AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

WARRANTLESS SURVEILLANCE AND THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: THE ROLE OF CHECKS AND BALANCES IN PROTECTING AMERICANS' PRIVACY RIGHTS (PART I)

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

SEPTEMBER 5, 2007

Serial No. 110–78

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE

37–599 PDF WASHINGTON : 2007

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

JOHN CONYERS, JR., Michigan, *Chairman*

HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
LINDA T. SANCHEZ, California
STEVE COHEN, Tennessee
HANK JOHNSON, Georgia
BETTY SUTTON, Ohio
LUIS V. GUTIERREZ, Illinois
BRAD SHERMAN, California
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
ARTUR DAVIS, Alabama
DEBBIE WASSERMAN SCHULTZ, Florida
KEITH ELLISON, Minnesota

LAMAR SMITH, Texas
F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
CHRIS CANNON, Utah
RIC KELLER, Florida
DARRELL ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio

PERRY APELBAUM, *Staff Director and Chief Counsel*
JOSEPH GIBSON, *Minority Chief Counsel*

CONTENTS

SEPTEMBER 5, 2007

Page

OPENING STATEMENTS

The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Chairman, Committee on the Judiciary 1
The Honorable Lamar Smith, a Representative in Congress from the State of Texas, and Ranking Member, Committee on the Judiciary 2
The Honorable Jerrold Nadler, a Representative in Congress from the State of New York, and Member, Committee on the Judiciary 3
The Honorable Trent Franks, a Representative in Congress from the State of Arizona, and Member, Committee on the Judiciary 5
The Honorable Robert C. "Bobby" Scott, a Representative in Congress from the State of Virginia, and Member, Committee on the Judiciary 6

WITNESSES

The Honorable Bob Barr, former Member of Congress
Oral Testimony 7
Prepared Statement 10
Ms. Suzanne Spaulding, Principal, Bingham Consulting Group
Oral Testimony 16
Prepared Statement 18
Professor Robert F. Turner, University of Virginia School of Law
Oral Testimony 23
Prepared Statement 26
Mr. Morton H. Halperin, Director of U.S. Advocacy, Open Society Institute
Oral Testimony 66
Prepared Statement 68

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement of the Honorable Sheila Jackson Lee, a Representative in Congress from the State of Texas, and Member, Committee on the Judiciary 119
Prepared Statement of the Honorable Steve Cohen, a Representative in Congress from the State of Tennessee, and Member, Committee on the Judiciary 127
Senate bill S. 1927, the "Protect America Act of 2007" 128
CRS Report for Congress entitled "P.L. 110–55, the Protect American Act of 2007: Modifications to the Foreign Intelligence Surveillance Act," August 23, 2007 142
Letter from Denise A. Cardman, Acting Director, American Bar Association (ABA), dated September 14, 2007, to Chairman John Conyers, Jr., and Ranking Member Lamar S. Smith 165
Report of the Task Force on Domestic Surveillance in the Fight Against Terrorism, the American Bar Association (ABA), February 13, 2006 167

Page

Letter from John W. Whitehead, Founder and President, The Rutherford Institute, dated September 7, 2007, to Chairman John Conyers, Jr. 192

Prepared Statement of Caroline Frederickson, Director, Washington Legislative Office, American Civil Liberties Union (ACLU) 198

WARRANTLESS SURVEILLANCE AND THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: THE ROLE OF CHECKS AND BALANCES IN PROTECTING AMERICANS' PRIVACY RIGHTS (PART I)

WEDNESDAY, SEPTEMBER 5, 2007

HOUSE OF REPRESENTATIVES,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 10:23 a.m., in Room 2141, Rayburn House Office Building, the Honorable John Conyers, Jr. (Chairman of the Committee) presiding.

Present: Representatives Conyers, Berman, Nadler, Scott, Watt, Lofgren, Jackson Lee, Waters, Delahunt, Cohen, Johnson, Sutton, Baldwin, Schiff, Davis, Wasserman Schultz, Ellison, Smith, Coble, Goodlatte, Chabot, Lungren, Keller, Issa, Pence, King, Feeney, Franks, Gohmert, and Jordan.

Staff present: Ted Kalo, General Counsel/Deputy Staff Director; Sean McLaughlin, Deputy Chief Minority Counsel/Staff Director; George Slover, Legislative Counsel/Parliamentarian; and Anita L. Johnson, Professional Staff Member.

Mr. CONYERS. The Committee will reconvene and come to order.

We now turn to our consideration of Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights.

A month ago, the Congress passed an emergency wiretap law, at the President's urging, that granted the Attorney General largely unfettered authority to conduct surveillance of those who are engaged in communications abroad.

The law was controversial. I strongly opposed it. Fortunately, the law sunsets early next year. It had 6 months' duration.

Today, we begin the process of reviewing the law and considering modifications to it. In my judgment, there are three tests that ought be met as we consider additional legislation.

The first is we must be able to conduct real and meaningful oversight on the surveillance program. The second is that we must provide the courts with a meaningful role in reviewing surveillance that applies to American citizens.

And finally, we need to consider the role of telecommunications carriers. That, to me, summarizes what I think our present responsibilities are.

There is not a Member on this Committee or in this room—and I have invited the Chairman of Intelligence in the House to join us

this morning if his time permits—who would deny any Administration the legitimate tools and resources it needs to protect our citizens against terrorism.

But granting these tools cannot and should not involve abdicating our responsibility as a co-equal branch of Government to protect our precious rights and liberties. Both of them are important, and we can do these two things at once.

We urge my colleagues to remember what truly makes this country different from those of our enemies is that we can begin by reading the Constitution and the Bill of Rights, as well as our history books.

And I am happy today that we have such a distinguished group of witnesses to start off our consideration of this very important subject.

Our first witness is Bob Barr. Suzanne Spaulding is next. Dr. Robert F. Turner and Mort Halperin. I will introduce them in more detail later, but I want to welcome them right from the outset.

Good to have you all here and start us off.

And I now turn to the distinguished Ranking Member from Texas for his opening remarks, Lamar Smith.

Mr. SMITH. Thank you, Mr. Chairman.

Mr. Chairman, I hope that this hearing will lead to increased bipartisan support for measures needed to protect our country from terrorists.

We are a Nation at war with foreign terrorists who are continuing to plot deadly attacks. It is essential that our intelligence agencies have the necessary tools to detect and disrupt such attacks.

In the 30 years since Congress enacted the Foreign Intelligence Surveillance Act, telecommunications technology has dramatically changed.

As a result, the intelligence community has been hampered in gathering essential information about terrorists needed to prevent attacks against Americans.

Before we left for the August recess, Congress passed important legislation to fill a gap in FISA.

That bill clarified well-established law that neither the Constitution nor Federal law requires a court order to gather foreign communications from foreign terrorists, adopted flexible procedures to collect foreign intelligence from foreign terrorists overseas, and provided for court review of collection procedures under this new authority.

The director of national intelligence made it clear that these reforms were essential for the intelligence community to protect America from terrorist attacks.

Last April, the director submitted to Congress a comprehensive proposal to modernize FISA. The director's submission was ignored until the President made it clear in July that Congress had to act to ensure that our intelligence community obtains much-needed information about foreign terrorists.

During the recess, some Members of Congress made public statements promising to rewrite the bill we just passed. It would be a deadly mistake to weaken such legislation.

Nearly 60 percent of Americans polled on the subject of FISA reform supported the legislation Congress passed before the August recess. The simple fact is that Americans support surveillance of foreign terrorists when they contact persons in the United States.

Unfortunately, 90 percent of House Democrats voted to deny the director of national intelligence what he said he needed to prevent future terrorist attacks.

If the majority decides to reverse this law, they will hamper the ability of the intelligence community to prevent terrorist attacks. Innocent lives will be lost unnecessarily.

We all cherish our individual liberties, but our liberties cannot flourish without security. The pursuit of life, liberty and happiness can occur only in a safe and secure country.

I look forward to today's hearing with the hope that the debate on FISA reform will lead to enactment of all the director's proposals that he submitted in April.

These proposals would ensure assistance from private entities in conducting authorized surveillance activities, make certain that private entities are protected from liability for assisting the Government, and streamline the FISA process so that the intelligence community can direct resources to essential operation.

These reforms are long overdue. They should be debated without exaggerated claims of abuse or misleading claims of threats to civil liberty. Such a debate should also address the importance of all Americans living in a safe and secure country.

President George Washington once said there is nothing so likely to produce peace as to be well prepared to meet the enemy. We should maintain our commitment to winning the war against terrorism.

I thank you, Mr. Chairman, and I will yield back the balance of my time.

Mr. CONYERS. And I thank you, sir.

We have agreed to allow Congressman Bobby Scott to make a brief statement, Trent Franks to be recognized.

And I begin with Jerry Nadler, who is the Chairman of the Constitution Subcommittee, and I recognize the gentleman for 2.5 minutes.

Mr. NADLER. Thank you.

I would like to thank Chairman Conyers for his leadership in holding this hearing today.

This hearing is an important first step in examining the serious concerns regarding the recently enacted White House proposal to drastically alter the Foreign Intelligence Surveillance Act.

That law, rushed through Congress just before the August recess, gives unnecessary license for the Administration to wiretap Americans without court supervision.

Today's hearing specifically looks at one of the foundations of our fundamental liberties, the constitutional and statutory restrictions on the Government's ability to spy on people.

Both the fourth amendment and FISA were responsive to abuses by Government that thought they were above the law. The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures is a core limitation on the Government that protects each of us.

The framers of the Constitution understood this and, despite periodic lapses, so have most of our Nation's leaders.

Congress enacted FISA following the Church Committee report on surveillance abuses. It reflects Congress' understanding that the conduct of foreign intelligence activities is fundamentally different from domestic surveillance.

It nonetheless also reflects one of our Nation's founding principles that power, especially the power to invade people's privacy, cannot be exercised unchecked.

We rejected monarchy in this country more than 200 years ago. That means that no President, even this one, may become a law unto him or herself. As with every part of Government, there must always be checks and balances.

This President appears to have forgotten that fact. Not only has he asserted the right to go around the FISA court and the wiretap act, but he has actually done so.

Even more disturbing, he does not believe that he is accountable to the Congress, the courts or anyone else.

This Committee created the FISA statute and the FISA court, yet the President believes we are not entitled to know what he or the court are doing.

The President also believes that we are not entitled to know what he is doing, or has been doing, outside the confines of the FISA statute.

Now we have passed a flawed bill that, in the guise of updating the FISA law, actually gives the President almost unfettered power to spy without court supervision, not just on foreigners, but on Americans.

In the rush of the final hours before the August recess, we were stampeded by Administration fear-mongering and deception into signing away our rights. Thank God there is a 6-month sunset on the bill.

The legislation allows the NSA warrantless access to virtually all international communications of Americans with anyone outside the U.S. so long as the Government maintains that the surveillance is directed at people, including both citizens and foreigners, who are "reasonably believed to be located outside the U.S."

The Administration rejected all sensible efforts to focus such surveillance on terrorist activity or to provide meaningful court review of the rights of Americans who will be spied on in our country.

Make no mistake about it. We are speaking about domestic spying on American citizens.

We must act now to restore much-needed checks and balances into this damaged law. I look forward to——

Mr. CONYERS. The gentleman's time——

Mr. NADLER [continuing]. Standing with Chairmen Conyers and Reyes——

Mr. CONYERS [continuing]. Is nearly expired.

Mr. NADLER [continuing]. As we work with leadership to restore our freedoms that define America.

I thank you.

Mr. CONYERS. I thank you, sir.

Because the gentleman from Arizona, the Subcommittee Ranking Member, Trent Franks, is the only Republican that has agreed to

speak, we will give him 5 minutes. And we recognize Trent Franks of Arizona at this point.

Mr. FRANKS. Well, thank you very much, Mr. Chairman.

And, Mr. Chairman, I am hopeful that this meeting will lead, indeed, to a bipartisan effort to provide tools necessary and needed by our intelligence community to protect this Nation.

The arrest of eight suspected al-Qaida members in Denmark yesterday should serve as a reminder to us all that terrorists every day are plotting overseas to carry out deadly attacks.

Unfortunately, I am afraid the majority has failed to see the importance of monitoring terrorists overseas when they communicate with other terrorists outside this country or communicate with other terrorists inside the United States.

The director of national intelligence has made it clear the Foreign Intelligence Surveillance Act of 1978 needs to be updated.

It is imperative that the intelligence community have the flexibility to monitor foreign terrorists so that our Nation remains safe.

While opponents of FISA reforms continue to create, in my judgment, mountains out of molehills, it is important to remember that the Protect America Act restored FISA to its original focus by allowing the intelligence community to conduct surveillance of terrorists overseas without prior court approval.

The Protect America Act also allows for substantial oversight, including a submission of important implementation procedures for review by the FISA court.

The director of national intelligence has explained to Congress for more than a year that the Government devotes substantial resources to obtaining court approvals based on a showing of probable cause to conduct surveillance against terrorists, again, located overseas.

The Government does not know in advance who these terrorists will talk to and needs to have the flexibility to monitor calls that may occur between a foreign terrorist and a terrorist inside the United States.

Such monitoring of these communications can be conducted with well-established minimization rules that have been applied to restrict any unwarranted intrusion on the civil liberties of any United States citizen.

Requiring specific applications and authority for surveillance of such communications would impose burdens and delays with possible catastrophic consequences.

Mr. Chairman, so-called civil liberties groups and liberal newspaper editors have spent the last month spreading false allegations and misconceptions about foreign intelligence in order to gin up opposition to the Protect America Act.

