"The Foreign Intelligence Surveillance Act and Effectively Protecting the Liberty and Security of Americans"

Testimony of
Kate Martin and Lisa Graves
Center for National Security Studies
Washington, DC

Before the House Permanent Select Committee on Intelligence
United States House of Representatives
September 18, 2007

On behalf of the Center for National Security Studies and my partner there, Director Kate Martin, I thank Chairman Reyes and the Ranking Member for the privilege of testifying before this Committee today on the Foreign Intelligence Surveillance Act (FISA), effective intelligence and protecting the civil liberties of Americans. We appreciate your scheduling this public hearing so quickly in the aftermath of the temporary revision of FISA that was passed in haste in August.

We believe that the far-reaching changes written into FISA are unconstitutional. They are unnecessary because there are alternatives that would provide additional flexibility to the intelligence community and increase its effectiveness while preserving Americans' constitutional rights, and constitutional checks and balances. Nevertheless, every reasonable alternative—more funding for FISA procedures, streamlining rules for court review, additional time to seek warrants after-the-fact in emergencies, rules to clarify that purely foreign-to-foreign communications that transit the US do not require a warrant, and provisions to allow for the commencement of surveillance before it is known whether Americans' communications will be intercepted—was unreasonably rejected. We hope Congress will reverse course this fall.

The Center for National Security Studies was founded in 1974 to ensure that civil liberties are not eroded in the name of national security, just as Congress began a period of robust oversight of the secret, unchecked intelligence gathering that had violated the rights of hundreds of thousands of Americans. The Center is guided by the conviction that our national security must and can be protected without undermining the fundamental rights of individuals guaranteed by the Bill of Rights. In our work, we begin with the premise that both national security interests and civil liberties protections must be taken seriously and that by doing so, solutions to apparent conflicts can often be found without compromising either.

The Center was called to testify before Congress when FISA was first considered. FISA itself was the product of over two years of legislative drafting and thorough consideration, word by word, to establish clear rules to better protect the rights of Americans and ensure that intelligence gathering was properly focused. Since then, the Center has been asked to testify many times concerning FISA, and we have filed numerous amicus briefs and lawsuits concerning the lawfulness of FISA and related procedures.

We applaud this Committee's insistence on this public debate about FISA and the Protect America Act (PAA). It is essential to the proper functioning of our constitutional democracy, and the complaint that it is harmful is, at its heart, a claim for unreviewed and unchecked presidential power to conduct secret surveillance of Americans.

The PAA amendments authorize unconstitutional surveillance of Americans.

The amendments enacted in August authorize a dramatic increase in secret surveillance of Americans in violation of the Fourth Amendment's requirements for a judicial warrant based on individualized probable cause. As described below, the amendments authorize the NSA and other government agencies to seize massive volumes of telephone and e-mail communications to and from individuals and Americans located in the United States from communications facilities in the United States. The PAA authorizes such seizures without:

- ✓ Any judicial warrant;
- ✓ Any finding of probable cause by any court or even by the Attorney General; or
- ✓ Any requirement that any court or even the Attorney General specify
  - the persons whose communications will be seized,
  - the location of such seizures, or
  - the method or means of such seizures.

Individualized review of such activities by an independent court is the fundamental safeguard for protecting the civil liberties of Americans. The orders the administration has authorized itself to write could well be blanket orders, the kind of "general warrants" the Founding Fathers sought to prevent in the Fourth Amendment, which commands that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

When Congress passed FISA in 1978, it recognized that adherence to these Fourth Amendment requirements is necessary to protect against the kind of abuses that had occurred for many years before then. It specifically required a FISA warrant for the acquisition of electronic communications in the United States of international or domestic communications to or from United States persons. The PAA eliminated this constitutionally required protection in the FISA. Congress should restore those Fourth Amendment protections for individual privacy.

A sea change—broad expansion of warrantless access to Americans' calls and e-mails.

