Testimony of

Suzanne E. Spaulding

September 25, 2007

Hearing of the
United States Senate
Committee on the Judiciary
Strengthening FISA:
Does the Protect America Act
Protect Americans' Civil Liberties and Enhance Security?
Tuesday, September 25, 2007
Testimony of Suzanne E. Spaulding

Hearing of the
United States Senate
Committee on the Judiciary
Strengthening FISA: Does the Protect America Act
Protect Americans' Civil Liberties and Enhance Security?
Tuesday, September 25, 2007
Testimony of Suzanne E. Spaulding

Chairman Leahy, Ranking Member Specter, Members of the Committee, thank you for this opportunity to testify on changes to the Foreign Intelligence Surveillance Act (FISA). In the twenty years that I spent working on efforts to combat terrorism, at the Central Intelligence Agency, at both the House and Senate intelligence oversight committees, and as Executive Director of two different commissions, on terrorism and weapons of mass destruction, I developed a strong sense of the seriousness of the national security challenges that we face and deep respect for the men and women in our national security agencies who work so hard to keep our nation safe.

We owe it to those professionals to ensure that they have the tools they need to do their job; tools that reflect the ways in which advances in technology have changed both the nature of the threat and our capacity to meet it. Equally important, they deserve to have clear guidance on just what it is that we want them to do on our behalf -- and how we want them to do it. Clear rules and careful oversight provide essential protections for those on the front lines of our national security efforts. Unfortunately, the newly enacted changes to the Foreign Intelligence Surveillance Act (FISA) provide neither clear guidance nor the mechanisms to ensure careful oversight.

Problems with the Protect America Act of 2007
Changing the Definition of Electronic Surveillance.

First, I would urge Congress to avoid trying to accomplish objectives by changing definitions. The terms in FISA not only appear throughout this complex statute; they are also referenced in or inform other laws, Executive Orders, directives, policies, etc. The risk of unintended consequences is significant, particularly when changing the definition of something a fundamental as electronic surveillance. The report recently prepared by the Congressional Research Service points out several ways in which defining a range of activity out of electronic surveillance (section 105A), while still setting up a potential process to authorize those activities within this statute designed to regulate electronic surveillance (section 105B), creates confusion. This does not even address the consequences for internal NSA directives and other legal and policy documents that reference electronic surveillance.

Most importantly, as Ken Wainstein noted in his testimony before the House Judiciary Committee on September 18, 2007, the definition of the statutory term electronic surveillance "is sort of the gatekeeper term in the statute that identifies those government activities that fall within the scope of the statute and, by implication, those that fall outside

the scope of the statute." By defining out of FISA the acquisition of any communication when it is directed at someone reasonably believed to be outside the United States, you remove any statutory protection that FISA might otherwise provide for Americans whose communications might fall into this category.

None of the FISA provisions apply to intercepts defined out of FISA by section 105A. There is no statutory minimization requirement, no court review of any procedures before or after the fact, no reporting requirements. These intercepts are not covered by FISA at all. There may be Executive Orders, directives, or other internal policies that call for minimization of even these intercepts, but those can be changed unilaterally at any time by the Executive Branch.

What about the requirements and safeguards in 105B? This section is an optional process that the Attorney General and the DNI "may" use if they require the assistance of a third party and need to compel that assistance. Some telecommunication providers, for example, may demand some sort of express legal authorization before they will help the government access communications inside the United States. In fact, prior to the talk of granting full retroactive immunity to carriers who helped with surveillance outside of FISA, I would have thought all telecom providers would have insisted on written assurances about the legal authority under which the government would be accessing their customers' communications. However, if companies can expect the government to protect them regardless, they may be more willing to help without regard to the law--in which case the government would not need to use the optional procedures and safeguards in 105B.

Notwithstanding Any Other Law.

