Statement of James X. Dempsey
Policy Director
Center for Democracy and Technology[1]

before the

House Committee on the Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security

"Updating FISA"

H.R. 4976, the "NSA Oversight Act"
H.R. 5113, the "Fairness and Accountability in Reorganizations Act of 2006"
H.R. 5371, the "Lawful Intelligence and Surveillance of Terrorists in an Emergency by NSA Act"
H.R. 5825, the "Electronic Surveillance Modernization Act"
S. 2453, the "National Security Surveillance Act of 2006"
S. 2455, the "Terrorist Surveillance Act"

September 6, 2006

Chairman Coble, Ranking Member Scott, Members of the Subcommittee, 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 updated already several times since 9/11, most notably in the recently reauthorized PATRIOT Act.

Something fundamentally different than mere updating is being proposed today. The Administration, caught in its secret violation of FISA, is now seeking radical changes in the law, changes that go farther even than ratifying the President's program. The most radical proposal is that of Chairman Specter, which would effectively gut FISA by repealing its exclusivity provision, making it merely optional for the Administration to seek a court order for electronic surveillance inside the United States against American

[1] The Center for Democracy and Technology is a non-profit, public interest organization dedicated to promoting civil liberties and democratic values for the new digital communications media. Among our priorities is preserving the balance between security and freedom after 9/11. CDT coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for computer, communications, and public interest organizations, companies and associations interested in privacy and security issues.

citizens. The bill co-sponsored by Chairman Sensenbrenner, while it would preserve the nominal exclusivity of FISA, not only would ratify the President's program of warrantless surveillance for foreign-to-US communications, but also would permit much more warrantless surveillance of purely domestic calls. The result would be to cast a cloud of constitutional uncertainty over what the Administration claims is a valuable tool in preventing terrorism.

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

So far, the Administration has made on the public record only three, quite narrow arguments that FISA is in need of further amendment:

- the Attorney General's explanation of problems involving the timely invocation of FISA's emergency exception, problems due in part to the paperwork burdens created by the Executive Branch and perpetuated by this Administration;
- the concern that a court order is required for the interception of foreign-to-foreign communications of non-U.S. persons that happen to pass through the US, where they can be more readily accessed by US government agencies;
- the concern that, when the government is targeting the foreign communications of a non-US person overseas, the wiretap has to be turned off when the target makes a call to the US.

The first of these problems is addressed in the Harman-Conyers bill. The second may not even need legislation, but presumably a narrow clarification could be crafted. The third issue is one that was mentioned at the Senate hearing in July, but again, if it genuinely is a problem, it could be dealt with by a narrow amendment. In contrast, the bills of Chairmen Sensenbrenner and Specter go dramatically further and make radical changes to FISA.

Perhaps at this hearing, the Administration's witnesses will describe further specific defects in FISA. If they do, surely they will require further careful study to ensure that any solution is responsive but not overbroad.

Congress can best update FISA – if it needs updating -- only after further hearings, focusing on the problems publicly identified 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.

In addition, 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 Harman-Conyers Bill (H.R. 5371, the LISTEN Act) Charts the Correct Approach

Rather than radically amending or de facto repealing FISA, as some other measures would, the LISTEN Act reiterates that FISA and Title III are the exclusive means by which the President can conduct domestic electronic surveillance. It requires the President to obtain a court order before targeting someone in the US for surveillance and it directs the President to report to Congress on the need for more resources and any legislative and procedural changes that are necessary. It also makes clear that the Authorization to Use Military Force did not authorize the President to conduct warrantless surveillance outside of FISA or Title III.

By returning the courts and the Congress to their proper places as equal branches of government, this bill restores the constitutional balance of power that the Administration's warrantless surveillance program has upended. CDT supports H.R. 5371's reaffirmation of congressional oversight and judicial supervision of governmental surveillance.

The Flake-Schiff Bill (HR 4976, the "NSA Oversight Act") Reaffirms Congress's Constitutional Role

We also support the Flake-Schiff bill, which similarly reinforces the exclusive procedures for wiretapping passed by Congress and also requires additional reporting about surveillance to Congress. The bi-partisan NSA Oversight Act also reaffirms that FISA is the exclusive process through which foreign intelligence surveillance can be conducted on these shores. Further, the bill insists on full disclosure to the Congress from the President about the domestic targets of the so-called "Terrorist Surveillance Program."

