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

before the

House Permanent Select Committee on Intelligence

"Modernization of the Foreign Intelligence Surveillance Act"

July 19, 2006

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

Surely, 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 changes in communications and surveillance technology. However, the PATRIOT Act has been modernized already several times since 9/11, and so far there has been no showing by the Administration that it is in need of further amendment.

A number of ideas for major changes to FISA have been offered recently, but they have been conceived or put forth in a vacuum and must be set aside as premature. First let's identify any problems, then draft legislative language. Congress can best identify the specific ways, if any, that FISA should be amended only with further hearings, starting with public testimony by the Administration, and through an iterative process of in-depth analysis (some of it necessarily classified) and public dialogue. Such a process should be open not only to ways in which FISA 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.

---

[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 information privacy and security issues.

If the Administration is encountering a problem with FISA, it should come forth and explain that problem and ask Congress for an amendment tailored to it. If the Administration makes the case in public that FISA is outdated, Congress should be prepared to amend FISA as necessary, consistent with the Fourth Amendment. My organization stands ready to contribute its expertise to that process.

Of course, terrorism poses a grave threat to our nation. To prevent terrorism to the greatest extent possible and to punish it when it occurs, 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 these powers, government surveillance must be subject to executive, legislative and judicial checks and balances.

The Administration Has Offered No Evidence that Any of FISA's Core Principles Need to be Altered

FISA contains five basic principles, each of which is independent from the others, and so far 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.
- 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, the Administration's extreme views of executive power have been rejected twice by the Supreme Court, 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, pending bills – including Cheney-Specter – 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. Administration officials have consistently praised FISA. 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.

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.

A process authorized by Congress and providing for particularized judicial review provides the greatest assurance to those in the government and the private sector who must carry out electronic surveillance that it is lawful and that they can act without fear of criminal and civil penalties. It ensures the public trust and bi-partisan consensus that is so crucial to forging a strong policy to combat the terrorist threat.

Proponents of weakening these protections bear a heavy burden of justification and, so far, there has been none at all on the public record.

The Blind Leading the (Semi-)Blind - Congress Should Not Legislate in the Dark

While CDT welcomes these hearings, and while we are honored to have been asked to testify, most of us in the room today are guessing about whether the government needs any changes, what it has been doing, what is effective, and even how FISA is currently being interpreted and applied. To answer those questions, it is really the Administration that should be here, testifying in public.

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."

So far, the Administration has identified only one problem, relating to the law's requirement that the Attorney General personally certify emergency wiretaps—a problem that could readily be addressed through far less radical means than the sweeping Cheney-Specter legislation and the Wilson legislation

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.

FISA Should Remain The Exclusive Framework For Non-Criminal Government Electronic Surveillance Inside the United States

In 1978, Congress expressly decided that FISA would be the exclusive framework for the government's conduct of electronic surveillance inside the United States. The Senate Judiciary Committee Report on FISA made clear 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."[2]

In his recent opinion in *Hamdan v. Rumsfeld*, Justice Kennedy explained why it is both constitutional and desirable for the Congress and the President to work together to devise and adhere to a consensus set of rules for the exercise of national security powers:

> 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

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

> 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. . . .[3]

FISA's drafters demonstrated that it is possible to craft a statute that is both flexible and comprehensive. They addressed the need for secrecy by providing for a secret court authorized to examine classified information and issue secret wiretap orders. They recognized the need for standards suited to the context of counterterrorism by allowing a judge to issue a warrant on a showing of probable cause that the target of surveillance is a member of a foreign terrorist group, rather than the more stringent criminal standard applicable to law enforcement wiretaps. At a time when the criminal wiretap law still used outdated technology specific language, FISA's drafters used technology neutral language, encompassing all forms of electronic communications. They anticipated the government's need to act quickly to protect national security by providing an emergency exception that allows the government to begin electronic surveillance as long as it files a warrant application with the court within 24 hours. (After 9/11, Congress, at the request of the Administration, extended the emergency period to 72 hours.) And they included a wartime provision that suspends the warrant requirement for 15 days after a declaration of war, giving the President time to come to the Congress if he needed additional authority during a war.

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.[4]

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:

---

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

[4] 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 … .[5]

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.

Technological Changes Improve the Government's Surveillance Capabilities

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 and ISP "is highly flexible, utilizing either passive probes or active software functionality within the network nodes to filter out traffic of interest."[6] Cisco recently released its "Service

---

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

[6] VERINT Systems, Inc., STAR-GATE for Broadband Data and ISP, http://www.verint.com/lawful_interception/gen_ar2a_view.cfm?article_level2_category_id=7&article_level2a_id=59

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 Verisgin 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.[7]

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. [8]

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.