Second, avoid using the words "notwithstanding any other law." This is how the new section 105B begins and these words should always raise a red flag. In this case, it raises serious questions about the continuing applicability of other laws that regulate the collection of intelligence inside the United States, including restrictions within FISA with regard to physical searches. If there are particular provisions of law that Congress wishes to ensure do not hamper the collection of this intelligence inside the US, they should specify those provisions and be clear about how they will and will not apply.
Section 105B provides authority for the AG and DNI to collect intelligence information inside the United States so long as (1) the information is about a person who happens to be outside the US at the time--including, of course, a US citizen, (2) the collection of that information does not involve electronic surveillance, and (3) the government requires the assistance of someone with access to a communication or communication equipment. It appears to be about electronic surveillance targeting someone outside the US (which is now no long considered "electronic surveillance"), but it in fact provides authorization for the government to gather any kind of communication and to gather it inside the United States. Thus, it would appear to authorize intercepting US mail between two people inside the United States, so long as the government reasonably believes the letter discusses, at least in part, someone outside the US. The careful legal regime governing mail intercepts is overruled by the "notwithstanding any other law" language" in section 105B.

Moreover, it would appear that the AG could authorize the physical search of your home to find a letter from your son overseas or the family computer on which you've stored his emails, although this would raise significant 4th Amendment issues. The FISA provisions that regulate physical searches become irrelevant because section 105B applies "notwithstanding any other law."

Similarly, the protections that Congress worked so hard to enact last year for section 215, the so-called business records provision, would also appear to be overruled under circumstances in which Section 105B applies. Thus, any individual who can help the government obtain access to communications that involve someone outside the United States can now be compelled to provide that assistance under section 105B, with fewer safeguards.

And it is not just other sections of FISA that are effectively repealed by this language. It appears to overrule any laws that might otherwise affect the gathering of information about communications that concern people outside the US. Thus, whatever privacy protections Congress may have enacted in other laws, including the Electronic Communications Privacy Act, would no longer have any impact on this activity.

The Administration has indicated that it did not intend for the law to have such broad implications and is willing to work with Congress to clarify the statutory language. I urge Congress to take them up on this offer and ensure that the law is narrowly drafted to fix only specific problems clearly identified and justified by the intelligence community.

Not Limited to Terrorism.

Despite this new law having been explained to the American public as necessary to protect them from the next terrorist attack, none of the intelligence collection it authorizes has to be related in any way to terrorism. It applies to any "foreign intelligence," a term which has been amended over the years to include a very broad range of information.

Inadequate Minimization.

It is true that information gathered under 105B must be subjected to minimization procedures, but it appears that the statutory requirements that apply are the less rigorous procedures that apply when a FISA judge has reviewed a full FISA application and found probable cause to believe that the target of the surveillance was a foreign power or agent of a foreign power.

The Protect Act simply refers to "the minimization procedures in section 101(h)." There are two sets of minimization procedures proscribed in that section. The first set applies when a FISA judge has approved an application. The second set is much more stringent and applies when the Attorney General has approved surveillance without going to a FISA judge. These more rigorous procedures are statutorily limited to situations in which the AG is acting pursuant to the authority granted him in section 102(a). Thus, they would not apply to the unilateral authority granted to the AG and DNI in the Protect Act.

The general minimization procedures in 101(h)(1)-(3) reflect a recognition that, even after all the application requirements had been met and approved by a FISA judge, there remains some risk that information about U.S. persons (USPs) might be collected. These procedures require steps be taken to minimize the acquisition and retention, and prohibit the dissemination, of such information. However, the procedures are to be "reasonably designed in light of the purpose and technique" of the surveillance and "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." This is a very broad and flexible standard, particularly given the current scope of "foreign intelligence."

Under section 101(h)(4), if surveillance is conducted pursuant to AG authorization rather than a warrant from a FISA judge--a situation more analogous to the 105B authority-- no contents of any communication to which a USP is a party can be disclosed, disseminated, or used for any purpose or retained for more than 72 hours without getting a court order, unless the AG determines that the information indicates a threat of death or serious bodily harm. Concern about ensuring that electronic surveillance authorized unilaterally by the AG could not be used to gather information about USPs was so strong when FISA was enacted that even the mere existence of such a communication was included in this restriction. At a minimum, this stricter procedure should apply to information collected under section 105B.

Require Proactive Efforts to Identify Parties' Locations.

The Protect Act requires that the AG and DNI develop procedures to reasonably ensure that the target is outside the US (or the information concerns someone outside the US and is not "electronic surveillance") but the Act does not provide any other requirements for those procedures.