The NSA Oversight Act reaffirms that under our system of government, Congress makes the laws and the President must faithfully execute them. It reestablishes that laws passed by Congress cannot be modified unilaterally by any President but must be amended by Congress.

The Wilson-Sensenbrenner-Hoekstra Bill Would Make Radical Changes to FISA

Chairman Sensenbrenner, along with HPSCI Chairman Hoekstra, has cosponsored legislation introduced by Rep. Wilson that would make significant changes to the Foreign Intelligence Surveillance Act, mainly by expanding the circumstances under which the government can conduct warrantless electronic surveillance in the United States, including surveillance of the communications of US citizens. Chairman Specter has added similar language to his bill, as a new Section 9, so in this analysis we also reference the Specter legislation. (Sometimes herein we refer to the Wilson-Sensenbrenner-Hoekstra bill as simply "the Wilson bill.") The Wilson bill, unlike the Specter bill, does not repeal FISA's exclusivity provision.

How The Revised Definitions Expand Warrantless Surveillance

Probably 30% of the meaning of FISA is buried in its definitions, especially its definition of "electronic surveillance" and "minimization procedures." The changes made by Wilson-Sensenbrenner-Hoekstra 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.

"Agent of a foreign power:" Both bills would expand the definition of an agent of a foreign power to include a non-US person who "otherwise possesses or is reasonably expected to transmit or receive foreign intelligence information within the United States." It is unclear what is the purpose of this change, but since the FISA definition of "person" includes corporations, this amendment could expand FISA to permit surveillance (sometimes with a court order, sometimes without) of communications to, from or through every foreign-owned bank, airline, or communications company and any other foreign corporation in the US if it has information that is foreign intelligence (such as financial transactions, travel arrangements, or communications).

"Electronic surveillance:" Both bills would amend the crucial definition of "electronic surveillance" in FISA, in ways that would allow much more warrantless surveillance. The following is the text of FISA as it would be amended by the bills. (Deleted text is crossed out and new text is in italics. The amendments are largely identical. Where the Wilson bill would differ from Chairman Specter's, the variations are indicated by footnotes). The Center for National Security Studies produced the following "redline:"

"(f) 'Electronic surveillance' means—

"(1) the ~~acquisition by~~ *installation or use of* an electronic, mechanical, or other[2] surveillance device ~~of the contents of any wire or radio communications sent by or intended to be received by~~ *for the intentional collection of information concerning*[3] a

[2] The Wilson bill would delete the phrase "electronic, mechanical, or other."

[3] The Wilson bill would use the phrase "relating to" rather than "concerning."

particular known[4] ~~United States~~ person who is *reasonably believed to be* in the United States ~~if the contents are acquired~~ by intentionally targeting that ~~United States~~ person under circumstances in which that person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; or

~~(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, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of title 18;~~

~~(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or~~

~~(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.~~

(2) the intentional acquisition of the contents of any communication[5] under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States."

The net result of these changes is as follows: Currently, FISA requires a court order to intercept wire communications into or out of the US, many of which involve US citizens. Under the proposed new definition, wire communications to or from the US could be intercepted using the vacuum cleaner of the NSA, without a warrant, so long as the government is not targeting a known person in the US. If the government were targeting someone who is overseas, they would be able to intercept communications between that person and citizens in the US without a warrant. And if the government is engaged in broad, unfocused collection, it could intercept all international communications without a warrant, even those originated by citizens and even those involving citizens on both ends.

"Minimization procedures:" Under current law, if the government, acting without a warrant under Section 102(a) of FISA, obtains the communications of a US person, those communications cannot be disclosed, disseminated or used, and the

---

[4] The Wilson bill would delete the phrase "particular known."

[5] The Wilson bill would insert the phrase ", without the consent of a party to the communications," after "any communication."

government must destroy them within 72 hours unless the Attorney General obtains a court order or determines that the information indicates a threat of death or serious physical harm. Both bills would permit unrestricted retention and use of the communications of US citizens obtained without a warrant.

This change is especially important in light of the changes made to Section 102(a), which include new authority for warrantless surveillance of a wide range of domestic and international calls involving US citizens. Current law requires a warrant if there is a substantial likelihood that surveillance inside the US will acquire the contents of communications of US persons. Both the Wilson bill and the Specter bill repeal that limitation and also eliminate the requirement in Section 102(a) that any warrantless wiretapping be limited to means of communications "used exclusively between or among foreign powers."