Such claims and efforts are irresponsible. We are a Nation at war with foreign terrorists who continue to plan deadly attacks against America. The safety of Americans depends on action by Congress.

al-Qaida released a video recently promising a "big surprise." This threat, along with other activity, has heightened concern among our intelligence agencies.

Mr. Chairman, I have said many times in this Committee that we are at war with an ideology that is dedicated to the destruction

of the western world. And what we do will be considered carefully by future generations.

We have, in this Congress, given the President the authority to hunt down, ferret out and kill terrorists. The Constitution of the United States, as it empowers him to be the commander in chief, gives him the power to hunt down, ferret out and kill terrorists.

Surely he has the right and even the responsibility to listen to them on the phone before he proceeds. And I am hopeful that the Protect America Act will be made permanent and that other responsible FISA reforms will be crafted by this Committee and passed by the House.

And, Mr. Chairman, I yield back my time. Thank you.

Mr. CONYERS. Thank you, Trent.

I am now pleased to recognize Bobby Scott of Virginia, who is the Subcommittee Chairman of the Crime Subcommittee, and we recognize the gentleman at this time for 2.5 minutes.

Mr. SCOTT. Thank you, Mr. Chairman, and I appreciate you holding this hearing on warrantless surveillance under the Foreign Intelligence Surveillance Act, or FISA.

Because of the Department of Justice's refusal to respond to requests for information, we have been stymied in conducting meaningful oversight with respect to the Administration's warrantless surveillance and have been prevented from serving as an independent check on abuses by the President and the National Security Agency.

And so there is a sense, now, there are virtually no checks and balances on the Administration's discretion on who or what is the subject of warrantless surveillance.

Now, there has never been any controversy over overseas surveillance. You don't need any oversight for that. They can do what they want.

But now, based on the Administration's own certification, the Administration is now free to intercept communications believed to be from outside the United States into the United States and possibly even, because of ambiguities in the law, domestic calls that involve any vague notion of foreign intelligence.

Now, that is not terrorism. Foreign intelligence includes information regarding trade deals, or international politics or any kind of diplomacy.

And the standard the Government has to meet to engage in such data mining is that the acquisition of information has to be a significant justification for the invasive surveillance techniques, not the traditional primary justification.

Now, the Department of Justice has not credibly refuted the allegations that United States attorneys were fired because they failed to use the criminal justice process to pursue partisan political agendas.

So now, if the Department of Justice wiretaps when foreign intelligence is just a significant purpose and not the primary purpose, you wonder what the primary purpose may be.

Now, let's be clear. This is not a question of balancing rights and liberties versus security. The requirement that the Department of Justice has to essentially notify the FISA court of its surveillance activities in no way restricts what it can do.

There is even an emergency exception. If they are in a hurry, they can get the warrant after the fact. But meaningful FISA oversight will give the public confidence that the Department of Justice is complying with the law.

Thank you, Mr. Chairman, and I appreciate the fact that you are holding this hearing.

Mr. CONYERS. Thank you, Bobby Scott.

What a distinguished group of witnesses we have today. Our first witness is a former colleague and a Member of the Judiciary Committee who served with great distinction over the years that he was in the Congress.

Bob Barr is also a founding member of the Liberty and Security Initiative of the Constitution Project and just from what I have been observing, he has been almost as active out of the Congress as he has been in the Congress.

And we are delighted that he has once again accepted an invitation to come before the Judiciary Committee on this very important subject.

And without objection, his and all other Members' statements will be included in their entirety in the record.

Welcome, Congressman Barr.

TESTIMONY OF THE HONORABLE BOB BARR, FORMER MEMBER OF CONGRESS3

Mr. BARR. Thank you, Mr. Chairman. It is both a pleasure and an honor to be back among so many former colleagues and continuing friends on both sides of the aisle, and particularly on such an important topic as the Chairman and the Committee is set to consider today.

It is a pleasure also being with my good friend and colleague from my home state of Georgia, Congressman Johnson.

Hank, it is great to be with you and, as the Chairman has indicated, an extremely distinguished panel.

Mr. Chairman, I read with some interest a recent interview with National Intelligence Director Mike McConnell which appeared in the El Paso Times.

And I can't help but note that the dire warnings by the Administration similar to those which were employed to secure very rapid passage of the FISA amendments exactly 1 month ago, or 1 month ago and then signed exactly 1 month ago by the President, continue unabated.

And they ill serve any Administration, Republican or Democrat. And I refer particularly to the words of Mr. McConnell that indicate that simply debating this topic as this Committee is doing today will "cost American lives."

I think this is a completely unacceptable approach to the democratic representative process that we have in this country whereby the Congress and the Administration are both deemed not just—it is deemed not just appropriate, but absolutely essential, to debate important policy issues, particularly those, as today, which are very well-founded, inextricably founded, in constitutional principles. Noted among them is the fourth amendment.

And to try and squelch even the debate of these topics by raising the false specter that debating the constitutionality of FISA or

amendments to FISA will some how cost American lives, and therefore we ought not to even debate these issues, ought not to be something that the American people accept.

And I am certainly glad that this Committee and the current leadership—yourself, certainly, Mr. Chairman—are not falling prey to that. These matters are, indeed, very worthy of debate.

If these matters are not worthy of debate—that is, the extent to which our own Government can spy on our own citizens in this, our own land, are not worthy of debate—then it is hard to imagine any issue that would be worthy of debate.

So I think it is extremely important that this topic is coming before the Committee.

The very title of this hearing places the subject away or removes the topic away from simply a dry technical discussion to a discussion not only of the technology but, more importantly, of the fundamental constitutional principles and rights underlying intelligence surveillance or any kind of electronic surveillance by this Government, which, indeed, immediately and necessarily involves the privacy rights of our citizens as embodied not only but particularly in the fourth amendment.

The manner in which this Administration argued in support of what it termed a technical amendment to FISA in order to accommodate the problem at hand as it identified it—that is, two individuals, both outside the United States, engaging in electronic communication, but because of the technology that communication is routed through the United States—is one issue, and it is a legitimate issue.

Unfortunately, as the Chairman and some of the other Members on the Chairman's side have indicated, the supposed fix by the Administration as embodied in the legislation, P.L. 110–55, that the President signed on August 5, go far, far beyond any reasonable effort to address that particular problem.

And now virtually any electronic communication—that is, a telephone call or an e-mail—by any person in this country, U.S. citizen or otherwise, that simply has as one of its parties somebody reasonably believed to be overseas, is now subject to surveillance by the Government without ever even contemplating, much less going before, the Foreign Intelligence Surveillance Court or any court.

And this notion that we address a very specific technical problem by a massive rewrite, in essence, of the entire FISA mechanism is one that I believe is entirely unacceptable.

And hopefully now, beginning with the process here today, the Congress will rectify and restore constitutional balance to the FISA process.

This will not weaken the legislation. I fail to see that ever when legislation is crafted to bring it in accord with the Constitution, that weakens it. This would not weaken it.

It would, indeed, greatly strengthen not only the legislation but also the constitutional underpinnings of the right to privacy for all Americans.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Barr follows:]

PREPARED STATEMENT OF THE HONORABLE BOB BARR

OFFICE OF BOB BARR
Member of Congress, 1995-2003

TESTIMONY BY FORMER REP. BOB BARR BEFORE THE JUDICIARY COMMITTEE OF THE U.S. HOUSE OF REPRESENTATIVES CONCERNING OPPOSITION TO S. 1927, "THE PROTECT AMERICA ACT"

SEPTEMBER 5, 2007

Mr. Chairman, and Members of this distinguished Committee on the Judiciary of the U.S. House of Representatives, on which I was privileged to serve throughout my eight years as a Member of this body, it is an honor to appear today to speak to the vitally important topic at hand, "Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights." The very title of this hearing is a tribute to your understanding – apparently lost on many in the administration – that electronic surveillance even in this post-911 world, is about much more than technology, and that consideration of the mechanisms and parameters of FISA cannot be considered in the sterile vacuum of technical amendments alone. Surveillance, whether for law-enforcement or foreign-intelligence purposes, does affect the fundamental privacy rights of American citizens, and this recognition must be the underpinning of any consideration of this inherently intrusive technique.

Thank you, Mr. Chairman, for inviting me here today to appear with this distinguished panel of Americans, to discuss this crucially important topic. I appear today as a private citizen, but also as a former Member of this Committee and as a once-again practicing attorney. I am also privileged to inform the Committee that I continue to serve as chairman of Patriots to Restore Checks and Balances, and as the holder of the 21st Century Liberties Chair for Freedom and Privacy at the American Conservative Union.

For several months leading to the passage and subsequent signing by the President of S. 1927, "The Protect America Act," on August 5, 2007 as

P.L. 110-55, the administration had been beating the PR drums clamoring for amendments to the Foreign Intelligence Surveillance Act (FISA), ostensibly in order to bring the 1978 law into accord with 21st Century technology. Then, shortly prior to its passage, the administration and its supporters in the Congress raised the decibel level of their arguments; claiming that a recent federal court decision finding that an electronic communication between two non-U.S. persons both outside the United States was nonetheless subject to the FISA warrant requirements because the communication was routed through the United States, made it absolutely urgent that the Congress "fix" FISA. The administration said it was crucial that such communications be monitored without being subject to the delays and uncertainties that the administration said would hamper its foreign intelligence-gathering efforts in light of the secret court decision.

The administration's gambit worked. A majority of members in both houses of the Congress, apparently receptive to the administration's dire warnings and its thinly-veiled warnings that failure to pass the remedial FISA legislation would likely result in a terrorist incident that -- for failure of the Congress to give the administration the tools it needed to gather electronic intelligence to help thwart such incidents – would be laid at the doorstep of the Congress.

Unfortunately, the legislation that passed in this atmosphere did not simply "fix" the problem identified by the administration – which arguably is meritorious – but went far, far beyond what could reasonably be deemed necessary to address a technological problem with the 1970s-era FISA law that manifested itself because of 21st-Century technology. Now, thanks to the poorly-considered "Protect America Act" the administration is able to order the surreptitious interception and surveillance of virtually any electronic communication (including phone calls and e-mails) from or to any person in the United States, so long as the government reasonably believes one of the parties is "located outside of the United States." Insofar as one party to a communication being outside the United States is the very definition of an "international communication," the universe of calls and e-mail transmissions subject now to warrantless monitoring by agencies of the federal government encompasses all such communications. This result is fully breathtaking in the practical scope of its reach, and in its potential damage to the very foundation of the Fourth Amendment to our Constitution.

Despite continued efforts by the Administration to characterize these changes as merely "technical" and only "corrective" of technological problems arising in and as a result of the "internet age" – problems compounded by the [still-secret] court decision – the changes wrought by "The Protect America Act" are neither "technical" nor "corrective." Especially those provisions found in Section 2 of the Act (which amends FISA by adding new Sections 105A and 105B), represent a profound alteration in the scope and reach of FISA, and a dramatic "brave new world" of electronic surveillance.

Essentially, thanks to this law, the government has potentially carved out from Fourth-Amendment protection an entire class of communication – electronic communications going to a person outside the United States, or coming to a person inside the United States. There is -- and here again contrary to the public missives by the Administration and its supporters -- no requirement whatsoever, implied or express, that even one of the parties to such category of communications subject to warrantless surveillance would first have to have any known or even suspect connection with any terrorist or other targeted group or activity.

As a result of the broad manner in which the Administration was able to effect this change to FISA – removing from the definition of "electronic surveillance" and therefore from the entire reach and mechanism of FISA entirely, any communication of a person "reasonably believed to be located outside of the United States" – it has effectively neutered any oversight role the Congress or the Foreign Intelligence Surveillance Court (FISC) might play in overseeing or limiting the government's surveillance. The only oversight role either the Congress or the FISC would be able to exert would be superficial at best.

Even a Reagan-appointed federal judge, who has served with distinction on the FISC – the Honorable Royce Lamberth – understands the gravamen of the danger posed by unfettered electronic surveillance in the name of "fighting the war on terrorism":

> "We have to understand you can fight the war [on terrorism] and lose everything if you have no civil liberties left when you get through fighting the war…[b]ut what we have found in the history of our country is that you can't trust the executive…[w]e still have to preserve our civil liberties. Judges are the kinds of people you want to entrust that kind of judgment to more than

> the executive," U.S. District Court Judge Royce Lamberth, June 23, 2007.

Judge Lamberth's relevant and timely admonition follows the prescient warning by the well-known jurist, Justice Louis Brandeis, who, in the 1928 *Olmstead* decision issued this ominous warning:

> "Subtler and more far-reaching means of invading privacy have become available to the government… Ways may someday be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home… It is not the breaking of his doors, and the rummaging of his drawers that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property."

These jurists are hardly alone in sounding the alarm against unfettered government invasion of citizens' privacy through the use of electronic surveillance powers and equipment, regardless of whether done in the name of fighting organized crime, communist infiltrators, or terrorists. I am gratified this Committee, or at least you, Mr. Chairman, and some of your colleagues, have heard this call and heeded the warnings of these wise jurists and many others in government, academia and the private sector who understand the bedrock principles embodied in our Constitution and its Bill of Rights and who understand also that no threat, no matter how serious, should ever provide the excuse for decimating the carefully constructed set of checks and balances woven into the fabric of our system of government.