The government should have a proactive obligation to take whatever steps are feasible, on an ongoing basis rather than just at the outset of surveillance or other intelligence collection, to determine whether the target is in fact overseas and whether the other party to a communication is inside the United States. The phone company always seems to be able to determine whether I am using my cell phone at home or overseas--I know this because they charge me a lot more when I use it overseas! There ought to be a way for the government to know, even if it is after the fact, where the parties to many of these communications are located. This begins to provide the basis for a legal regime that is much more narrowly focused, with precise procedures and safeguards to govern surveillance that involves persons inside the United States.

Ensure Independent Oversight.

Rigorous oversight of the use of this authority will be essential. The Administration has promised that it will provide such oversight and provide reporting to Congress, which is important and reassuring. However, given the reported failure of the Attorney General to properly report to Congress regarding problems with the use of national security letters, I would urge Congress to direct, in statute, that the Justice Department and DNI Inspectors General report jointly on implementation within 90 days of enactment and every 90 days thereafter.

Context for FISA Changes

The Administration has indicated that it plans to seek broader changes to FISA. As the committee and the Congress consider how to move forward on this issue, I would offer some overarching thoughts on the challenge presented by the national security imperative to monitor communications of those who wish to do us harm.

First, any expansion of authority should be limited to terrorism targets. This is how the authority is sold to the American public by the Administration. To then broaden the authority to include any and all foreign intelligence on any topic is a kind of "bait and switch."

Second, craft the narrowest changes possible to remove whatever impediment has arisen to using FISA. Technology experts and FISA judges, current and former, can provide essential insights into what the government and the communications providers can and cannot do, as well as what safeguards are most important to prevent abuse.

Third, be extremely cautious about limiting the role of the FISA judges. As Supreme Court Justice Powell wrote for the majority in the Keith case, "The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility are to enforce the laws, to investigate, and to prosecute. ...But those charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks. The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech."

Finally, Congress should seek a stronger commitment from the Administration that it will actually abide by the law. As noted earlier, the new procedures under section 105B are optional; the AG and DNI "may" choose to use them but they are not required to follow this process. However, the rest of FISA is not optional. Until Congress gets some assurance from the Executive Branch about where they draw the line on Presidential authority in this area, it is hard to see why Members should continue to work so hard to craft careful laws.

On a related point, the Administration has indicated that it will be back in front of Congress seeking immunity for carriers and others who cooperated in the Terrorist Surveillance Program and, perhaps, other intelligence activities. It is hard to imagine a more powerful way to undermine respect for the rule of law and the critical role that communication providers play as the last line of defense against government abuse. Moreover, it's not clear why this is needed. Under current law, communication providers already can avoid liability if they simply have a letter from the AG saying the government's request is legal. If they did not even get that, what message do we send by giving them immunity for totally disregarding the law? Why wouldn't the next telecommunications CEO decide to go ahead and ignore the legal requirements, figuring the government would bail the company out if it ever became public?

In an area such as this, where the normal safeguards of transparency are lacking, requiring communication providers to at least get a certification that the request to hand over customer information or allow communication intercepts is legal serves as an important potential deterrent to abusive behavior by the government. At a minimum, Congress needs to fully understand what past activities would be immunized before adopting such a wide-ranging provision.

Undertake a Broader Review of Domestic Intelligence Collection

FISA is the primary statute governing domestic intelligence collection. Rather than attempt to guess at what might really be needed to meet today's challenges and how these and other changes will affect our ability to meet those challenges and protect Americans' privacy, Congress should take the time to ensure they understand the full context in which these changes are being sought. This includes the problems that have prompted them, particularly as these relate to current and past intelligence activities and the changing nature of the threat, as well as how these new

authorities, definitions, and procedures would relate to all of the other national security and law enforcement tools available to the government.

I urge Congress not to consider any "overhaul" of FISA without first undertaking a comprehensive review of domestic intelligence collection. The attacks of 9/11 revealed a vulnerability at home that led to a dramatic increase in domestic intelligence activity. The Federal Bureau of Investigation's priorities turned 180 degrees, as it was pressed to place domestic intelligence collection at the forefront rather than criminal law enforcement. But the FBI is not the only entity engaged in domestic intelligence. The Central Intelligence Agency, National Security Agency, Department of Defense, Department of Homeland Security, and state and local law enforcement are among the many entities gathering intelligence inside the US. The threat to the homeland presents unique challenges, both to effective intelligence and to appropriate protections against unwarranted government intrusion.