"Surveillance device:" The Wilson bill includes a new definition for "surveillance device," a term that is not currently defined in FISA. It defines "surveillance device" as a "device that allows surveillance by the Federal Government, but excludes any device that extracts or analyzes information from data that has already been acquired by the Federal Government by lawful means." This appears to exclude data mining activities from coverage under the statute, and, given the breadth of warrantless surveillance permitted under the Wilson bill, amounts to a Total Information Act program, in which the government collects large amounts of data without court order, keeps it forever, and analyzes it at any time without court approval. The Specter bill does not include this definition.

"Attorney General:" The Specter bill redefines "Attorney General" to include "any person or persons" designated by the Attorney General, which means any janitor can be designated by the Attorney General to exercise his powers under FISA. The Wilson bill does not include this provision.

How the Amendments to FISA Section 102 Expand Warrantless Surveillance

Both bills would significantly expand Section 102(a) of FISA, 50 USC § 1802(a), which allows warrantless surveillance inside the US under certain conditions for up to a year. While the two bills are somewhat different, both would vastly expand the warrantless surveillance of US citizens.

- While the Specter bill expands warrantless surveillance of all communications of all foreign powers and non-US person agents of foreign powers, the Wilson bill would expand warrantless surveillance of the communications of only certain foreign powers (i.e., those that are foreign governments, factions of foreign nations or entities controlled by foreign governments) and all non-US person agents of foreign powers (AFPs). Both bills would allow warrantless surveillance whenever a citizen calls the Israeli embassy or Olympic Airlines.

- Both bills would permit warrantless surveillance of both international and domestic calls.

- Both bills would permit the warrantless acquisition of "technical intelligence," which is not a defined term.

- Both bills would permit the acquisition of communications to which a US person is a party. Currently, warrantless surveillance under1802 is permitted only if the surveillance is not likely to acquire communications to which a US person is a party.

- Both bills would eliminate the requirement in 1802(a) that the warrantless electronic surveillance be targeted at means of communications used *exclusively* "between or among" foreign powers and non-US person AFPs.

Thus, the government could collect, without a warrant, any communication between any US person and a foreign power or agent of a foreign power, so long as the government was directing its activity at the foreign power or AFP. Since, as stated above, both bills delete the minimization language prohibiting the use, dissemination, disclosure or retention of US person communications intercepted without a court order, these amendments would allow the interception, indefinite storage and essentially unlimited use of the contents of communications of US persons without a warrant.

Reducing Judicial Oversight By Reducing The Detail In FISA Applications

Both bills would delete some of the information the government is currently required to include in its applications to the FISA court—

- A detailed description of the nature of the information sought and the type of communications or activities to be subject to surveillance;
- A statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance (The Wilson bill would retain the statement about physical entry.);
- Information about previous applications submitted relating to this target; and
- Information on minimization procedures and the number of surveillance devices to be used, if more than one device is expected to be used.

All of this information is useful to the court in determining if the surveillance is reasonable and if the government's minimization procedures are tailored to the type of surveillance for which approval is sought. Without this information, it will be hard for the court to issue an order specifying the scope of permitted surveillance.

Reducing Political Accountability

FISA currently requires that applications require a certification by the President's National Security Advisor or by a Senate confirmed official. Both bills eliminate that and allow the President to designate anyone to make the certification.

Under the Wilson bill, the authority to issue emergency surveillance orders would remain with the Attorney General. The Specter bill, however, would place that authority in the hands of anyone authorized by the President.

Expanding Emergency Taps

The Wilson bill changes the emergency exception by allowing surveillance in an emergency to last for 120 hours (5 days) before an application is made to the FISA court. The current time is 72 hours (up from 24 pre-PATRIOT). The Specter bill would give the government **7 days** to apply for a FISA order.

Expanding Non-Emergency Taps

The Specter bill would allow the FISA court to issue regular FISA orders under Section 105, including for surveillance of US persons, for one year in duration, up from 90 days under current law.

Authorizing Warrantless Surveillance After an Armed Attack and After Terrorist Attacks

The Wilson bill would authorize warrantless electronic surveillance and warrantless physical searches for 2 months after an "armed attack against the territory of the United States." There is no definition of "armed attack against the territory of the United States" and nothing to indicate that the attack must be by a foreign terrorist group. Are US embassies "territory of the United States?" Was the July 4, 2002 attack at the El Al check-in counter at Los Angeles airport, in which a solo gunman killed three people, an armed attack against the territory of the US? How about the attacks of the Washington DC sniper?