I know this Committee understands as do few citizens that the quest – legitimate as it is – for actionable foreign intelligence, should never be allowed to serve as a subterfuge for circumventing the requirements of the Fourth Amendment, which functions in essence as the fundamental privacy right for each and every citizen of this great land. This understanding was the basis for creation of the FISA mechanism in the first instance; yet with the stroke of the presidential pen in signing P.L. 110-55, that rationale and that principle has been swept aside. What is left is a structure with no foundation. The sole limitation on which communications involving American citizens the government could

surreptitiously monitor without any intervention of the courts, is that the government "reasonably believe[s]" at least one of the parties to be "located outside of the United States." That's it; that's all; end of argument.

The silver lining in this dark cloud of unfettered and unsupervised surveillance of virtually all or any international electronic communications, is the fact that the leadership of this 110th Congress granted the administration only a six-month expansion of FISA. All freedom-loving Americans should applaud the Congress for having taken this step and at least provided a hedge against perpetual government warrantless surveillance. In addition to repealing the changes to FISA resulting from Section 2 of P.L. 110-55, and reining in the unnecessary and constitutionally-destructive expansion of FISA, the Congress should take the opportunity provided by this six-month sunset period, to address in a narrow and focused manner the specific change sought by the administration. This could include addressing the anomaly of requiring a court order to intercept a communication between two persons both outside the United States if the communication is simply routed through our country. The administration should not be permitted to take a mile when they ask for – and are entitled to only – an inch.

Additionally, the Congress should avail itself of this opportunity, and of your leadership, Mr. Chairman, to replace the fig-leaf court and congressional oversight provided for in P.L. 110-55, with meaningful oversight such as contained in the original FISA; a mechanism, I might add, that, despite cries to the contrary by the administration, has worked well and expeditiously these many years. If in fact the administration can point to a specific area in which the judicial or congressional oversight needs to be tweaked to strengthen or streamline it – consistent with and not adverse to the original intent of both FISA and the Fourth Amendment – then I would respectfully recommend this Committee afford the administration a willing but skeptical ear, force it to justify the changes sought, and then provide only the clearest and most narrow remedy to address the problem.

In closing, Mr. Chairman, let me refer back to April 12, 2000, on which date I testified on FISA before your sister committee, the Permanent Select Committee on Intelligence. That same day, before that same committee, on that same subject, Gen. Michael Hayden, in his then-

capacity as Director of the National Security Agency (NSA), testified. He correctly noted that before the NSA could lawfully initiate any surreptitious collection of intelligence by electronic surveillance on any American in the United States, the government first "must have a court order." Until the President signed P.L. 110-55 last month, this remained the law.

General Hayden had it right then, and this committee has it right now in insisting that the privacy rights of American continue to be thus protected; and that necessary exceptions to the general principle that when an American citizen picks up a phone or types an e-mail into their Blackberry to someone or some entity that happens to be outside the geographic boundaries of the United States, he or she can rest assured their communication will *not* be intercepted absent a good, sufficient and constitutionally-based reason. In this expectation, we are all children of of our Founding Fathers. I thank this Committee for working to reestablish this foundational principle by reining in the power shift from citizen to government represented by "The Protect America Act."

Mr. CONYERS. I thank you very much.

Congressman Hank Johnson was desperately trying to get my attention before we started. I yield him a very small amount of time.

Mr. JOHNSON. I thank you, Mr. Chairman.

Mr. Chairman, the purpose of my request is to simply acknowledge the presence of my Georgia colleague in the bar of Georgia, Mr. Bob Barr, a man who we have not agreed on all of our political issues.

But I certainly deeply respect the patriotism that he has displayed throughout his career, both as a U.S. attorney where he prosecuted public corruption cases in a bipartisan way, as well as was tough on other crime, and also as a congressman, and then his post-congressional career where he has been an eloquent spokesperson for our adherence to constitutional principles, as we proceed in a more dangerous existence on this planet.

So I just wanted to acknowledge your great work and say that I appreciate the fact that you are a lawyer from Georgia, and you continue to do great work. So thank you very much.

Mr. BARR. Appreciate very much the very kind and unwarranted words of my friend from Georgia. Thank you.

Mr. CONYERS. Our next witness is attorney Suzanne Spaulding, who was Assistant General Counsel at the CIA, previously a minority staff director on the House Permanent Select Committee of Intelligence, Executive Director of the National Commission on Terrorism, and currently Managing Director of the Harbour Group, specializing in national security and terrorism issues.

We are delighted and pleased that you could join us this morning.

TESTIMONY OF SUZANNE SPAULDING, PRINCIPAL, BINGHAM CONSULTING GROUP

Ms. SPAULDING. Chairman Conyers, Ranking Member Smith, Members of the Committee, thank you for this opportunity to testify on changes to the Foreign Intelligence Surveillance Act.

I would like to begin by emphasizing that in the over 20 years that I have spent working on efforts to combat terrorism, I developed a strong sense of the seriousness of the national security challenges that we face and a deep respect for the men and women in our national security agencies who work so hard to keep us safe.

We all agree that we owe it to those professionals to ensure that they have the tools they need to do their jobs, tools that reflect the ways in which advances of technology have changed both the nature of the threat and our capacity to meet it.

They also 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.

Unfortunately, the newly enacted changes to FISA do not provide clear guidance and instead appear to provide potentially very broad authority and inadequate safeguards.

I will touch on just a few points today with additional comments in my written testimony.

First, avoid changing definitions. The terms in FISA not only appear throughout this complex statute, they are also referenced in and inform other laws, executive orders, directives and policies.

The risk of unintended consequences is significant, particularly when changing the definition of a term as fundamental as electronic surveillance.

Second, the words "notwithstanding any other law," which is how the new section 105(b) begins, should always raise a red flag. These words mean that all other laws that regulate the collection of intelligence inside the United States no longer apply to activities undertaken under section 105(b).

And those activities are potentially extremely far-reaching. Section 105(b) appears to provide statutory authorization for the Government to gather information on any kind of communication and to gather it inside the United States from U.S. citizens, so long as it is about someone who happens to be outside the United States at that time.

Thus, it would appear, for example, to authorize intercepting U.S. mail between two people inside the United States, as long as the Government reasonably believes that the letter discusses someone outside the United States.

The careful statutory regime governing mail intercepts is overruled by the "notwithstanding any other law" language in section 105(b).

Similarly, it would appear that the Attorney General could authorize the physical search of a person's office for stored e-mails or letters concerning their colleagues overseas. The FISA provisions that regulate physical searches become irrelevant if section 105(b) applies.

This language also overrules privacy protections in the Electronic Communications Privacy Act and other privacy laws. And none of this domestic intelligence collection 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.

The Protect Act requires that information be minimized but it appears to apply the relatively relaxed, permissive procedures that currently apply when a FISA judge has reviewed a full FISA application and found probable cause.

Instead, what should be required are the far more stringent procedures that currently apply when the Attorney General has unilaterally approved surveillance under his current authority under 102(a) of FISA.

Changes to FISA should be the narrowest possible to remove whatever impediment has arisen to using FISA. There ought to be a way for the Government to know, even if it is after the fact, where the parties to these communications are located.

My phone company seems to be able to determine whether I am using my cell phone at home or overseas. They charge me a lot more when I use it overseas.

This technology can begin to provide the basis for a legal regime that is much more narrowly focused with precise procedures and safeguards to govern surveillance that involves people inside the United States.

Finally, Congress should seek a stronger commitment from the Administration that it will actually abide by the law.

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.

In conclusion, Mr. Chairman, I believe that ultimately 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 or undermine our carefully constructed system of checks and balances make it more likely, not less likely, that we will be attacked again.

The long-term challenge of international terrorism is a struggle for hearts and minds, a competition of narratives.

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 extremism.

We can only defeat this threat by building upon the strengths of our system, including its checks and balances. That city on a hill can outshine the twisted but compelling lure of violent jihad. That is how we will ultimately prevail.

Thank you, Mr. Chairman.

[The prepared statement of Ms. Spaulding follows:]

PREPARED STATEMENT OF SUZANNE E. SPAULDING

Mr. Chairman, Ranking Member, Members of the Committee, thank you for this opportunity to testify on changes to the Foreign Intelligence Surveillance Act (FISA). I'd like to begin by emphasizing that I have spent over twenty years working on efforts to combat terrorism. Over those two decades, in my work 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

I understand that the committee plans to hold further hearings to examine in greater detail the specifics of the Protect Act and assess whether to make changes or replace it. Thus, I will limit my testimony today to a few key points.

Avoid trying to accomplish your objective 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, while still setting up a scheme to govern those activities within this statute designed to regulate electronic surveillance, creates confusion. This does not even address the consequences for internal NSA directives and other legal and policy documents that reference electronic surveillance.

A better approach would be one similar to that found in the bill introduced by Representative Reyes, Chair of the House Permanent Select Committee on Intel-

ligence, that explicitly authorizes the surveillance when the target is reasonably believed outside US, with strong safeguards to protect against "reverse targeting" or unnecessary intrusions on the privacy of the US—end of a communication.

As a general rule, never use the words "notwithstanding any other law." This is how the new section 105B begins and that 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.

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 when 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 overrules 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, the Communications Privacy Act, even HIPPA and the Privacy Act, would no longer have any impact on this activity.

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.

And none of this domestic intelligence collection 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.

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. 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, 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.

In addition, 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.

Finally, rigorous oversight of the use of this authority will be essential. Given the reported failure of the AG to properly report to Congress regarding problems with the use of national security letters, I would urge Congress to direct the Justice Department and DNI Inspectors General to 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 anything 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. This new procedures under section 105B are optional; the AG and DNI "may" choose to use them; they are not required to follow this process. But 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 also decide to go ahead and violate the law, 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 live 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 Attor-

ney General and the FBI Director that the program was reportedly shut down for weeks until more safeguards were added. That means for weeks we were not listening to what we are told are conversations between terrorists and people inside the US. 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. Why was it leaked? Because the professionals at NSA were so troubled by what they believed was an illegal program. Had the program been placed on a more solid legal footing, these dedicated professionals would 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 for political reasons. 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 President 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 draw of violent jihad. That is how we will ultimately prevail.

Mr. CONYERS. Thank you, Attorney Spaulding.

We next turn to Dr. Robert Turner, who has served in both the Department of Defense and the Department of State. He is a professor at the University of Virginia School of Law, and serves as the Associate Director of an organization he helped create there, the Center for National Security Law. And we welcome him at this time.

Welcome to the Committee, sir.

TESTIMONY OF PROFESSOR ROBERT F. TURNER, UNIVERSITY OF VIRGINIA SCHOOL OF LAW

Mr. TURNER. Thank you, Mr. Chairman. It is a pleasure to be here.

Mr. Smith and Members of the Committee.

I have prepared a rather lengthy statement I would submit for the record at this time.

I worked in the Senate when FISA was enacted, and I later oversaw the compliance with FISA when I served as counsel to the President's Intelligence Oversight Board in White House in the early 1980's.

But the central focus of my testimony and my expertise in this area is on the separation of national security constitutional powers. I have sent more than 30 years working in this area, and I have given you a fairly long statement focusing on that.

Speaking personally, and certainly not on behalf of the organization, I am a strong supporter both of the legislation you just passed, the Protect America Act, and also of the revisions submitted by the Administration, but I don't pretend to be an expert on all the details of those.

When FISA was first enacted, I believed it was unconstitutional. I continue to feel that way.

In my testimony, I have given you quotations from people like James Madison, Thomas Jefferson, George Washington, Alexander Hamilton, John Jay, John Marshall—some of the most important people who set up this country—all of them arguing that when the Constitution gave the President "the executive power" in article II, section 1, that carried with it the general control of foreign affairs, save for the specific exceptions mentioned in the Constitution which were to be construed narrowly.

In the area of foreign intelligence, it is absolutely clear that this is presidential business. It has always been viewed as presidential business. It was not even questioned until well into my adult lifetime in the 1970's.

John Jay, in Federalist Number 64, specifically talked about this. And he explained that foreign sources of intelligence would not trust, would not cooperate, if they knew the information would be shared with Congress. And therefore the Constitution had left the President "able to manage the business of intelligence as prudence might suggest."

Every President going back to George Washington has conducted intelligence without sharing it with Congress, without seeking permission from Congress. Every President from FDR to Jimmy Carter engaged in warrantless wiretapping and said that was legal.

The Carter Justice Department said there was a national security, a foreign intelligence national security, exception to the warrant requirement of the fourth amendment.

And when Griffin Bell testified on FISA he said, obviously FISA cannot take away the President's independent powers. But he went on to say however, President Carter is willing to agree to comply with FISA so there is no problem. That, obviously, did not bind any future Presidents and could not take away their constitutional power.

When Congress in 1790 first appropriated funds for foreign intelligence, it was extremely deferential. It said the President should account specifically for those sums which, in his judgment, could be made public and for the amount of other expenditures so Congress could replenish the kitty.

In 1818, there was a debate in this chamber in which Henry Clay and other Members said, of course it would be improper for us to inquire into how money is spent for foreign intelligence purposes.

And when Congress in 1968 passed title III, the first wiretap statute, it said specifically that nothing in this title shall limit the constitutional power of the President to obtain foreign intelligence information. Thus, Congress, by statute, recognized this independent power.

When the Supreme Court in 1967, for the first time, declared that wiretaps were, in fact, a seizure under the fourth amendment, it included a footnote that exempted national security wiretaps.

In the *Keith* case in 1972, when the Supreme Court held warrants would be required for domestic wiretaps, twice Justice Powell, speaking for the unanimous court, said this does not affect foreign powers, or wiretaps of foreign powers or their agents, in this country.