---

[7] http://www.verisign.com/products-services/communications-services/connectivity-and-interoperability-services/calea-compliance/index.html

[8] http://www.epic.org/privacy/carnivore/2003_report.pdf.

The Cheney-Specter Legislation Would Gut FISA and Insulate Domestic Surveillance From Judicial Review

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 probable cause to believe that the target is associated with al Qaeda.

Senator Specter, however, has negotiated with the Vice President a bill that would gut FISA, not only legalizing the President's conduct by repealing FISA's exclusivity provision but also by authorize a program broader than the program the President and Attorney General have described.

Rather than restoring judicial controls, the latest version of Chairman Specter's bill would --

- gut FISA and ratify the Administration's secret violations of the law by repealing FISA's exclusivity provision and making compliance with Act merely optional;
- make it even more difficult for Americans to obtain judicial review of extrajudicial surveillance activities, by allowing the government to transfer any challenges to the Foreign Intelligence Surveillance Court, which operates in secret and ex parte;
- authorize general warrants for electronic surveillance in violation of the Fourth Amendment's requirements of probable cause and particularity; and
- at a crucial time in the war on terrorism, further open intelligence gathering to constitutional uncertainty and legal challenge; and
- curtail congressional oversight.

Section 9 – Repeal of Exclusivity

Section 9 of Cheney-Specter 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 repeal the reforms enacted 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.

Section 9 amends the exclusivity provision of FISA to allow the President to conduct electronic surveillance under Title 18, under FISA *or "under the constitutional authority of the executive*." It thus makes compliance with FISA optional. The bill *allows*, but does not require, the President to seek judicial review of a "surveillance program" lacking in particularity (not the one described by the President and the Attorney General since last December).

This provision would take foreign intelligence gathering out of the solid framework provided by FISA and put it under a constitutional cloud, exposing it to legal challenge whenever the government might seek to use the fruits of the surveillance in arresting or prosecuting terrorists.

Sections 5-6 -- General Warrants

Sections 5 and 6 of Cheney-Specter would authorize (but not require) the Administration to apply for, and the FISA court to grant, "general warrants," which are prohibited by the Fourth Amendment. It thus would authorize surveillance in violation of two key Fourth Amendment requirements: particularity and probable cause.

The surveillance program the bill would authorize is far broader even than the program the President has said is necessary to protect national security. The Attorney General has said that the program targets only communications with particular suspected terrorists, only on the basis of probable cause, and only communications where one party is overseas. Cheney-Specter would authorize seizing the contents of purely domestic calls without probable cause and without particularity, something the Administration has repeatedly said it is not doing. We believe that the use of general warrants for domestic surveillance would be blatantly unconstitutional.

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 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 what 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 for judicial review. So the program need never receive constitutional scrutiny.

Other elements of the wide-scan surveillance program:

- the substitute applies only to surveillance against United States persons (citizens and permanent resident aliens) – it seems to leave unregulated surveillance targeted against non-U.S. persons, yet the Constitution applies to all persons inside the U.S. and FISA has always required a court order for most surveillance of non-U.S. persons inside the U.S.;
- the substitute, 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 the only purpose is the collection of criminal evidence; and
- 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 4 - Privatizing Judicial Oversight While Stacking the Deck

Contrary to press reports, Cheney-Specter would not subject the TSP to judicial review. The bill puts the burden of going forward and the burden of proof on those who think they may have been the subject of illegal surveillance.

If Congress wants to ensure judicial review of the current warrantless surveillance program, it should facilitate challenges by those who were targeted or harmed by the surveillance instead of allowing the President to use his claims of inherent power to avoid ever seeking judicial approval and ever notifying Congress. Furthermore, this bill allows the administration to preclude meaningful judicial review of the warrantless surveillance program in the more than 30 cases already pending, as well as any future cases. It allows the government to divert these cases from courts designed to provide a fair forum for all parties under settled procedural and evidentiary rules to the court that the government believes most favorable to it and to change the rules to make such challenges more difficult. The government should not be allowed to forum shop and change the rules midcourse in Constitutional cases that affect the privacy of millions of Americans. The Cheney-Specter substitute would accomplish the opposite, by allowing the government to transfer any challenges to the FISCR, which operates in secret and ex parte.

Chairman Specter's original bill required the Attorney General to submit the electronic surveillance program to the Foreign Intelligence Surveillance Court for review. Under the original bill, the government would have borne the burden of proving that the program passed Constitutional muster and met the standards prescribed in the bill.