Although the administration initially said it was having difficulty obtaining access to terrorists' foreign-to-foreign communications that transit the US, the PAA authorizes warrantless acquisition of vastly more communications than simply those among foreign terrorists or even other foreign nationals abroad.

It is important to remember that even the surveillance authorized by court order under FISA is an extraordinary and extremely instrusive prower. FISA confers extraordinary authority on the government, namely to wiretap Americans in secret and never notify them that the government has obtained tapes of all their conversations and copies of all their e-mails. Congress approved such authority in 1978, on the stipulation that there would be individualized determinations of probable cause made by a judge before such secret surveillance could be undertaken. When the constitutionality of such secret searches was challenged (by individuals who had been notified of the wiretapping because they had been indicted), FISA was upheld because of the protections it contained. The PAA eliminates many of these constitutionally required safeguards in the FISA.

We fear that the PAA authorizes too much secret surveillance involving Americans and fails to provide the kind of independent, individualized checks that are essential to protect civil liberties. The breadth of the statute's exemptions from FISA's warrant requirements is extremely troubling. While we have respect the professionalism of NSA linguists, analysts, and technicians who work to protect our nation, their jobs are to collect against requirements. And the requirements permitted by the PAA will undoubtedly sweep in increasing numbers of American communications, with no independent protections for their rights. Moreover, history has demonstrated that political leaders will—especially in times of fear such as this period following the tragic attacks of 9/11—unilaterally and secretly read even narrow authorizations broadly.

The broad language appears to authorize some physical searches without warrants.

For example, it is very unclear what effect the PAA has on the Executive's authority to conduct secret physical searches inside the United States. The plain language of the law written by the administration is so broad that it permits the "acquisition" (seizure) of "information" (electronic communications or stored communications) "concerning" (about) a person located outside the US (a person, company, or group). In addition, the PAA contains express language allowing the Executive to unilaterally "extinguish" any "electronic surveillance or physical search" orders of the FISA court that were in effect when the law was passed while giving broad authority to obtain information in secret through searches of stored records.

While it is not clear what such secret searches (whether physical or electronic) might entail—the kind of who, what, where, how and how often or long required by FISA but not the PAA—it seems clear that the intent was to eliminate the requirement for a search warrant in at least some circumstances. The Congress needs a clear understanding of that intent and any court orders extinguished or modified pursuant to the PAA. Certainly no public justification has been offered to eliminate or weaken any of the requirements for physical searches in the US. Assurances aside, the breadth of the language is very troubling.

The PAA sweeps much more broadly than the controversial TSP activities.

We would also note that the PAA authorizes much broader warrantless surveillance of Americans than the surveillance described as the "Terrorist Surveillance Program." There is no requirement that PAA's surveillance involve foreign terrorists and those suspected of conspiring with them. There is not even any requirement that the purpose of such warrantless surveillance be to obtain information related to terrorism. Time and again, the administration deliberately

insisted on broad language over clearer language with defined parameters. The law must be clear and there must be real judicial oversight to protect individual rights—we must be governed by the rule of law, not the whims or even good intentions of political or career appointees.

The PAA appears to authorize access without warrants to all international communications of Americans, whenever the surveillance is "directed at" a person, group, corporation, foreign political party or government outside the US.

We do not believe there is any serious dispute that the administration's intent in the PAA was to allow the warrantless interception of any communication with at least one foreign terminal or leg. But neither terminal is required to be a foreign terrorist. The potential reach is sweeping. It appears to allow the warrantless interception of any communication involving any person located outside the US—a definition that covers roughly potentially millions of people, thousands of corporations, and hundreds of groups—and their communications with any one of 300 million people in the US, including countless corporations and groups, so long as gathering foreign intelligence is the objective.