This was, in fact, consistent with a blue ribbon panel of the American Bar Association in 1971 which concluded there should be a distinction. There should not be a requirement for warrants for foreign intelligence wiretaps, but when the target is purely a domestic subversive group or something like that, you must have a warrant.

Since *Keith*, every single Federal court of appeals to decide the issue agreed the President has independent constitutional power to decide this.

FISA set up a special court of review consistent of Federal court of appeals judges. In 2002, they unanimously noted that every Federal court to decide the issue had said the President has this power, many of them saying specifically there is a foreign intelligence national security exception to the fourth amendment.

And the court of review went on to say, "FISA could not encroach on the President's constitutional power."

Now, a second point. FISA contributed to the success of 9/11. You all have heard about Colleen Rowley, the Time Magazine person of the year, in 2002 who complained the FBI lawyers would not even submit her FISA warrant so she could look at Moussaoui's laptop.

The reason was that FISA forgot to include lone wolf terrorists. I discuss this in my testimony. Congress finally corrected this a few years ago. But it was FISA that kept the FBI from perhaps discovering that plot.

In addition, General Michael Hayden, who was the director of NSA for many years, including through 2001, has testified it is his professional view that had the terrorist surveillance program that was blocked by FISA been in effect in 2001, NSA would have identified at least some of the al-Qaida terrorists as such prior to the attacks.

My fundamental conclusion, Mr. Chairman, is a simple one. When a mere statute like FISA does battle with our majestic Constitution, the Constitution always wins, and properly wins.

As John Marshall told us in *Marbury v. Madison,* an act of the legislature repugnant to the Constitution is void.

My bottom line conclusion is it is not the President who, in trying to protect the country, has been gathering foreign intelligence who has been the lawbreaker. Rather, it is Congress.

Thank you, Mr. Chairman. That concludes my remarks.
[The statement of Mr. Turner follows:]

PREPARED STATEMENT OF ROBERT F. TURNER

IS CONGRESS THE REAL "LAWBREAKER"?:

Reconciling FISA with the Constitution

Prepared Statement of

Prof. Robert F. Turner, SJD

Cofounder
CENTER FOR NATIONAL SECURITY LAW
University of Virginia School of Law

Before the

House Judiciary Committee

Hearing on

Warrantless Surveillance and the Foreign Intelligence Surveillance Act:
The Role of Checks and Balances in Protecting Americans' Privacy Rights

Wednesday, September 5, 2007 • 10:15 A.M.

2141 Rayburn House Office Building

CONTENTS

Introduction 5
The Constitution and Control Over "The Business of Intelligence" 6
Congress and the Keeping of Secrets 9
Unchecked Presidential Discretion 10
The Fourth Amendment 11
Presidential Recognition of Executive Control Over Foreign Intelligence Activities 14
Congressional Recognition of Executive Control Over Foreign Intelligence Activities 15
Judicial Recognition of Executive Control Over Foreign Intelligence Activities 17
- *Katz v. United States* (1967) 17
- The *Keith* Case (1972) 17
- Other Pre-FISA Cases 20
- *United States v. Truong* (1980) 21
- *In re Sealed Case (2002)* 22

What About *Youngstown*? 23
Post-Vietnam Congressional Usurpation of Presidential Power and Its Consequences 28
Conclusions 34
- FISA Was Essentially a Gentleman's Agreement Between Congress and President Carter 34
- Why President's Like FISA 35
- Confusing Law Enforcement Search Warrants and the Business of Foreign Intelligence Collection 35
- Revising FISA 38
- Focus on Minimization Issues 39
- The Stakes Are High for Congress Too 40

GOOD MORNING, MR. CHAIRMAN. It is an honor to appear before this distinguished Committee to discuss issues of checks and balances and the FISA statute.

These are not new issues to me. I have focused much of my academic career on the separation of national security constitutional powers since first becoming interested in these issues more than four decades ago. I witnessed first hand the tragic consequences of the breakdown of legislative-executive relations in Indochina, and as a Senate staff member I followed the Church Committee hearings on intelligence abuse. Three years later in that same capacity I followed the enactment of FISA; and three years after that I was hired to oversee executive branch compliance with FISA and other intelligence laws and executive orders as Counsel to the President's Intelligence Oversight Board in the White House.

I was raised in a military family and taught to believe that when our nation goes to war we set aside our differences and unite against the common enemy. My father and his brother each served in the Army in Europe in World War II, and my only brother and I each served twice in Vietnam – he as a Marine sergeant and later lieutenant, and I as an Army lieutenant and captain. Because I had written my undergraduate honors thesis on the conflict, I was detailed to work for the American Embassy. Ironically, a major part of my work involved investigating Viet Cong terrorism. Long before the attacks of September 11, 2001, I was warning that America was vulnerable and the only issue was *when* and not *whether* we were going to be hit.

After 9/11, I was delighted to see America come together in a display of unity not seen since World War II. I think one of the reasons we have not been hit at home again may be the message that display of bipartisan unity sent to our enemies – they had united and awakened a sleeping giant. Watching the way partisan politics has torn this nation apart these past few years has therefore been a source of great sadness to me, as it has undone much of the good we accomplished and provided incentives for our enemies to strike us again.

And sadly, much of the discord appears to be a result of *ignorance*. I don't question the sincerity of either side, but it would be difficult to overstate the harm that has resulted from the failure of our education system to train our public leaders about our constitutional system in the realm of national security and foreign affairs.

This morning, I would like to examine some important constitutional history that I hope may help both sides better understand this dispute. I will quote to you from the *Federalist* Papers and from the writings of men like Washington, Jefferson, Madison, Hamilton, Jay, and John Marshall – letting their words explain their understanding of our Constitution in this specialized area. I will also quote to you from congressional documents and court opinions, and I will show that there was a broad consensus among all three branches of government about the control of foreign intelligence activities under our Constitution prior to the Vietnam War. It is as if during the heated debates which

characterized the later years of that conflict we had a collective national hard-drive crash, and both sides forgot the original understanding. I think it is time that we pause for a few moments and revisit that history.

Introduction

Let me start by setting forth my perception of the two major competing interests here today. On one side we have people focused heavily on the terrorist threat who believe we need to unite behind our elected president and give him the flexibility and discretion to collect the intelligence we need to identify and neutralize the al Qaeda threat. At least some of them believe the Constitution gives the president the discretion to do that without being told how by Congress. On the other side we have people who agree it is important to collect foreign intelligence to protect America against terrorism, but who don't want to sacrifice the Bill of Rights in the process. To them, claims of broad "executive power" over intelligence, war, and other issues ring of the regime of King George III rather than a constitutional president in a free and democratic republic. They want to protect our nation, but not at the expense of the Constitution and the rule of law. I respect that view, but I am now going to tell you why I believe they are mistaken.

I would like to to begin by summarizing a few basic points:

- In our system of government we have a hierarchy of "laws," with the Constitution being supreme and superior to a conflicting act by either the president or Congress. Article V provides several means for amendment, but they do not include merely passing an inconsistent legislative statute or an informal agreement that a particular president will comply with a statute that in reality seeks impermissibly to narrow his constitutional discretion. Congress may no more usurp the constitutional powers of the president by statute that it may usurp the rights guaranteed to the people by enacting legislation contrary to the First Amendment.

- Not all presidential decisions were intended by the Constitution to be "checked" by Congress or the courts.

- This is especially true with respect to the conduct of business with foreign states and protecting the security of the nation against foreign powers and their agents within this country. When the Founding Fathers gave the nation's "executive" power to the president, they understood that this power included the general control of our nation's relations with the external world. To be sure, both the Senate and Congress were given certain "negatives" in this area as well as several affirmative powers often viewed as part of "foreign affairs"; but, as "exceptions" in the eyes of the Framers of our Constitution to the general grant of executive power to the president, these powers were intended to be construed strictly.

• At the core of exclusive presidential constitutional powers are the conduct of diplomacy, the collection of foreign intelligence, and the supreme command of military forces and conduct of military operations. Into these areas, Congress was not intended by the Founding Fathers to interfere. This was the consistent view of the *Federalist Papers* and the courts have repeatedly affirmed these principles.

• The distinction between domestic or internal affairs that affect the rights of individuals, on the one hand, and foreign or external affairs that affect the nation, on the other, is fundamental to understanding our constitutional separation of powers. That is the difference between the Steel-Seizure case (*Youngstown*) and *Curtiss-Wright*. And the failure of many scholars to see this distinction has led to a great deal of confusion and misunderstanding.

• Admittedly, not every decision can be neatly placed into a "domestic" or "foreign" box. Many decisions touch on both areas. And often in resolving them we must balance competing interests. But the distinction is nevertheless an important one.

The Constitution and Control Over "The Business of Intelligence"

It is often noted that the Constitution does not even mention the words "national security" and "foreign affairs," and from this many modern commentators conclude that this area is no different from domestic affairs – Congress has the power to set policy by law and the job of the Executive is to see that those laws and the policies they embody are "faithfully executed." Some who are familiar with our history note that this was not in reality the paradigm that prevailed, and it is speculated that when the beloved President George Washington seized control in this area the other branches went along rather than risk offending this wonderful old man.

In reality, there was a broad consensus among all three branches that foreign affairs were different than domestic affairs, and the reason we don't understand this today is because of changes in our language over the centuries. I remember once being confused when I read a letter from one of the great champions of our new Constitution around 1788 who described it to a friend as an "awful" document. It took some research into the etymology of "awful" to realize that in the eighteenth century the term described something that filled one with awe or was awe inspiring. And in a similar way, concepts like "executive power" and "declaration of war" had specific meanings when the Constitution was written that have largely been forgotten.

The Founding Fathers were remarkably well-read men, and they were familiar with John Locke's *Second Treatise on Civil Government*, Montesquieu's *Spirit of the Laws*, and Blackstone's *Commentaries on the Laws of England*. Each of these distinguished theorists – and most of their contemporaries as well – viewed the control of foreign affairs (what Locke described as control over 'war, peace, leagues, and alliances") as part of the "executive" power.

We know that this was the shared understanding of the content of the grant in Article II, Section 1, of the Constitution of the nation's "executive Power" to the president, because it was widely discussed at the time. For example, in a June 1789 letter, Representative James Madison explained: "[T]he Executive power being in general terms vested in the President, all powers of an Executive nature, not particularly taken away must belong to that department. . . ."[1]

Relying upon this same clause ten months later, Thomas Jefferson wrote in a memo to President Washington:

> The Constitution . . . . has declared that "the Executive power shall be vested in the President," submitting only special articles of it to a negative by the Senate . . . . *The transaction of business with foreign nations is executive altogether*; it belongs, then to the head of that department, except as to such portions of it as are specially submitted to the Senate. Exceptions are to be construed strictly.[2]

Three days later, Washington recorded in his diary that he had discussed Jefferson's memo with Representative Madison and Chief Justice John Jay – who was by far the nation's most experienced authority on foreign relations – and both shared Jefferson's view that the Senate had "no constitutional right to interfere" with the business of diplomacy save for its expressed constitutional negatives. As Washington explained, "all the rest being Executive and vested in the President by the Constitution."[3]

Writing as *Pacificus* in 1793, the third author of the *Federalist Papers* (in addition to Madison and Jay), Alexander Hamilton, also pointed to the grant to the president in Article II, Section 1, of the Constitution of the nation's "executive" power in remarking:

> [A]s the participation of the Senate in the making of treaties, and the power of the Legislature to declare war, are exceptions out of the general "executive power" vested in the President, they are to be construed strictly, and ought to be extended no further than is essential to their execution.[4]

Another of Jefferson's political enemies to make this observation was the legendary John Marshall, who as a Federalist member of the House of Representatives in 1800 defended President Adams' decision to surrender an alleged British deserter pursuant to the extradition clause of the Jay Treaty without any involvement of the judiciary by reasoning: "The President is the sole organ of the nation in its external relations, and its

---

[1] *Madison to Edmund Pendleton*, 21 June 1789, *in* 5 WRITINGS OF JAMES MADISON 405-06 n. (Gaillard Hunt, ed. 1904).

[2] *Jefferson's Opinion on the powers of the Senate Respecting Diplomatic Appointments*, April 24, 1790, in 3 THE WRITINGS OF THOMAS JEFFERSON 16 (Mem. ed. 1903) (italics added).

[3] 4 DIARIES OF GEORGE WASHINGTON 122 (Regents' Ed. 1925).

[4] 15 THE PAPERS OF ALEXANDER HAMILTON 39 (Harold C. Syrett ed., 1969)

sole representative with foreign nations. . . . He possesses the whole Executive power. . . . In this respect the President expresses constitutionally the will of the nation."[5]

Arguably the finest book on this topic is the late Quincy Wright's 1922 classic, *The Control of American Foreign Relations*. As you may know, Professor Wright served as president of the American Political Science Association and was a leading constitutional scholar for most of the twentieth century. (My own interest in the field was sparked by a lecture I heard him give in 1966.) He wrote that "When the constitutional convention gave 'executive power' to the President, the foreign relations power was the essential element in the grant, but they carefully protected this power from abuse by provisions for senatorial or congressional veto."[6]

Many of you will remember the late Senator J. William Fulbright, who served as chairman of the Senate Foreign Relations Committee for fifteen years and was a leading critic of the Vietnam War. Speaking at Cornell Law School in 1959, Chairman Fulbright captured the conventional wisdom shared by all three branches until that time when, in arguing for even greater presidential power, he explained:

> The pre-eminent *responsibility* of the President for the formulation and conduct of American foreign policy is clear and unalterable. He has, as Alexander Hamilton defined it, all powers in international affairs "which the Constitution does not vest elsewhere in clear terms." He possesses sole authority to communicate and negotiate with foreign powers. He controls the external aspects of the Nation's power, which can be moved by his will alone—the armed forces, the diplomatic corps, the Central Intelligence Agency, and all of the vast executive apparatus.[7]

I would emphasize the word "formulation" here. The president's authority was not merely to carry out policies established by Congress, as is the case domestically, but to *make* policy as well. When those policies took the form of a solemn treaty, the Senate had a negative. But otherwise foreign policy was an executive function.