Unfortunately, the legal framework governing this intelligence activity has come to resemble a Rube Goldberg contraption rather than the coherent foundation we expect and need from our laws. The rules that govern domestic intelligence collection are scattered throughout the US Code and a multitude of internal agency policies, guidelines, and directives, developed piecemeal over time, often adopted quickly in response to scandal or crisis and sometimes in secret.

Rather than continuing this pattern, the House of Representatives should consider establishing a Joint Inquiry or Task Force with representation from the most relevant committees (Intelligence, Judiciary, Armed Services, Foreign Affairs, and Homeland Security), to carefully examine the nature of the threat inside the US and the most effective strategies for countering it. Then this task force, the entire Congress, and the American public, can consider whether we have the appropriate institutional and legal framework for ensuring that we have the intelligence necessary to implement those strategies, with adequate safeguards and oversight.

The various authorities for gathering information inside the United States, including the authorities in FISA, need to be considered and understood in relation to each other, not in isolation. For example, as discussed earlier, Congress needs to understand how broader FISA authority relates to the various current authorities for obtaining or reviewing records, such as national security letters, section 215 of FISA, and the physical search pen register/trap and trace authorities in FISA, and the counterparts to these in the criminal context, as well as other law enforcement tools such as grand juries and material witness statutes.

Executive Order 12333, echoed in FISA, calls for using the "least intrusive collection techniques feasible." The appropriateness of using electronic surveillance or other intrusive techniques to gather the communications of Americans should be considered in light of other, less intrusive techniques that might be available to establish, for example, whether a phone number belongs to a suspected terrorist or the pizza delivery shop. It's not the "all or nothing" proposition often portrayed in some of the debates.

Congress should undertake this comprehensive consideration of domestic intelligence with an eye toward the future but informed by the past and present. Until Congress fully understands precisely what has and is being done in terms of the collection and exploitation of intelligence related to activities inside the US, by all national security agencies, it cannot wisely anticipate the needs and potential problems going forward.
This applies particularly to changes to FISA. Congress must be certain that it has been fully informed about the details of the Terrorist Surveillance Program and any other surveillance programs or activities initiated after 9/11, not just in their current form but in the very earliest stages, including the legal justifications offered at the time the activities were initiated. Understanding how the law operates in times of crisis and stress is key to understanding how it might need to be strengthened or adjusted to meet national security imperatives in ways that will protect against future abuse.
Conducting this kind of careful and thorough oversight is particularly challenging in today's environment, as we saw with the rush to enact the Protect Act just before the August recess. Congress' ability to insist that the expansion of authority be appropriately limited and safeguarded was significantly hampered by concerns that the American public would view Members as "soft" on national security.

Reshape discussions about how best to address the terrorist threat

Effective oversight and thoughtful legislation will require reshaping the discussion about how to best address the long term threat of terrorism. We need a broader discussion about the ways in which policies that mock the rule of law and undermine our carefully constructed system of checks and balances make it more likely, rather than less likely, that we will be attacked again.

Military and civilian experts agree that the long-term threat from international terrorism is not going to be defeated militarily. In addition to eliminating the terrorists' leadership, it is at least equally essential to reduce their ability to recruit new young people to join their "cause" and to generate and maintain support within communities around the world. This is a struggle for hearts and minds; a competition of narratives. The "jihadist" narrative is undeniably compelling to many young Muslim men--and we unfortunately strengthen this narrative when we speak in terms of a Global War on Terrorism. The narrative of democracy, individual freedoms, and the rule of law can be equally compelling but its credibility is dramatically undermined if the greatest democracy is not clearly committed to living that narrative rather than simply mouthing the words.