When confronted with this interpretation, the administration has responded that they could not possibly process *all* international calls and e-mails of Americans, not that they would not have greatly expanded access to them. We have asked whether they will "sit on the wire" monitoring communications flowing through US telephone and internet companies and use technology to acquire and analyze digital calls and e-mails to or from Americans without warrants, and there is no straight answer.1

So, to determine what kind of surveillance is now authorized, the first two sections of the PAA must be read together with the sections of FISA containing the definitions. Section 1 of the PAA exempts from FISA's warrant requirements and other protections any "surveillance directed at a person reasonably believed to be located overseas" by exempting such surveillance from the definition of "electronic surveillance," which is the trigger for FISA's warrant requirements. This change alone does not "clarify" the intent of FISA to exempt foreign to foreign communications even if seized in the United States. Instead, it fundamentally weakens FISA by drastically limiting the requirement to obtain a warrant for "the acquisition . . . of the contents of any wire communication to or from a person in the United States . . . if such acquisition occurs in the United States." The PAA thus eliminates the FISA warrant requirement for international communications by Americans, whenever such acquisition is carried out as part of "surveillance directed at a person reasonably believed to be overseas." This authorization could sweep in millions upon millions of private communications of Americans.

The PAA's exception to the definitions would seem to allow the government to acquire all communications by or from Americans to a group, corporation, or individual overseas, so long as such surveillance is directed at the group, corporation, or overseas individual. There is no limitation on who the overseas target is or how many overseas targets may be selected by the NSA's supercomputers. There is no requirement of any court supervision of such surveillance,

1 It seems the administration believes that answering this question would reveal "sources and methods," but FISA's whole framework for protecting Americans' privacy is about having a public law setting forth clear limits on the "methods" of surveillance of Americans—what type of communications are protected, where, and how.

much less any requirement that if such surveillance acquires significant communications or a significant number of communications by Americans a warrant must be obtained. There is no requirement that anyone outside the NSA even be informed of how many communications by Americans are intercepted, analyzed or retained by the NSA's supercomputers.

The PAA's broad language also appears to authorize warrantless access to the domestic communications of Americans, so long as the government is not intentionally targeting a particular American and is seeking foreign intelligence information about a person abroad.

The plain language of the PAA goes even further than the international communications of Americans. Section 2 provides that if surveillance is directed at a "person" overseas (*i.e.,* is not "electronic surveillance,") the government can compel communications carriers to provide access to their US facilities if the government asserts, without any oversight, that the purpose is to acquire "foreign intelligence information concerning persons reasonably believed to be outside the US." There is no doubt that communications between two Americans in the U.S. could well contain foreign intelligence information concerning groups or corporations or governments overseas, which group, corporation or government may be the entity at which the government is directing its surveillance. Thus, the executive branch could authorize the interception or other acquisition of such domestic communications containing foreign intelligence, unless some other provision of the FISA prohibits such acquisition.2

While the administration carefully dodges these issues by referring to FISA's protections for domestic communications, the interplay between FISA and the PAA's new regime is such that the government could now acquire such domestic communications, so long as the government is not "intentionally targeting" "a particular known United States person who is in the United States." Thus, so long as the NSA is engaging in a broad, non-targeted surveillance program, it can acquire the domestic as well as the international communications of Americans in the US.

This is perhaps most easily seen by using a hypothetical example. The PAA can be read to authorize the acquisition of foreign intelligence information concerning the political leadership in India.3 They can do so by directing the NSA to program its device for intercepting and analyzing communications at US facilities to select out and copy for the NSA all calls to or from a list of phone numbers belonging to the leaders of the major political parties in India, which would include all calls to or from Americans in the US, and the same for e-mail communications. Such acquisition appears to meet the requirements of subsection (a) of section 2 of the PAA.