The Wilson bill also adds a detailed new section – "Authorization Following a Terrorist Attack Upon the United States" – which would allow warrantless electronic surveillance for 45 days after "a terrorist attack against the United States" as long as the President (1) notifies the congressional intelligence committees and (2) a FISA judge that the US has been "the subject of a terrorist attack" and "identifies the terrorist organizations or affiliates of terrorist organizations believed to be responsible for the terrorist attack."

This warrantless electronic surveillance can continue indefinitely as long as the President submits a certification every 45 days. Warrantless electronic surveillance of US persons under this section is limited to **90 days** unless the president submits a

certification to the congressional intelligence committees that (1) continued surveillance is vital to US national security, (2) describes the circumstances preventing the Attorney General from obtaining an order, (3) describes the reasons to believe that the US person is affiliated with or communicating with the terrorist organization or affiliate, and (4) describes the foreign intelligence information derived.

- The President or an official he designates may conduct warrantless electronic surveillance of a person under this "Terrorist Attack" section only when the President or such official determines that (1) there is a "reasonable belief that such person is communicating with a terrorist organization or an affiliate of a terrorist organization that is reasonably believed to be responsible for the terrorist attack;" (2) "the information obtained…may be foreign intelligence information; and …." [*The section ends there with no number (3)*.]

- Information obtained under this section can be used to obtain a subsequent court order authorizing surveillance.

- The President is required to report to the intelligence committees after 2 weeks and then at 30-day intervals. The report must include (1) a description of each target and (2) the basis for believing that each target is in communication with a terrorist organization or an affiliate of a terrorist organization.

Other Provisions

The Wilson bill would amend Section 1805(i), which provides immunity to electronic communications services for cooperation with the government, to provide immunity if the entity (1) complied with requests for cooperation pursuant to a court order or a request for emergency assistance (for electronic surveillance or physical searches) or (2) "in response to a certification by the Attorney General or [his designee] that … [the surveillance] does not constitute electronic surveillance."

Chairman Specter's Legislation 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 Supposed Core of the Specter Bill, Is Unnecessary

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

First, it is now clear that no legislation is necessary to get the President's program reviewed, since a case is already headed to the Court of Appeals in the Sixth Circuit and probably onward to the Supreme Court, and another case seems likely to be decided on the merits in the Ninth Circuit.

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 Chairman Specter'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 Chairman Specter'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 Chairman Specter's bill applies *only* when it is not possible to specify who is being targeted.

Finally, even assuming that Chairman Specter's bill would allow the FISA court to review the President's program, the 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.

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 Chairman Specter's amendments, merely optional; the repeal of 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 Chairman Specter'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, Chairman Specter'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 Chairman Specter'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, Chairman Specter's bill 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 Chairman Specter's bill, the substitute does not require the Administration to submit the President's warrantless surveillance program or any future program for judicial review.

Chairman Specter'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 8 of Chairman Specter'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."[6]

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

[6] Report of Senate Committee on the Judiciary, Foreign Intelligence Surveillance Act of 1977, S. Rep. No. 95-604, 95th Cong., 1st Sess., at 16.)

> standards tested over time and insulated from the pressures of the moment. . . .[7]

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.

The Specter- Feinstein Bill Takes a More Targeted 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;

---

[7] *Hamdan v. Rumsfeld*, 548 U.S. ___, ___ (2006) (Kennedy, J., concurring).

- 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.

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.[8]

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 Updated

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.[9]

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:

---

[8] FISA as written, while protecting civil liberties, also has problematic provisions, including broad authority for secret searches of Americans' homes, limited opportunity for after-the-fact challenges to surveillance, and broad records seizure authority provided by the PATRIOT Act.

[9] Remarks by the President at Signing of the Patriot Act (Oct. 26, 2001) http://www.whitehouse.gov/news/releases/2001/10/20011026-5.html.

> 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 … .[10]

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.

---

[10] Fact Sheet: USA PATRIOT Act Improvement And Reauthorization Act Of 2005, http://www.lifeandliberty.gov/.

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.

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 Subcommittee, we urge you to look on this as a process that will take some time. Any changes to FISA should be narrowly crafted to meet specific problems identified by the Administration. 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.