We believed the standards in the original bill were too loose and did not comport with the Fourth Amendment. However, the Cheney-Specter substitute stacks the deck and undermines due process by giving courts the option to dismiss outright any challenges to the legality of electronic surveillance programs. If they do not dismiss the cases, the Cheney-Specter substitute requires courts to transfer them to the Foreign Intelligence Surveillance Court of Review (FISCR) if there is a substantial question whether the communications of one of the parties has been intercepted under the

program. Unlike under Chairman Specter's original bill, where the government would have borne the burden of proof, the parties challenging the program would bear the burden of proving the surveillance was illegal. Proceedings before the FISCR are conducted ex parte and evidence is received in camera, making it virtually impossible for parties challenging the government program to overcome the evidentiary burden they would face as petitioners. Rather than restoring the Constitutional balance of power by ensuring judicial review of government surveillance in the U.S., the Cheney-Specter bill would further insulate the government from accountability for violation of American civil liberties.

Why Do We Need Section 4 Anyhow?

Section 4 of the Cheney-Specter bill purports to authorize judicial challenge to the Administration's electronic surveillance activities outside FISA. Yet more than thirty cases challenging the Administration's warrantless surveillance program are now pending including challenges filed by criminal defendants who may have been targeted. Several federal judges have already heard arguments about the legality of the surveillance. (Many are stayed in order to resolve issues associated with "multi-district litigation.") These cases cover not only the Administration's limited admissions about the program, but also evidence that the Administration, aided by AT&T and likely other telecommunications companies, has been conducting wholesale surveillance on the communications and communications records of millions of Americans for four years.

Indeed, three U.S. district court judges have already considered the Administration's national security arguments, complete with secret evidence: Judge Vaughn Walker in San Francisco; Judge Anna Diggs Taylor in Detroit; and Judge Matthew Kennelly in Chicago.

The Administration will surely use the mandatory transfer provision to move all these challenges to the FISAcourt of review because they believe that that court will be most favorable to them. At the same time the bill would change the procedures applicable to such challenges in ways that favor the government. The government should not be permitted to forum shop in constitutional cases that affect the privacy of millions of Americans, especially where the law and the procedures are then stacked in favor of the government.

Weakening Congressional Oversight

The bill would implicitly amend the National Security Act's requirement—rooted in the doctrine of separation of powers—that the President keep Congress fully informed of all intelligence activities. It *allows* him, if he chooses, to inform Congress about surveillance activities inside the United States, but it also allows the President to use his claims of inherent power to avoid ever notifying Congress.

Section 10 – PATRIOT 3

Section 10 of the Cheney-Specter draft emerged last week and has already changed several times. It is apparently NSA's wishlist. It is very hard to parse, but our initial review reveals:

- the bill makes major changes to FISA's definition of electronic surveillance; a lot of meaning has always been packed into that definition, and it is very hard to tell what would be the impact of the changes;
- the bill defines "Attorney General" to include the AG, the Deputy AG and any person or persons designated by the AG or DAG, thereby allowing anyone designated by the Attorney General to authorize emergency surveillance;
- broadens scope of those who can authorize electronic surveillance in an *emergency*, to include not just the AG but "an official authorized by the President"
- in what may be the most far-reaching provision, amends section 102 of FISA (50 USC 1802) to allow the Attorney General (which would be defined as any person or persons designated by the AG) to carry out warrantless surveillance if it is "solely directed at the acquisition of the communications of a foreign power or agent of a foreign power." That is potentially everything. What FISA surveillance today is not directed at the communications of a foreign power or agent of a foreign power? Is "solely" sufficient to exclude communications of a foreign power when one of the parties on the call is not a AFP? They are still the communications of the AFP.
- narrows the scope of information expressly required to be provided to Congress--to include just (1) a report about minimization, (2) the means and operational procedures of surveillance and (3) "significant decisions" of the FISC. It deletes requirements in an earlier version of the bill that would have required reporting of the number of communications intercepted and the identity (if known) of US persons whose communications were intercepted;
- amends the definition of a non-US person AFP to include someone who "possesses or is expected to transmit or receiving foreign intelligence while in the" US.

The Harman Bill (H.R. 5371) Is 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, and hope that it garners widespread support.

Flake-Schiff - HR 4976, the "NSA Oversight Act"

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.

Conclusion

Mr. Chairman, Members of the Committee, we urge you to look on this a process that will take some care. We should not be reading draft legislative language and guessing what it may mean. 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.