But the administration could authorize much more. They could direct the NSA to program its interception and selection devices so that the NSA obtains all subsequent communications for some period of time by anyone who contacts or is contacted by any of the initial numbers or e-mails in India. Having thus acquired these communications, the NSA supercomputers can then search such communications for information concerning the Indian political parties, either by using search terms to scan the content or by determining whether such subsequent

---

2 This point has been raised by former Justice Department official David Kris. *See* Slate.com.

3 Such parties come within FISA's definition of "foreign power" and information about such parties can be said to relate to the conduct of the foreign affairs of the US as well as in all likelihood the security of the US and therefore constitutes foreign intelligence information under FISA.

communications were with individuals who might also communicate about those political parties. The only actual numbers or e-mail addresses plugged into the acquisition/selection device would be the original phone numbers or e-mails in India—the other directions simply consist of an algorithm directing the acquisition of the subsequent communications by individuals in contact with Indian leaders. Those subsequent communications could include contacts by Americans with other Americans.

We are very concerned that there may be nothing in FISA as amended by the PAA that would prohibit this and it seems clearly authorized by the legislation. It meets all the requirements: it is acquisition of foreign intelligence information about "persons" located outside the United States; it does not constitute "electronic surveillance" because it is surveillance directed at foreign political parties and it is not acquiring the content of any communication by a "particular known United States person who is in the United States" "by intentionally targeting that United States person." Quite to the contrary, not only are particular known Americans not being intentionally targeted, but when the surveillance begins, the NSA does not even know whether its algorithm will acquire any communications by any Americans. Thus, the essence of the PAA is to allow the NSA broad access to Americans' communications so long as it is done as part of an effort to collect foreign intelligence information concerning overseas persons, groups, corporations, or foreign political parties or governments.

Under the PAA's regime there is no independent check to monitor the deployment of computer sorting methods by NSA systems that may well be a permanent presence on the global telecommunications infrastructure in the US. There is no system for guarding the guardians exploiting new access to the global communications of Americans.

While we have seen repeated statements by administration officials attempting to dodge this issue, we have seen nothing categorically denying that the PAA would permit this. When confronted with this interpretation, the administration has not flatly denied it; their responses have been carefully drafted to the effect that they will continue to comply with the FISA's requirements for domestic surveillance. But those requirements have been changed, so that warrants are only required in much more narrow circumstances than before, such as the intentional targeting of a particular known US person.

The PAA paradox means that more collection results in less protection for more Americans.

The PAA changes seem to create a paradox that the less targeted the NSA is, the greater the number of communications it can obtain. The targeting language of FISA that was supposed to be a shield for privacy rights has been transformed into a sword. By not targeting particular Americans the NSA gains the power to obtain many more communications of Americans than ever before.

The PAA does not "restore" FISA authorization to monitor Americans here because there never was such authorization.

One of the administration's main assertions is that the PAA merely restores the "original intent" of FISA, by restricting the application of the warrant requirement. Their claim is that Congress

did not intend to require a warrant for international calls unless the government was "targeting" an American. This incorrect claim is followed by the false claim that back in 1978 all international communications came within the "radio exception" because they were carried by satellite (and thus accessible to NSA receivers) and all domestic communications were carried by "wire" (and thus inaccessible to NSA "ears") and that now the situation is reversed. These claims are wrong.

It is not correct to say that changes in technology have deprived the NSA of access to Americans' international communications that it was previously entitled to. To the contrary, FISA was intended to prohibit precisely the kind of NSA activity that now seems to be authorized by the PAA, the mass interception of international communications by Americans off the wires in the US.

The administration's description of the previous status quo is simply inaccurate as a matter of historical record. In 1978, it was already known that many and maybe most international communications of Americans traveled into and out of the country by wire, such as through the newer transatlantic cables that were laid in 1978.4 And Congress specifically protected international communications traveling by cables in the US from interception without a warrant.5 The legislative history specifically states that those international wire communications are covered by FISA if the acquisition of the contents of the communication occurs from the wire in the US, a requirement that was also explicit in the text of FISA, 50 U.S.C. 1801(f)(2). The use of transatlantic and transpacific cables to transmit Americans' communications was hardly unforeseen. Ten years after FISA was passed these metal cables were replaced by fiber optic ones. In the intervening twenty years the government did not claim a right to access Americans' communications on those cables without warrants, but now it does.