Does this mean that Congress and the Senate have no powers related to foreign affairs? Of course not. Congress has important powers, including control over foreign commerce, a negative over a decision to launch a major offensive war, control over appropriations,[8] and many other powers enumerated in Article I, Section 8. But none of these give Congress a role in the conduct of war or diplomacy or the business of intelligence. The Senate has even more authority related to foreign affairs. It shares the powers of

---

[5] 10 ANNALS OF CONG. 613-15 (1800).

[6] QUINCY WRIGHT, THE CONTROL OF AMERICAN FOREIGN RELATIONS 147 (1922).

[7] J. William Fulbright, *American Foreign Policy in the 20th Century Under an 18th-Century Constitution*, 47 CORNELL L. Q. 1, 3, (1961).

[8] However, Congress may not use "conditions" on appropriations bills to indirectly do things it is prohibited from doing directly. Congress may no more properly condition military appropriations upon the president's agreement to fight the war as instructed by Congress than it may condition appropriations for the judiciary upon the Supreme Court's deciding a particular case as directed by Congress or promising never to strike down legislation on constitutional grounds.

Congress with the House, and also is given several negatives – such as the right to block a completed treaty or a diplomatic nomination. But it is important to keep in mind that when the Senate considers treaties and nominations, it is acting not as a chamber of the legislature but rather in "executive session" considering business from the "executive calendar."

Congress and the Keeping of Secrets

A key consideration in the decision to deny Congress a role in diplomacy and the conduct of war (both of which involve the critically important function of gathering foreign intelligence and safeguarding secrets) is that Congress was not thought able to keep secrets. I testified at length on this issue in 1994 before the House Permanent Select Committee on Intelligence (HPSCI), so I will not spend a great deal of time on this issue this morning.[9] But it is important to understand that this was not just a concern of the executive branch. Indeed, before there was an executive branch, under the Articles of Confederation in 1775, the Continental Congress understood that it was not competent for the business of diplomacy and its members could not be relied upon to keep secrets, so it established a "Committee of Secret Correspondence" to conduct diplomacy, run spies, and the like. And in setting up this committee, the Continental Congress expressly instructed it to delete the names of intelligence sources in any reports it made to Congress.[10]

In reality, the Committee of Secret Correspondence found it necessary to conceal from Congress many secrets other than the names of spies and other intelligence sources. When France agreed to a major covert operation to provide support to the American Revolution, the committee members were delighted. But Benjamin Franklin and the other four members unanimously resolved that they could not share the information with others in Congress, explaining "We find by fatal experience that Congress consists of too many members to keep secrets."[11]

The *Federalist Papers* are replete with references to the need for secrecy, unity of design, and speed and dispatch in war and foreign affairs – and each of these was recognized as a strength of the executive branch. Since the official journal and Madison's notes on the proceedings of the Federal Convention were not made public until decades after the Constitution was ratified, these brilliant essays on the principles of our new government were the most important single source in explaining the Constitution to the people. And in *Federalist* No. 64, John Jay made it clear that neither Congress nor the Senate were to have any role in the business of intelligence. His essay is worth quoting at length:

> There are cases where the most useful intelligence may be obtained, if the persons possessing it can be relieved from apprehensions of discovery. Those apprehensions will operate on those persons whether they are

[9] My prepared statement is available on line at: http://www.fas.org/irp/congress/1994_hr/turner.htm.
[10] 4 JOURNALS OF THE CONTINENTAL CONGRESS 1774-1789 at 345 (Worthington C. Ford, *et al.* eds, 1905.)
[11] "Verbal statement of Thomas Story to the Committee," 2 PAUL FORCE, AMERICAN ARCHIVES: A DOCUMENTARY HISTORY OF THE NORTH AMERICAN COLONIES, 5th Ser., 819 (1837-53).

> actuated by mercenary or friendly motives, and there doubtless are many of both descriptions, who would rely on the secrecy of the president, but who would not confide in that of the senate, and still less in that of a large popular assembly. The convention have done well therefore in so disposing of the power of making treaties, that although *the president* must in forming them act by the advice and consent of the senate, yet he *will be able to manage the business of intelligence in such manner as prudence may suggest.*[12]

Sadly, my experience both in the legislative and executive branches and as a scholar have persuaded me that the Framer's concern was justified. I've seen far too many harmful leaks from Capitol Hill. (To be sure, too many leaks also come from the executive department.)

Unchecked Presidential Discretion

It is popular today to teach that in our government, all presidential powers must be checked by Congress and/or the courts. But that is in fact neither an accurate statement nor the original understanding as explained by the Framers of our Constitution – especially with respect to the nation's external relations. We have already seen that the "executive" power was only to be checked by the expressed "exceptions" clearly vested in Congress or the Senate and that these were to be construed strictly. Obviously, some powers not involving foreign affairs – such as the president's pardon power – are also exclusive. But as the Supreme Court noted in the landmark 1936 *Curtiss-Wright* decision – which remains by far the most frequently cited Supreme Court case on foreign affairs – there was a marked difference between domestic and foreign affairs. The Court explained:

> Not only, as we have shown, is the federal power over external affairs in origin and essential character different from that over internal affairs, but *participation in the exercise of the power is significantly limited.* In this vast external realm, with its important, complicated, delicate and manifold problems, the President alone has the power to speak or listen as a representative of the nation. He makes treaties with the advice and consent of the Senate; but he alone negotiates. *Into the field of negotiation the Senate cannot intrude, and Congress itself is powerless to invade it.*[13]

That this was consistent with the original understanding of the Constitution is apparent from perhaps the most famous Supreme Court case of all times, Chief Justice John Marshall's landmark opinion in the 1803 case of *Marbury v. Madison*:

---

[12] FEDERALIST No. 64 at 434-35 (Jacob E. Cooke, ed. 1961) (emphasis added).
[13] *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 319 (1936) (emphasis added).

> By the constitution of the United States, the President is invested with certain important political powers, in the exercise of which he is to use his own discretion, and is accountable only to his country in his political character, and to his own conscience. . . . [A]nd *whatever opinion may be entertained of the manner in which executive discretion may be used, still there exists, and can exist, no power to control that discretion.* The subjects are political. They respect the nation, not individual rights, and being entrusted to the executive, *the decision of the executive is conclusive.*[14]

To illustrate this point, Chief Justice Marshall continued:

> The application of this remark will be perceived by adverting to the act of congress for establishing the department of foreign affairs. This officer, as his duties were prescribed by that act, is to conform precisely to the will of the president. He is the mere organ by whom that will is communicated. The acts of such an officer, as an officer, can never be examinable by the courts.[15]

So it is apparent that the idea of presidential supremacy is foreign affairs – subject to narrow but very important "negatives" or "checks" vested in Congress and the Senate – is not some grand scheme for seizing monarchial powers for another "King George" dreamed up by John Yoo or David Addington, but was in fact the original design of our Constitution.

Another key point from Chief Justice Marshall's *Marbury* opinion is equally important and addresses a situation in which Congress acts without constitutional authority or attempts to exercise powers vested by the people through the Constitution in another branch. Marshall declared, and again I quote: "an act of the legislature, repugnant to the constitution, is void."

The Fourth Amendment

In *Curtiss-Wright* and many other cases, the Supreme Court has noted that all constitutional powers "must be exercised in subordination to the applicable provisions of the Constitution."[16] This is critically important. And while Congress was not given constitutional authority to interfere in the business of intelligence, that does not mean there are no checks at all – particularly when a foreign affairs or intelligence issue also involves the constitutional rights of Americans.

The Bill of Rights – including the Fourth Amendment – is every bit as in effect in wartime as in peacetime. To be sure, the determination of what is a "reasonable" search

---

[14] *Marbury v. Madison*, 5 U.S. [1 Cranch] 137, 165-66 (1803) (emphasis added).
[15] *Id.* at 165-66.
[16] *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 320 (1936).

may well shift when the government is seeking to prevent a WMD attack on the American mainland versus more traditional peacetime concerns like enforcing laws against white-collar criminals. But all exercises of presidential power must comply with relevant provisions of the Constitution.

One popular myth today is that the Fourth Amendment requires probable cause and a judicial warrant for any lawful search or seizure. When I entered this building a short time ago a government agent demanded to search my briefcase and made me pass through a metal detector. This was a "search" under the Fourth Amendment, and that government agent had neither probable cause to believe that I had done anything wrong nor a judicial warrant for the search. And since the First Amendment guarantees "the right of the people . . . to petition the Government," such "searches" are arguably an impediment to the exercise of a constitutional right.

Yet few would argue that such searches are a bad idea, and perhaps fewer that they are unconstitutional. For the Constitution does not prohibit "searches and seizures" by government, but only those searches and seizures that are "unreasonable." And as I will discuss, these public safety searches have long been upheld as reasonable by the courts without the slightest degree of individualized suspicion or probable cause and without a warrant. They are similar to the searches we all endure before boarding a commercial airplane. In a similar way, monitoring the electronic communications of foreign nationals outside this country who are believed to be affiliated with terrorist groups – particularly during a period of congressionally-authorized war – is reasonable. And it is perhaps even *more* reasonable when they are communicating with people inside the United States, who might be plotting the next catastrophic terrorist attack.

In assessing the Fourth Amendment, we need to remember that the Supreme Court has repeatedly observed that its language is not absolute. Thus, speaking for a unanimous Court in the so-called *Keith* case (*United States v. United States District Court*), which will be discussed in some detail in a few minutes, Justice Powell observed: "As the Fourth Amendment is not absolute in its terms, our task is to examine and balance the basic values at stake in this case: the duty of Government to protect the domestic security, and the potential danger posed by unreasonable surveillance to individual privacy and free expression."[17]

In making this balance, we should keep in mind that – even in peacetime – the Supreme Court has repeatedly recognized that "It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation. . . ."[18] This is presumably all the more true in situations like the present, when the nation is involved in a war authorized by Congress. As the unanimous Supreme Court noted in the Keith case, "unless Government safeguards its own capacity to function and to preserve the security of its people, society itself could become so disordered that all rights and liberties would be endangered."[19]

---

[17] *United States v. United States District Court*, 407 U.S. 297 at 314-15 (1972).
[18] *Haig v. Agee*, 453 U.S. 280, ___ (1981).
[19] 407 U.S. at ___.

On the other side of the scale, the interception of electronic communications is not generally viewed as among the more egregious violations of individual privacy. Indeed, it was not until 1967 that the Supreme Court decided that wiretaps even involved a Fourth Amendment interest, and when they did the great defender of the Constitution, Justice Hugo Black, refused to accept it. Lower courts have also recognized that wiretaps are "a relatively nonintrusive search."[20]

In addition, the Fourth Amendment was designed primarily to guard against unreasonable searches and seizures in a *criminal law* context, and in other settings the Supreme Court has recognized a number of exceptions. As the Court explained in *Von Raab* in 1989:

> While we have often emphasized, and reiterate today, that a search must be supported, as a general matter, by a warrant issued upon probable cause, . . . our decision in *Railway Labor Executives* reaffirms the longstanding principle that neither a warrant nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every circumstance. . . . As we note in *Railway Labor Executives*, our cases establish that where a Fourth Amendment intrusion serves special governmental needs, beyond the normal need for law enforcement, it is necessary to balance the individual's privacy expectations against the Government's interests to determine whether it is impractical to require a warrant or some level of individualized suspicion in the particular context.[21]

These "special needs" cases usually involve some aspect of public safety or security. The Court has permitted warrantless searches of individuals crossing into the United States from other countries or even within a certain distance of national borders,[22] safety inspections of restaurants and certain types of factories, and even fairly intrusive mandatory drug testing of customs agents and even high school athletes.[23]

I suspect that each of you regularly encounters one classic example of these exceptions to the warrant requirement each time you enter a public airport and have to submit to a search of your person and baggage. These can be more than a little annoying and costs each of us many hours of time each year that we can never recover. Yet most of us recognize that being inconvenienced by our government to guard against our plane being hijacked or blown up is a good trade-off.

