to the router or gateway that is handling the target's IP traffic and only activates an intercept when the target is accessing the network." http://www.cisco.com/technologies/SII/SII.pdf VeriSign is another company offering comprehensive services for interception:

VeriSign operates as a Trusted Third Party (TTP) assisting service providers in meeting the legal, technical and operational requirements for lawful assistance and legal interception as required by the Communications Assistance for Law Enforcement Act (CALEA). VeriSign NetDiscovery Service is a managed service provides a reliable, end-to-end solution that can help accomplish compliance quickly on traditional and packet-based network deployments.

CALEA, it should be noted, requires service providers in the United States to have the technological ability to isolate the communications of a surveillance target to the exclusion of the communications of all other users of the network. It must be emphasized that FISA only applies to surveillance inside the United States, where the intelligence agencies have the willing and court-ordered cooperation of service providers. The vacuum cleaner approach is sometimes necessary overseas because the intelligence agencies do not have the cooperation of local service providers. The vacuum cleaner, let alone being unconstitutional, is not necessary inside the US. It is also noteworthy that the FBI reports that it does not have to use its notorious Carnivore, or DCS 1000, which was intended to isolate targeted IP communications, because commercially available software is able to do the job.

Technology is not a substitute for sound policy. In this case, however, the trend of technology seems to favor, not excuse, particularity.

Improving FISA Compliance, Transparency, Accountability and Oversight

There are a number of steps Congress could take improve to FISA compliance, accountability, oversight and transparency, including facilitating district court review of FISA surveillance when the government uses FISA evidence in criminal cases, providing notice to individuals who have

been FISA targets and who turn out to be innocent, and developing procedures for handling judicial challenges to surveillance short of invoking the state secrets doctrine.

Conclusion

Mr. Chairman, Members of the Committee, we urge you to look on this as a process that will take some care. The Administration should engage in a debate on the public record, and equal attention should be given to ways in which civil liberties safeguards should be strengthened as well as to ways in which procedures can be streamlined.