Moreover, FISA was enacted precisely to prevent NSA programs for the wholesale acquisition of Americans' international communications. FISA was enacted after the revelations about Operation Shamrock—an operation where the NSA had obtained copies of almost all international telegrams of Americans. The Congress and the NSA agreed that such programs should end and that agreement was reflected in FISA.

The administration's retroactive reading of FISA is inconsistent with that agreement. Its reading would have allowed the NSA to simply move Operation Shamrock to satellite interception. But the NSA at the time assured Congress that it rarely intercepted American communications. For example, in 1975 NSA Director Lew Allen promised Congress that the NSA was only targeting foreign communications channels, which carried only a minuscule number of international communications by Americans. *See* Letter from General Lew Allen to Chairman Pike, August

---

4 It is also not true that purely domestic calls traveled only by wire—most long distance interstate calls were transmitted in part by radio towers. Because radio communications, now called "wireless" communications, between Americans could be accidentally intercepted through monitoring of the airwaves, Congress forbade "intentional" interception and was assured that communications accidentally or unintentionally intercepted would be "immediately destroyed."

5 *See* S.Rep. No. 94-1035, 94th Cong., 2d Sess. 28 (1976); S.Rep.No. 94-1161, 94th Cong., 2d Sess. 26 (1976). Congress intentionally barred the tapping of wire communications without a warrant for "either a wholly domestic telephone call or an international call . . . if the acquisition of the content of the call takes place in this country . . . ." S. Rep. 95-604, at p. 3934 (1978).

25, 1975, confirming that the NSA was not "monitoring any telephone circuits terminating in the US." It was on the basis of such assurances that FISA's prescriptions for wiretapping were written.

In summary, the so-called radio exception was never meant to bless the deliberate, wholesale interception of channels carrying Americans' communications by the NSA without a warrant. FISA was based on agreement that the NSA was properly focused on foreigners overseas, not on Americans' communications. Amending FISA now to exempt from the warrant requirement any surveillance concerning a person or entity overseas and all their communications with Americans does not restore the status quo from 1978, it rolls back the clock to the era of Operation Shamrock. Such sweeping changes are a significant step towards adopting the viewpoint of those in the Justice Department and the White House that FISA and its procedures for judicial review unconstitutionally impinge on presidential power. The changes passed in August overturn the congressional/executive branch agreement of the past 30 years that giving the President such authority is unnecessary, unconstitutional and dangerous.

Changes in government surveillance technologies and increased contacts between Americans and the world require greater, not fewer privacy protections.

If allowed to stand, this law marks a fundamental change in the scope of surveillance operations of Americans' communications. For the first time, Congress will have authorized the NSA to turn its extraordinary technical surveillance capabilities, inward—to intercept Americans in the United States, rather than events overseas. The NSA, with its vast resources and technological capabilities, conducts surveillance on a massive scale and the PAA eliminates any requirement of targeted individualized surveillance based on a court's finding of probable cause. (While FISA did not bar the NSA's monitoring of international radio signals that might result in some incidental unintentional reception of Americans communications, the overall intent was to prevent the NSA from monitoring Americans or channels of communications of Americans.6)

The administration has argued that changes in technology merit more power with fewer checks. While it is true that the intelligence community needs the capability to track down terrorists using modern communications technologies, there has been no demonstration that the most effective way to do this is to give the community carte blanche to surveil the communications of millions instead of requiring the kind of predicated and focused surveillance that would both protect Americans' privacy and make it more likely that intelligence efforts are focused on the right targets.