American courts have recognized that airport security screenings constitute a "search" under the Fourth Amendment, yet have consistently upheld their legality despite the slightest individualized suspicion, much less "probable cause" and a judicial warrant. As the legendary Second Circuit jurist Henry Friendly —rumored to have achieved the

---

[20] *United States v. Ehrlichman*, 376 F. Supp. 29, __ (1974).
[21] *National Treasury Employees Union v. Von Raab*, 489 U.S. 656 at 665-66 (1989).
[22] *See, e.g., Schmerber v. California*, 384 U.S. 757 (1966).
[23] *See, e.g., Von Raab, supra* at 656; *Board of Education v. Earls*, 536 US 822 (2002).

highest grade-point average in the history of Harvard Law School – explained in the 1974 *Edwards* case:

> The reasonableness of a warrantless search depends, as many of the airport search opinions have stated, on balancing the need for a search against the offensiveness of the intrusion. We need not labor the point with respect to need; the success of the FAA's anti-hijacking program should not obscure the enormous dangers to life and property from terrorists, ordinary criminals, or the demented. The search of carry-on baggage, applied to everyone, involves not the slightest stigma . . . . More than a million Americans subject themselves to it daily; all but a handful do this cheerfully, even eagerly, knowing it is essential for their protection. To brand such a search as unreasonable would go beyond any fair interpretation of the Fourth Amendment.[24]

Given the risks inherent in modern terrorist attacks, one might think that the same logic that leads courts to conclude that conducting mandatory drug tests for student athletes and rather intrusive personal searches of any American who wishes to travel by airplane would, *a fortiori*, apply to electronic searches designed to obtain foreign intelligence information, and in reality, every federal court of appeals to have decided the issue has held that the president has independent constitutional authority to approve foreign intelligence national security wiretaps without a warrant. But let me save that discussion for later.

Presidential Recognition of Executive Control Over Foreign Intelligence Activities

I shall not take your time to document the long history of both affirmative assertions of constitutional power for presidents to authorize the collection of foreign intelligence information and the actual exercise of that power, for I suspect that point is not in controversy. Even before we had a Constitution, General George Washington authorized the opening of mail coming from Great Britain – instructing that it be carefully resealed before delivery so as not to disclose it had been read and risk losing a valuable source of future intelligence.

Thomas Jefferson and his Secretary of State James Madison conducted a number of foreign intelligence activities ddand even paramilitary operations without informing or seeking authorization from Congress, including sending two-thirds of the new American navy half-way around the known world with instructions to sink and burn ships and raising an small army of Greek and Arab mercenaries to send across a vast North African dessert to attack a foreign government.[25]

---

[24] *United States v. Edwards*, 498 F.2d 496, 500 (2d. Cir. 1974).

[25] *See, e.g.*, Robert F. Turner, *State Responsibility and the War on Terror: The Legacy of Thomas Jefferson and the Barbary Pirates*, 4 CHICAGO J. INT'L LAW 121 (2003).

In an 1804 letter to Treasury secretary Albert Gallatin, President Jefferson explained:

> The Constitution has made the Executive the organ for managing our intercourse with foreign nations. . . . The Executive being thus charged with the foreign intercourse, no law has undertaken to prescribe its specific duties. . . . From the origin of the present government to this day . . . . it has been the uniform opinion and practice that the whole foreign fund was placed by the Legislature on the footing of a contingent fund, in which they undertake no specifications, but leave the whole to the discretion of the President.[26]

This was in fact a longstanding practice. Save for the Senate's legitimate authority to reject or consent to the ratification of treaties, it was not until my lifetime that Congress made serious efforts to seize control of presidential powers in this area. Most of those came in the wake of the Vietnam War.

Discussing Jefferson's behavior in 1996, Dr. Stephen F. Knott – a leading authority on the history of covert operations in this country – observed: "Jefferson's employment of covert operations was not an example of an extraconstitutional abuse of power but a simple exercise of the president's prerequisite to implement foreign policy."[27]

In the twentieth century, both Woodrow Wilson and Franklin D. Roosevelt acted unilaterally to authorize wartime interception of international cable traffic. Every American president from Roosevelt to Carter authorized the warrantless collection of foreign intelligence information without judicial or legislative sanction.[28]

Congressional Recognition of Executive Control Over Foreign Intelligence Activities

In his first State of the Union Address on Jan 8, 1790, President Washington asked for "a competent fund designated for defraying the expenses incident to the conduct of foreign affairs."[29] The statute that resulted reflected the broad recognition in Congress that foreign affairs was the president's business. Despite the requirement in Article I, Section 9, of the Constitution that "a regular Statement and Account of the Receipts and Expenditures of all public Money shall be published from time to time," the statute permitted the president at his discretion to conceal how he had spent the money:

> [T]he President shall account specifically for all such expenditures of the said money *as in his judgment may be made public*, and also for the *amount* of

[26] 11 WRITINGS OF THOMAS JEFFERSON 5, 9, 10 (Mem. ed. 1903).
[27] STEPHEN F. KNOTT, SECRET AND SANCTIONED 83 (1996).
[28] Cite to 1 House Rep't 95-1283 at 13-17. For information on the use of a warrantless national security wiretap by the Carter administration for more than 250 days without judicial or legislative involvement, see [*Truong* case] XX
[29] Available on line at:
http://dcms.gov/index.asp?Type=B_BASIC&SEC=%7BA31FEC3A-8CFA-4D86-A3BE-4708342FD755%7D .

> such expenditures *as he may think it advisable not to specify*, and cause a regular statement and account thereof to be laid before Congress annually . . . .[30]

This deferential language was incorporated in similar bills for many years.

Similarly, although Article II, Section 2, of the Constitution gave the Senate a negative over many presidential appointments, Congress recognized that the president needed no legislative sanction to hire spies.[31] Indeed, in 1818, when a debate occurred in the House chamber about reports of a diplomatic mission to a South American country, the legendary Henry Clay declared that expenditures from the president's "secret service fund" were not "a proper subject for inquiry" by Congress, and others quickly echoed this view.[32]

The congressional view of presidential authority over the collection of foreign intelligence could hardly have been more clearly explained as in the Omnibus Crime Control and Safe Streets Act of 1968, when Congress enacted Title III establishing legal rules for wiretaps for the first time in our history. (This followed the Supreme Court's decision of the previous year declaring that wiretaps constituted a "seizure" under the Fourth Amendment.) But in so doing, Congress emphasized that it was not attempting to usurp the constitutional powers of the president over foreign intelligence:

> Nothing contained in this chapter . . . shall limit the *constitutional power of the President* to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, *to obtain foreign intelligence information* deemed essential to the security of the United States, *or to protect national security information* against foreign intelligence activities.[33]

Some have attempted to play down the significance of this language, correctly observing that it did not constitute a grant of any power to the president. It did, however, constitute a clear recognition by Congress that the president has independent constitutional authority to collect foreign intelligence. Others have dismissed it on the grounds that, in enacting FISA a decade later, Congress repealed this language. However, that does not change the fact that in 1968 Congress itself, as a matter of law, recognized the independent constitutional power of the president to authorize warrantless foreign intelligence wiretaps.

Judicial Recognition of Executive Control Over Foreign Intelligence Activities

[30] 1 STAT. 129 (1790) (emphasis added).
[31] HENRY MERRITT WRISTON, EXECUTIVE AGENTS IN AMERICAN FOREIGN RELATIONS 224-39 (1929).
[32] 32 ANNALS OF CONG. 1466 (1818).
[33] 18 USC § 2511(3) (1970) (emphasis added).

Not only did both political branches from the earliest days of our nation recognize exclusive presidential control over the business of intelligence, but the courts, too, have been consistent in recognizing that authority. To be sure, there are no cases directly addressing a legislative challenge to presidential authority – in large part because until relatively recently no such challenges existed. But there have been several criminal cases in which defendants challenged the president's authority to authorize warrantless surveillance, and a brief review of some of those is instructive. But first we should briefly deal with *Katz*.

Katz v. United States (1967)

In 1967, for the first time the Supreme Court held that wiretaps "conducted without prior approval by a judge or magistrate were *per se* unreasonable, under the Fourth Amendment."[34] However, in footnote 23 the Court specifically distinguished its holding from a case involving national security wiretaps, writing: "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case."[35] While this footnote clearly left the issue of the constitutionality of presidentially-authorized national security wiretaps unresolved, the fact that the Court included it strongly suggested that at least some of the justices believed such activities were lawful.

The *Keith* Case (1972)

The issue of warrantless national security wiretaps came before the Court five years after *Katz*, when a member of the White Panther Party (an ally of the better-known Black Panthers) named "Pun" Plamondon, who had been on the FBI's Most Wanted list for bombing a CIA office in Ann Arbor, Michigan in 1968, was arrested with sixty-five pounds of dynamite in his possession along with maps showing military installations in the area.[36] This was one of the first opinions written by Justice Lewis Powell, and to fully understand it some background on Justice Powell may be useful.

As an OSS officer during World War II, Powell had worked on the ULTRA Project with British Intelligence breaking German codes. He thus brought to the bench a rare personal expertise in the business of intelligence. He had also served as president of the American Bar Association, and in that capacity had been involved in creating and serving on an ABA blue-ribbon committee to establish standards for electronic surveillance. Completed in 1971, the ABA committee endorsed the use of warrantless electronic surveillance in cases involving threats from a "foreign power" or "to protect military or other national security information against foreign intelligence activities"; and

[34] *Katz v. United States*, 389 U. S. 347 (1967).
[35] *Id.* at ___ n. 23.
[36] JOHN C. JEFFRIES, JR., JUSTICE LEWIS F. POWELL, JR. 375 (1994).

recommended as well that evidence obtained through such activities be admissible in criminal court when the search was found to be "reasonable."[37]

However, in the commentary to the ABA report, the committee explained that the foundation for this recommendation was "the relation between this country and foreign nations," adding: "The Committee considered and rejected language which would have recognized a comparable residuary power in the President not subject to prior judicial review to deal with purely domestic subversive groups."[38]

Noting that the Supreme Court had carved out a number of special needs exceptions to the warrant requirement, the ABA Committee observed:

> Indeed, if the interest of 'national self protection' warrants the present far-reaching practice in border searches, the interest of protecting the national security from foreign powers would seem to do no less. . . . The standard, therefore, recognizes that the techniques must be, ought to be, and will be employed in the national security area.[39]

Justice Powell's biographer and former law clerk, University of Virginia Law School Dean John Jeffries, writes that a year later in a Richmond newspaper article, Powell expressed serious doubts about the decision to exclude domestic national security wiretaps from the proposed exception to the Fourth Amendment's warrant requirement. Three months later, Powell found himself facing confirmation hearings in the Senate to become a member of the Supreme Court. During this process, Senator Birch Bayh and others grilled him repeatedly about the propriety of "warrantless surveillance in domestic security cases."[40] Powell sought to dodge some of the more detailed questions, but in the end promised to "consider the entire case in light of the Bill of Rights and the restrictions in the Constitution of the United States for the benefit of the people of our country."[41] Within a year, Powell was called upon to write what turned out to be the unanimous Supreme Court opinion in the *Keith* case.

To the surprise of many, Powell declared that the warrant requirement would apply to national security investigations involving purely domestic targets with no suspected ties to a foreign power. But he carefully distinguished this from a foreign intelligence case, writing: "Further, the instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of *foreign powers, within or without this country*."[42] Powell found the distinction important enough to reemphasize it near the end of the opinion:

---

[37] AMERICAN BAR ASSOCIATION PROJECT ON STANDARDS FOR CRIMINAL JUSTICE, ELECTRONIC SURVEILLANCE 120 (Approved Draft 1971 and Feb. 1971 Supp. 11). This study was footnoted by Justice Powell the following year in *Keith* at 322 n.20.

[38] AMERICAN BAR ASSOCIATION PROJECT ON STANDARDS FOR CRIMINAL JUSTICE, ELECTRONIC SURVEILLANCE 121.

[39] *Id.* at 123.

[40] JEFFRIES, JUSTICE LEWIS F. POWELL, JR. 377.

[41] *Id.*

[42] *United States v. United States District Court,* 407 U.S. 297, 308 (1972) (emphasis added).

> We emphasize, before concluding this opinion, the scope of our decision. As stated at the outset, this case involves only the *domestic* aspects of national security. We have not addressed and express no opinion as to, the issues which may be involved with respect to *activities of foreign powers or their agents*.[43]

From the opinion alone, it is difficult to divine the views of the justices on the issue before us, the constitutional power of the president to authorize warrantless foreign intelligence surveillance. Fortunately, Powell's able biographer fills in some of the blanks for us, writing that only Powell, Douglas, Brennan, Stewart, and Marshall were prepared to "say once and for all that warrantless wiretaps in domestic security cases were flatly unconstitutional."[44] Justice Rehnquist did not participate, presumably because he had been involved in the matter while a senior Justice Department official. The other three justices were willing to join the opinion on non-constitutional grounds.

We of course cannot be certain, but on the basis of Justice Powell's well-established belief that warrantless wiretaps *were* constitutional in the *foreign* intelligence area, and the fact that only four other justices were prepared to strike down such wiretaps even in a case involving a purely *domestic* target, there is little reason to believe that had this case involved an agent of a foreign power the surveillance would have been declared unconstitutional. One might add to this equation the strongly pro-national security views of Justice Rehnquist had he been in a position to vote on a case.

Before leaving the *Keith* case, one more observation is in order. It has often been alleged that FISA was enacted at the urging of the Supreme Court in *Keith*. That is simply not true, and this is absolutely clear from the language of the opinion:

> Given those potential distinctions between Title III criminal surveillances and those involving the *domestic* security, Congress may wish to consider protective standards for *the latter* which differ from those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection.[45]

Thus, the Court was inviting Congress to legislate standards for "domestic security" surveillance, not to enact a *foreign* intelligence surveillance act. But few people actually read Supreme Court decisions, and by 1978 Congress was on a roll in grabbing control

---

[43] *Id.* at 321-22 (emphasis added)

[44] *Id.* at 379.

[45] 407 U.S. at 322-23 (emphasis added).

over national security powers that has for nearly two centuries been recognized by all three branches as the province of the executive.