We have to demonstrate that we still believe what our founders understood; that this system of checks and balances and respect for civil liberties is not a luxury of peace and tranquility but was created in a time of great peril as the best hope for keeping this nation strong and resilient. It was a system developed not by fuzzy-headed idealists but by individuals who had just fought a war and who knew that they faced an uncertain and dangerous time. They saw first-hand the how the whims of a single, unchecked ruler could lead a country astray. They knew that in times of fear and crisis, the instinct is to reach for power--and they determined that balancing power between all three branches would protect against that frailty of human nature and ultimately make for wiser, better decisions and a more unified and strong nation.

Our greatest weapon against global terrorism is a committed and determined American public. Public support is strengthened by developing consensus through public discussion and debate-not by developing policies in secret or by stifling dissent by labeling those who disagree as "unpatriotic" or insufficiently aware of the post 9/11 threat. Statements claiming that Congressional debate over proposed FISA changes costs American lives are not only suspect in terms of credibility, they also reflect a fundamental failure to appreciate the strength of our democracy.

The wisdom of this system and the importance of remaining true to it even in times of peril can perhaps best be understood with regard to fears of home-grown terrorism. The best hope for detecting and preventing this threat lies not in intrusive intelligence methods, which are better suited to monitoring a known target than in finding out who might be a target. Instead, our best hope lies in working closely with communities, particularly Muslim American communities. Yet, many of our policies and practices since 9/11 that unnecessarily compromise civil liberties or seem to reflect a lack of respect for the rule of law risk alienating those very communities. In this regard, they make us less secure.

It is also clear that the failure of the Administration to follow the law or take advantage of our system of checks and balances in its implementation of the Terrorist Surveillance Program, and other related intelligence activities, had significant negative consequences for our national security. The Administration tells us that these surveillance activities were, and are, vital to our security. Yet here are some of the consequences of the failure to build a firm legal foundation for these programs:

* The program was shut down for weeks: The shaky legal ground for surveillance activities apparently caused sufficient concern by the Acting Attorney General and the FBI Director that the program was reportedly shut down for weeks until more safeguards were added. A firmer legal footing, based on a stronger consensus, would have avoided this potentially dangerous gap in coverage.
* The program was leaked to the press, something the Administration claims has hurt our national security. We do not know who may have provided reporters with information about the program, but there were reports that some information may have been provided by professionals at NSA or DoJ who were extremely troubled by what they believed was an illegal program. Had the program been placed on a more solid legal footing, these dedicated professionals may not have felt compelled to seek outside oversight.
* Prosecutions may be jeopardized. Prosecutions that were based in any way on information obtained by this program may now be jeopardized if a court finds that the information was collected or used improperly. A more solid legal basis could have avoided this risk.
* Damaging impact on intelligence professionals. The legal uncertainty of this program (1) puts the men and women

who were conducting this surveillance program, and those who were using the information, in jeopardy of potential criminal liability, (2) hurts agency morale, and (3) may well undermine officials' confidence that they can and should carry out future presidential directions without facing potential liability. (The same is true for the torture debate--where intelligence officials operated pursuant to a DOJ memo that was later repudiated when it became public. How are the folks on the front line of intelligence supposed to react to all of this?)
* Diverted vital investigative resources. There are indications that this program produced too many false leads and may have led to an unproductive diversion of important FBI resources that could have been better used conducting more fruitful investigations of suspected terrorist activity inside the US. For example, press reports indicate that only about 10 intercepts each year--out of the thousands of communications intercepted through this program-- proved suspicious enough to justify intercepting all the domestic communications of the US-end of the original communication. Presumably, the rest of the intercepted communications with Americans ultimately proved to be unrelated to terrorism and involved innocent Americans or others inside the US.
* Complicates future efforts to gain the support of Congress. The expansive reading of the AUMF may make it harder to get such authorizations in the future, potentially weakening public support for future conflicts. Indeed, the mistrust created on both sides of the aisle in Congress may impact executive branch efforts in a number of ways beyond just authorizations for the use of force.

Ensuring appropriate safeguards in FISA is essential to avoiding similar national security problems in the future and, ultimately, to defeating the terrorists. The bottom line is that the best way to be strong on terrorism is not to defer to the avaricious accumulation of power by the Executive branch but to better understand the true nature of the long term struggle against violent extremists. We can only defeat this threat by building upon the strengths of our system. That city on the hill can outshine the twisted but compelling lure of violent jihad. That is how we will ultimately prevail.