At the same time that vast increases in the power and range of surveillance technologies give the government greatly expanded powers to intercept and analyze communications, Americans are committing more and more of their private thoughts and communications to electronic form. And globalization has meant an exponential increase in international contacts by Americans—over 40 million Americans travel out of the country each year, for vacations, jobs, missionary work, health care or adoptions; almost half a million Americans serve in the military

---

6 The radio exception "should not be viewed as congressional authorization of these activities" and Congress took pains to emphasize that "broadscale electronic surveillance" even of Americans who were abroad had been limited by the Executive. S. Rep. 95-604, at p. 3936 (1978).

or work overseas for the government; a couple million more live overseas; and about a quarter-million Americans study abroad every year. These Americans stay in closer contact with friends and family at home than ever before. In addition, more Americans work for or deal with foreign-owned companies than ever before in history, from J.C. Penney's to Dr. Pepper, and with outsourcing even contacts with American-owned companies can involve communication with foreign nationals. Americans routinely deal with many companies owned by foreign governments, which may come within FISA's definition of "foreign power." Plus, fully 80 percent of US ports are controlled by foreign-owned companies, including Chinese and Venezuelan companies.

This globalization calls for increased protections for the communications of Americans, wherever they may be communicating. Flexible judicial review is important for protecting Americans' privacy and freedom of speech and association by preventing the accumulation of massive databases storing Americans' private communications, even if those communications are not immediately disseminated.

After the fact "minimization" is insufficient to protect the constitutional interests at stake. As Senator Sam Ervin observed:

> [D]espite our reverence for the constitutional principles of limited Government and freedom of the individual, Government is in danger of tilting the scales against those concepts by means of its information gathering tactics and its technical capacity to store and distribute information. When this quite natural tendency of Government to acquire and keep and share information about citizens is enhanced by computer technology and when it is subjected to the unrestrained motives of countless political administrators, the resulting threat to individual privacy makes it necessary for Congress to reaffirm the principle of limited, responsive Government on behalf of freedom.
> …
> Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom. For the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets, we stand naked before official power. Stripped of our privacy, we lose our rights and privileges. The Bill of Rights then becomes just so many words.7

The warrantless surveillance of previously protected American communications which appears to be authorized by the PAA epitomizes these dangers, given its reach into people's private lives without even any suspicion, much less probable cause that they are doing anything wrong.

The PAA eliminated other important protections.

In addition to the concerns addressed above, the PAA eliminates other key safeguards in FISA. It appears to:

---

7 Senator Ervin,June 11, 1974, *reprinted in* COMMITTEE ON GOVERNMENT OPERATIONS, UNITED STATES SENATE AND THE COMMITTEE ON GOVERNMENT OPERATIONS, HOUSE OF REPRESENTATIVES, LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974 S.3418, at 157 (Public Law 93-579)(Sept. 1976)

- Allow warrantless secret searches of Americans' communications without even any after the fact meaningful oversight. As outlined above, the Act allows the interception and surveillance of Americans' domestic and international communications with no prior judicial authorization, no individualized determination of probable cause and no specification of which individuals or phone lines are to surveilled;
- Eliminate the requirement of fair notice to individuals that they have been overheard when they are indicted;
- Allow government access to stored communication records with no court orders or judicial oversight; and
- Allow the government to secretly obtain the call record information and other revealing meta-data on thousands or millions of Americans' communications with no judicial oversight, to conduct traffic analysis and construct maps of the associations and contacts of untold numbers of innocent Americans.

This recital may well be incomplete. As has been pointed out by others, there is no legislative record explaining either the understanding of the administration or the intent of Congress in enacting these amendments.

In addition to seeking to make these changes permanent (with only minor clarifications) the administration is seeking additional changes to the law. We strongly oppose these changes to FISA.

We believe there is no need to provide retroactive immunity to the carriers at this time or provide for substitution of the government. Doing so would eliminate a crucial check on government abuses. We oppose amnesty for companies as well as government actors, as called for by the administration's 2006 Statement of Administration Position on the Wilson bill.