Other Pre-FISA Cases

Since the *Keith* case, every U.S. Court of Appeals to consider the issue has ruled in favor of an independent presidential constitutional power to collect foreign intelligence information without a warrant. A useful summary is provided in the June 8, 1978, report of the House Permanent Select Committee on Intelligence on the FISA bill:

> Since the *Keith* case, four circuit courts of appeals have addressed the question the Supreme Court reserved. The fifth circuit in *United States v. Brown* . . . upheld the legality of a surveillance in which the defendant, an American citizen, was incidentally overheard as a result of a warrantless wiretap authorized by the Attorney General for foreign intelligence purposes. The court found that on the basis of
>
> > the President's constitutional duty to act for the United States in the field of foreign affairs, and his inherent power to protect national security in the conduct of foreign intelligence.
>
> In *United States v. Butenko*, . . . the third circuit similarly held that electronic surveillance conducted without a warrant would be lawful so long as the primary purpose was to obtain foreign intelligence information. The court found that such surveillance would be reasonable under the fourth amendment without a warrant even though it might involve the overhearing of conversations.[46]

The HPSCI report then mentioned a warrantless wiretap case involving a purely *domestic* target and noted that, in *dicta*, a plurality of judges, applying *Keith*, had "questioned whether any national security exception to the warrant requirement would be constitutionally permissible.[47] The HPSCI report then continued:

> Finally, in *United States v. Buck*, . . . the ninth circuit following *Brown* and *Butenko*, referred to warrantless surveillance of foreign powers and agents of foreign powers as a "recognized exception to the general warrant requirement."
> *On the basis of the three circuit court decisions upholding the power of the President* in certain circumstances to authorize electronic surveillance without a warrant, and in *the absence of any court holding to the contrary*, the [Carter] Justice Department firmly maintains that in the absence of legislation, such warrantless surveillances are constitutional.
> Thus, after almost 50 years of case law dealing with the subject of warrantless electronic surveillance, and despite the *practice* of warrantless

[46] 1 H. REP'T 95-1283 at 19-20.
[47] *Id.* at 20 (discussing *Zweibon v. Mitchell*, 516 F.2d 594 (D.C. Cir, 1975)).

> foreign intelligence surveillance sanctioned and engaged in *by nine administrations*, constitutional limits on the President's powers to order such surveillances *remains an open question*.[48]

Right! Every president has done it and every appeals court to decide the issue has upheld the power of the president – Congress itself has recognized the president's constitutional power as a matter of law, and the Supreme Court has repeatedly taken pains not to limit the president in this area – so Congress concludes the issue is a toss-up.

Consider also the sleight-of-hand used by HPSCI to explain away the admitted fact that every president had engaged in warrantless foreign intelligence surveillance and every court to address the issue had upheld such a power. "Under H. R. 7308, as amended, the authority of the President to engage in surveillance in certain cases without a warrant will derive from statute, not the Constitution . . . ."[49] This certainly seems to be asserting that statutes trump the Constitution – once Congress passes FISA, any constitutional power of the president will vanish – which suggests that someone didn't pay enough attention to *Marbury v. Madison* in law school. Imagine the consequences if this theory were applied to the First Amendment or judicial review.

***United States v. Truong* (1980)**

Before FISA was enacted, the Carter Administration engaged in extensive warrantless wiretapping and "bugging" with hidden microphones and video cameras to track the espionage activities of a Vietnamese national who had resided in the United States for more than a decade and was a vocal critic of American involvement in the Vietnam War. Some of the surveillance equipment had been in operation for nearly a year, running continuously and recording virtually every call. The effort paid off with evidence that Truong Dinh Hung was obtaining classified documents from a government employee and delivering them to another Vietnamese (who happened to be a CIA and FBI informant) for delivery to representatives of the Socialist Republic of Vietnam in Paris. The surveillance operation was personally approved by Attorney General Griffin Bell, without any effort to obtain judicial sanction or any notification of Congress.

At the district court level, the judge admitted into evidence the recordings that had been made prior to July 20, 1977, on the theory that their purpose was to gather foreign intelligence information. Recordings made after that date were excluded on the theory that the investigation had shifted from foreign intelligence gathering to law enforcement.

The Fourth Circuit Court of Appeals noted that the Carter administration had "relied upon a 'foreign intelligence' exception to the Fourth Amendment's warrant requirement," contending that no warrant was necessary because of the president's "constitutional prerogatives in the area of foreign affairs."[50]

---

[48] *Id.* at 20-21 (emphasis added).
[49] *Id.* at 26.
[50] *United States v. Truong*, 629 F.2d 908, 912 (1980).

Relying upon *Keith* and applying a balancing test, the court of appeals provided a lengthy analysis of why the executive branch was better suited to decide these issues than federal district judges and relied on *Curtiss-Wright* for the proposition that "separation of powers requires us to acknowledge the principal responsibility of the President for foreign affairs and concomitantly for foreign intelligence surveillance."[51] It emphasized that this "foreign intelligence exception to the warrant requirement" was only applicable to cases involving "a foreign power, its agent or collaborators."[52]

So both before and after FISA, federal appeals courts have remained *unanimous* in recognizing presidential power to authorize warrantless foreign intelligence surveillance. Indeed, as the next case will demonstrate, things got even worse for Congress after FISA was enacted.

In re Sealed Case (2002)

In addition to establishing the FISA Court to consider applications and grant or refuse[53] warrants, Congress established a FISA Court of Review consisting of U.S. Court of Appeals judges to review appeals from the FISA Court. That special appeals chamber has only issued one opinion to date, in 2002. And in that opinion the Court of Review unanimously declared:

> The *Truong* court, as did all the other courts to have decided the issue, held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information. . . . *We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach on the President's constitutional power.*[54]

Congress appears to have largely ignored this judicial declaration that it has broken the law by usurping an exclusive presidential power. But perhaps that's not surprising, given the other areas where Congress has decided to flagrantly thumb its nose at the Supreme Court and the Constitution. For example, since the Supreme Court nearly twenty-five years ago declared that "legislative vetoes" were unconstitutional on several grounds, Congress had made no effort to repeal them but instead has enacted *hundreds* of new ones.

---

[51] *Id.* at 914.
[52] *Id.* at 912, 915.
[53] There is a common misperception that the FISA Court is but a "rubber stamp" because it has approved the overwhelming majority of the applications submitted. Having been involved in this process in the early days, I can explain that the reason the court did not need to reject applications was because a truly remarkable woman named Mary Laughton, who set up and ran the Justice Department's Office of Intelligence Policy and Review for many years prior to her untimely death, made *certain* that no application went forward to the court that was not totally in order and consistent with the statute.
[54] *In re Sealed Case,* 310 F.3d 717, 742 Foreign Int. Surv. Ct. Rev., November 18, 2002 (NO. 02-002, 02-001).

What About *Youngstown*?

I will be shocked if at least one of the other witnesses at this morning's hearing does not rely heavily on Justice Robert Jackson's concurring opinion in the 1952 "Steel-Seizure" case of *Youngstown Sheet and Tube Co. v. Sawyer*.[55] Even if they don't, it was relied upon by HPSCI in its 1978 FISA report,[56] so it deserves some discussion.

My old friend Professor Harold Koh, now Dean of Yale Law School, probably deserves a large part of the credit for the theory that Jackson's *Youngstown* concurrence somehow has replaced *Curtiss-Wright* as the appropriate paradigm for foreign affairs cases in his prize-winning 1990 volume *The National Security Constitution*.

Like Lou Fisher and many others, Harold favors the "shared powers" concept of foreign affairs. I'm not fond of the term, not because I don't agree that many decisions in foreign affairs ultimately require the participation of more than one branch but because the specific role of each branch tends to be unique. The President "nominates" and "appoints," while the Senate may either consent to or veto the person nominated. The President has the exclusive power to speak to foreign governments on behalf of the nation, but before a treaty he has negotiated may bind the United States as conventional international law it must be approved by two-thirds of those Senators present and voting. I think it best not to merge these distinct roles with language that might suggest that the actual functions of each branch are interchangeable or "shared" in some way. It is not that Harold and Lou are necessarily *wrong* in this explanation, but rather that I fear the use of the term "shared powers" may promote sloppy thinking by readers less knowledgeable about the actual workings of government.

My real quarrel with Harold's scholarship involves his suggestion that there is some struggle going on between the Supreme Court's landmark 1936 *Curtiss-Wright* opinion and the concurring opinion of Justice Jackson in *Youngstown*. Candidly, I think this argument is silly. When properly understood, the two opinions are not at all in conflict. But before turning to that, let me put the issue in context by quoting from Harold's highly-acclaimed volume:

> At the Republic's birth, the Framers deliberately drafted a Constitution of shared powers and balanced institutional participation, fully aware of the risks that arrangement posed to the nation's international well-being. By mandating that separated institutions share powers in foreign as well as domestic affairs, the Framers determined that we must sacrifice some short-term gains for speed, secrecy, and efficiency in favor of the longer-term consensus that derives from reasoned interbranch consultation and participatory decision making. Although in the early years of the Republic, all three branches condoned a de facto transformation of the

[55] 343 U.S. 579.
[56] 1 H. REP'T 95-1283 at 24.

> original National Security Constitution from a scheme of congressional primacy to one of executive primacy, they never rejected the concept of power sharing and institutional participation . . . .[57]

He then goes on the explain how *Curtiss-Wright* radically changed the historic paradigm:

> In 1936, *Curtiss-Wright's* dicta boldly asserted the alternative vision of unfettered presidential management. But even as the Cold War raged, the 1947 National Security Act, *Youngstown*, and finally the post-Vietnam era framework statutes (e.g., War Powers Resolution) definitively rejected that vision as America's constitutional model for dealing with the outside world. Vietnam (and Watergate, as well, to the extent that it arose from Vietnam) then taught that even in a nuclear age, America would not conduct globalism at the price of constitutionalism. It is therefore ironic that the *Curtiss-Wright* model should now resurface . . . .[58]

In reality, throughout the Cold War the Supreme Court routinely relied upon *Curtiss-Wright* as the established foreign affairs paradigm, as it does today. If its status was weakened in any way by *Youngstown*, someone clearly forgot to tell the Court, which continues to cite *Curtiss-Wright* more than any other case dealing with foreign affairs more than half-a-century later.[59]

I was particularly amused by this passage of the Koh book:

> Critics on the right, in contrast, argue that to preserve our activist foreign policy, we must revise constitutionalism, abandoning the *Youngstown* vision in favor of *Curtiss-Wright*. Yet because many of these same critics also espouse the constitutional jurisprudence of original intent, they are forced to engage in revisionist history to contend that the Framers did not originally draft the Constitution to promote congressional dominance in foreign affairs.[60]

I think what I enjoyed the most was that, of the ten or so "[c]ritics on the right" he footnotes to this passage, he listed me *first* – well ahead of such distinguished scholars as former Yale Law School Dean Eugene Rostow and my University of Virginia colleague and mentor John Norton Moore. But, flattery aside, I've never been able to get Harold to come up with statements from men like Washington, Jefferson, Madison, Hamilton, or Jay supporting his theory that foreign and domestic affairs involved the same basic "sharing of powers" or that Congress was intended to be the senior partner in foreign affairs. Perhaps other witnesses here this morning can do so.

---

[57] HAROLD HONGKU KOH, THE NATIONAL SECURITY CONSTITUTION 211 (1990).
[58] *Id.* at 211-12.
[59] A WestLaw search reveals that *Curtiss-Wright* has been relied upon in Supreme Court cases in five of the last seven years. *See, e.g.*, *Pasquantino v. United States*, 544 U.S. 349, 369 (2005) ("In our system of government, the Executive is "the sole organ of the federal government in the field of international relations," *United States v. Curtiss-Wright* . . . .")
[60] *Id.* at 225.

I hope I've demonstrated the broad consensus among these key Founders that Congress and the Senate were to be excluded from many decisions in the foreign affairs realm, and the powers they were given that were viewed as *exceptions* to the broad grant of "executive Power" to the President and were thus intended to be construed strictly. In contrast, without any effort to document his assertion, Harold simply tells his reader "the first three articles of the Constitution expressly divided foreign affairs powers among the three branches of government, with Congress, not the president, being granted the dominant role."[61] And sadly, in the post-Vietnam era, this is the prevailing paradigm being taught in our universities and law schools.

Elsewhere in the volume, Professor Koh writes:

> This structural vision of a foreign affairs power shared through balanced institutional participation has inspired the National Security Constitution since the beginning of the Republic, receiving its most cogent expression in justice Robert Jackson's famous 1952 concurring opinion in *Youngstown*. Yet throughout our constitutional history, what I call the *Youngstown* vision has done battle with a radically different constitutional paradigm. This counter image of *unchecked executive discretion* has claimed virtually the entire field of foreign affairs as falling under the president's inherent authority. Although this image has surfaced from time to time since the early Republic, it did not fully and officially crystallize until Justice George Sutherland's controversial, oft-cited 1936 opinion for the Court in *United States v. Curtiss-Wright Export Corp.* As construed by proponents of executive power, the *Curtiss-Wright* vision rejects two of *Youngstown's* central tenets, that the National Security Constitution requires congressional concurrence in most decision on foreign affairs and that the courts must play an important role in examining and constraining executive branch judgments in foreign affairs.[62]

One wonders if Dean Koh has carefully *read* Justice Jackson's *Youngstown* concurrence, or the majority opinion in the case written by Justice Black. For both went to considerable lengths to emphasize that they were *not* endeavoring to constrain the powers of the President in dealing with the external world. At issue in that case was whether the President's "war powers" (in a conflict Jackson noted had not been approved by Congress[63]) authorized him to order the Secretary of the Interior to seize domestic steel mills – the *private property* of American citizens – in order to prevent a labor strike that

---

[61] *Id.* at 75.
[62] *Id.* at 72.
[63] In fairness, despite subsequent attacks from Republicans, Truman played the Korean conflict by the book. He repeatedly asked to address a joint session of Congress and had Secretary of State Acheson draft an authorization for the use of military force. But he decided not to push the idea when in consultation with congressional leaders he was repeatedly told th stay away from Congress and assured he had the power to send troops into hostilities pursuant to the Constitution and the UN Charter. *See* Robert F. Turner, *Truman, Korea, and the Constitution: Debunking the "Imperial President" Myth.* 19 HARV. J. L. & PUB. POL. 533 (1996).

might affect the availability of steel for the Korean War. (And keep in mind that the Fifth Amendment guarantees that "[n]o person shall . . . be deprived of . . . property, without due process of law . . . .")