In addition, we are very concerned that the administration may have already implemented by regulation, a proposal contained in its prior draft: namely that a warrant is only required for Americans' domestic communications if the government has reason to believe the sender and all recipients are in the US. That is, if the NSA does not know where you and all the recipients to your e-mails are at any given moment the government's position may be that no warrant is required. We have asked for the administration's assurances that they have not adopted such an unconstitutional presumption, but received none. The rhetoric of administration officials only underscores our deep concerns about the privacy of Americans' internet communications.

What is to be done?

As noted above, the PAA is unconstitutional and should not be made permanent. Neither Congress nor the American public has enough information yet to determine whether amendments are warranted nor what they should be. Without such information, it will be very difficult to draft changes that would prevent future violations of the law.

As outlined in the testimony of Dr. Morton Halperin before the House Judiciary Committee, the administration has not provided adequate information to show that amendments are needed. Their refusal to disclose information, varying public explanations, political posturing, and

selective disclosure of claimed classified information makes it impossible for the Congress to take them at their word, even if doing so were consistent with your constitutional responsibility.

We believe Congress should start by:

- Obtaining information about past surveillance activities in violation of the law;
- Ensuring adequate public disclosure about those activities; and
- Obtaining a binding public explanation of the administration's interpretation of each provision in the PAA.

This information alone is not enough. It is essential though because, as this committee knows well, the administration's rationale for why amendments to FISA are needed has shifted over time.

For example, while much of the administration's public rhetoric focused on the problem of having to obtain FISA warrants to intercept communications between two foreign terminals passing through switches in the United States, on occasion, they have admitted that such warrants have never been required by FISA. Moreover, the administration apparently also claims that the FISA requirement for warrants and court oversight should be eliminated because they cannot always tell where the parties to a communication are located. While this may be true some of the time or for brief periods, it is not true of the majority of Americans' communications. For example, many experts agree that it is relatively easy and quick to determine where the parties to any telephone call are located. The locations of parties to an e-mail may be more difficult to determine in some situations. But the administration has never offered a justification, nor do we believe there is one, for amending the FISA to eliminate the warrant requirement for all those international communications where it is reasonably likely that one end of the communication *is* located inside the U.S. And of course this problem provides no justification for allowing warrantless interception of domestic communications. Nevertheless, the PAA eliminated fundamental protections in FISA and appears to authorize the warrantless acquisition of many international and some domestic communications by persons *known* to be in the US, so long as the government's purpose is to collect information about a person believed to be overseas.

These and other potential issues cannot be adequately judged on the current record, because the administration has refused to disclose even a redacted version of the opinions by the FISA court and the legal arguments made by the government to the court. (We do not believe that the legal analysis – separate from identification of the surveillance targets – is properly classified. We have filed a Freedom of Information Act request for redacted versions of the courts' opinions and the legal arguments made by the government.)

Only after disclosure of all this information, can Congress consider whether permanent legislation is needed and what it should be. In addition, we believe the following general principles must be adhered to in considering any amendments to the FISA:

- The structure of FISA must be maintained;

- Surveillance must be carried out within the FISA structure—there should not be any change to the definition of electronic surveillance;
- Carriers must have the responsibility of sorting communications and insuring that the NSA is only given access to that which they are entitled to. Initial court authorization of surveillance in the US at US switches must be required;
- When the government intentionally acquires the communications of persons in the US, it must have a warrant to do so, which may authorize interception of the communications of either party to the call or e-mail;
- Acquisition of the increasing number of communications of US persons located overseas must comply with Fourth Amendment requirements;
- There may be limited exceptions for true emergencies, or when beginning surveillance of an individual target located overseas and it is not known whether the target will communicate with persons in the US; and
- Meaningful, mandatory and frequent reports to courts and Congress along with an IG audit must be required.

The draft bill crafted by Chairman Reyes and Chairman Rockefeller, described in the latter's August 1, 2007 news release appears to have incorporated many of these needed principles, but further public hearings on publicly available language would be essential to fully assess any such proposal.

Thank you again for considering our views.