There is no reason to believe that Justice Jackson was in any way hostile to *Curtiss-Wright* as the appropriate foreign policy paradigm. On the contrary, just two years before *Youngstown*, he wrote for the majority in *Johnson v. Eisentrager*:

> Certainly it is not the function of the Judiciary to entertain private litigation - even by a citizen - which challenges the legality, the wisdom, or the propriety of the Commander-in-Chief in sending our armed forces abroad or to any particular region. . . . The issue . . . involves a challenge to conduct of diplomatic and foreign affairs, for which the President is exclusively responsible. *United States v. Curtiss-Wright Corp* . . . .[64]

And consider this excerpt from Justice Black's majority opinion in *Youngstown*:

> The order cannot properly be sustained as an exercise of the President's military power as Commander-in-Chief of the Armed Forces. The Government attempts to do so by citing a number of cases upholding broad powers in military commanders engaged in day-to-day fighting in a theater of war. Such cases need not concern us here. Even though 'theater of war' be an expanding concept, we cannot with faithfulness to our constitutional system hold that the Commander in Chief of the Armed Forces had the ultimate power as such to take possession of private property in order to keep labor disputes from stopping production. This is a job for the Nation's lawmakers, not for its military authorities.[65]

Similarly, Justice Jackson in *Youngstown* was very deferential to presidential power with respect to the external world:

> [N]o doctrine that the Court could promulgate would seem to be more sinister and alarming than that a President whose conduct of foreign affairs is so largely uncontrolled, and often is even unknown, can vastly enlarge his mastery over the internal affairs of the country by his own commitment of the Nation's armed forces to some foreign adventure. . . .
> That military powers of the Commander in Chief were not to supersede representative government of internal affairs seems obvious from the Constitution and from elementary American history. . . . Such a limitation [the Third Amendment] on the command power, written at a time when the militia rather than a standing army was contemplated as a military weapon of the Republic, underscores the Constitution's policy that Congress, not the Executive, should control utilization of the war power as an instrument of domestic policy . . . .

[64] 339 U.S. 763 (1950).
[65] 343 U.S. 579, 587 (1952) (bold emphasis added).

> We should not use this occasion to circumscribe, much less to contract, the lawful role of the President as Commander in Chief. I should indulge the widest latitude of interpretation to sustain his exclusive function to command the instruments of national force, at least when turned against the outside world for the security of our society. But, when it is turned inward, not because of rebellion but because of a lawful economic struggle between industry and labor, it should have no such indulgence. . . . What the power of command may include I do not try to envision, but I think it is not a military prerogative, without support of law, to seize person or property because they are important or even essential for the military or naval establishment.[66]

Even more fundamentally, in *Youngstown* Justice Jackson actually cited *Curtiss-Wright* as authority, but then explained: "That case does not solve the present controversy. It recognized internal and external affairs as being in separate categories . . . ."[67] And as both Justice Black and Jackson repeatedly emphasized, *Youngstown* was an "internal affairs" case.

That is also the consensus of scholars like Professor Louis Henkin, who in *Foreign Affairs and the Constitution* noted:

> *Youngstown* has not been considered a "foreign affairs case." The President claimed to be acting within "the aggregate of his constitutional powers," but the majority of the Supreme Court did not treat the case as involving the reach of his foreign affairs power, and even the dissenting justices invoked only incidentally that power or the fact that the steel strike threatened important American foreign policy interests.[68]

Consider also the reaction of Justice Rehnquist, joined by Chief Justice Burger and two other members of the Court, in the 1979 dispute over President Carter's constitutional power to terminate the mutual security treaty between the United States and Taiwan. Senator Goldwater had urged the Court to decide the case on *Youngstown*, but Rehnquist wrote:

> The present case differs in several important respects from *Youngstown* . . . cited by petitioners as authority both for reaching the merits of this dispute and for reversing the Court of Appeals. In *Youngstown*, private litigants brought a suit contesting the President's authority under his war powers to seize the Nation's steel industry, an action of profound and demonstrable domestic impact. . . . Moreover, as in *Curtiss-Wright*, the effect of this action, as far as we can tell, is "entirely external to the United

[66] *Id.* at 642, 644, 645.
[67] *Id.* at 637 n.2 (bold emphasis added).
[68] HENKIN, FOREIGN AFFAIRS AND THE CONSTITUTION 341 n.11.

> States, and [falls] within the category of foreign affairs.[69]

Others may disagree, but my own sense is that *The National Security Constitution* is not a particularly useful contribution to the literature in this highly-specialized field. Indeed, my strong sense is that when the book was written Harold was unaware of many of the materials I have mentioned earlier from Washington, Jefferson, and all three authors of the *Federalist* papers.

Post-Vietnam Congressional Usurpation of Presidential Power and Its Consequences

Mr. Chairman, the FISA statute needs to be understood in the context of a period of congressional assault on the constitutional power of the executive that developed during the heat of the VietnamWar debates. We can quarrel about how many legislators believed they were defending the Constitution from another "imperial president" and how many realized they were violating their oaths of office, but in the end that doesn't much matter. The reality is that Congress took advantage of the flow of public opinion as the Vietnam War became unpopular, the weakness of Richard Nixon following Watergate, and the reality that Gerald Ford had not even been elected to the position of *Vice* President and had no clear pubic constituency. A very nice but largely (in this field) clueless Jimmy Carter then came to Washington, anxious to work with Congress to bring an end to intelligence abuse and restore power where he probably honestly assumed it belonged.

The earliest reference I have found proposing that Congress challenge presidential authority over foreign intelligence was in a 1969 book by radical activist Richard Barnet, a founder of the Institute for Policy Studies, who wrote:

> Congressmen should demand far greater access to information than they now have, and should regard it as their responsibility to pass information on to their constituents. Secrecy should be constantly challenged in Congress, for it is used more often to protect reputations than vital interests. There should be a standing congressional committee to review the classification system and to monitor secret activities of the government such as the CIA.[70]

Revelations a few years later of abuses in the intelligence area set the stage for that to become a reality.

Were there in fact "abuses" in the Intelligence Community? Anyone who followed the Church and Pike Committee hearings knows there were. But even Frank Church ultimately admitted that the CIA had not been a "rogue elephant" (as he had initially

---

[69] *Goldwater v. Carter* 444 U.S. 996 (1979) (bold emphasis added).
[70] RICHARD J. BARNET, THE ECONOMY OF DEATH 178-789 (1969).

charged), and that virtually every activity of which he disapproved had been ordered by a president or senior policy official.

President Franklin D. Roosevelt had bypassed his attorney general in 1936 and directly ordered J. Edgar Hoover to start "spying" on Americans thought possibly to be connected with Communism or Fascism, and Hoover had on his own initiative banned FBI "black bag" jobs nearly a decade before the Church Committee hearings took place.[71] Most of the abuses had already been investigated and made public by the Attorney General before the hearings even began. And some of the sensationalized charges in the end turned out to be largely unfounded.

For example, most people who followed the hearings in the press came away with the idea that the CIA routinely went around "assassinating" foreign leaders who would not do what America demanded. In fact, when the Church Committee published its massive volume on the subject,[72] it admitted it had not found a *single* case in which the CIA had ever assassinated anyone. And Directors of Central Intelligence Richard Helms and William Colby had each issued orders that no one connected with the CIA would have anything to do with assassination long before the hearings began.[73]

What about Fidel Castro? Yes, at the instructions of Presidents Eisenhower and Kennedy the CIA did make several plots to dispatch the Cuban dictator with extreme prejudice. But given Castro's unlawful intervention in several Latin American countries, one might make a plausible case that a use of lethal force was permissible as an act of collective self-defense under Article 51 of the UN Charter. There was also a decision made to kill the Congo's Patrice Lumumba, but before any action was taken he was arrested by his own government and killed soon thereafter by rival leftist guerrillas.[74] In all of the other cases investigated by the Committee, the CIA was cleared of wrongdoing.

What about allegations of "spying" on Dr. Martin Luther King and anti-war leaders? The charges appear to have been true. But as the 1978 HPSCI report on FISA observed, most of the truly objectionable disclosures involved "domestic" targets.[75] The Bush administration has agreed to obtain warrants from the FISA Court any time U.S. persons in this country are targeted for surveillance, so that problem is not in dispute. (In reality, with the extensive oversight mechanisms already in place within the executive branch, it is highly unlikely that any politician would even consider repeating those errors of the past. NSA alone is said to have a staff of 100 people in the office of its inspector general.)

---

[71] 2 S. Rep't No. 94-755 at 24; 3 *id.* at 355 (1976)

[72] ALLEGED ASSASSINATION PLOTS INVOLVING FOREIGN LEADERS, S. REP. NO. 94-465 (1975).

[73] *See* Robert F. Turner, *It's Not Really "Assassination" Legal and Moral Implications of Intentionally Targeting Terrorists and Aggressor-State Regime Elites*, UNIVERSITY OF RICHMOND LAW REVIEW, vol. 37, March 2003 at 791-98.

[74] S. REP. NO. 94-465 at 256.

[75] 1 H. REP'T No. 85-1283 at 21.

But in response to public perceptions of CIA assassins running loose and with weakened presidents in the White House, Congress passed a series of new laws claiming powers all three branches had historically recognized belonged exclusively to the executive.

Five years before FISA was enacted, Congress overrode President Nixon's veto to enact the War Powers Resolution. The constitutional shortcomings of the War Powers Resolution were expressed eloquently by Senate Majority Leader George Mitchell, who on May 19, 1988, declared on the Senate floor:

> Although portrayed as an effort "to fulfill"—not to alter, amend or adjust—"the intent of the framers of the U.S. Constitution," the War Powers Resolution actually expands Congress' authority beyond the power to declare war to the power to limit troop deployment in situations short of war....
>
> By enabling Congress to require—by its own inaction—the withdrawal of troops from a situation of hostilities, the resolution unduly restricts the authority granted by the Constitution to the President as Commander in Chief.
>
> ...[T]he War Powers resolution does not work, because it oversteps the constitutional bounds on Congress' power to control the Armed Forces in situations short of war and because it potentially undermines our ability to effectively defend our national interests.
>
> The War Powers Resolution therefore threatens not only the delicate balance of power established by the Constitution. It potentially undermines America's ability to effectively defend our national security.[76]

Senator Mitchell might have added that the highly partisan September 1983 congressional debates over extending the U.S. peacekeeping force in Beirut, Lebanon – a deployment that did not even arguably infringe upon the power of Congress to "declare war" – sent a signal to Islamic terrorists that America was "short of breath" and would abandon their commitment if more casualties were experienced. Indeed, shortly after the Congressional debate, we intercepted a message between two radical groups saying that if they killed 15 Marines, the rest would "go home." Presumably, the fact that congressional leaders had announced they would reconsider the vote by which the mission had been extended for 18 months if there were any more casualties might have been a factor in that analysis. In any event, a few days later, on October 23, 1983, 241 sleeping Marines were killed by a terrorist truck bomb. As predicted, we did bring the rest home.[77] And Osama bin Laden later said that our quick withdrawal after the attack had persuaded him that Americans were unwilling to accept casualties – which in turn

[76] CONGRESSIONAL RECORD, May 19, 1988.

[77] For a discussion of congressional responsibility for this tragedy, *see* P.X. Kelley & Robert F. Turner, *Out of Harm's Way: From Beirut to Haiti, Congress Protects Itself Instead of Our Troops*, WASH. POST, Oct. 23, 1994 at C2; and ROBERT F. TURNER, REPEALING THE WAR POWERS RESOLUTION 141-42.

just might have been a factor in his decision to attack the World Trade Center and other American targets on September 11, 2001.[78]

It seems very clear as well that FISA itself was a contributing factor to the success of the 9/11 attacks. I'm sure everyone here recalls the compelling congressional testimony of FBI lawyer Colleen Rowley, who was named one of *Time* magazine's "Persons of the Year" in 2002 because of her scathing memo to FBI Director Bob Mueller denouncing the incompetent bureaucrats in the FBI's Office of General Counsel who had repeatedly refused to even process her requests for a FISA warrant so field agents could examine the laptop computer of Zacharias Moussaoui. Most Americans never did learn the reason Rowley's requests had been denied. There was simply no evidence that Moussaoui was an officer, employee, member, or agent of al Qaeda or any other foreign terrorist organization. He was what we call a "lone wolf," a "sympathizer" or perhaps a "fellow-traveler." But in its wisdom, Congress made it a *felony* for anyone in the Intelligence Community to engage in surveillance of Moussaoui without a FISA warrant – and it also made it illegal for the FISA Court to issue such a warrant in Moussaoui's case. What those contemptible FBI lawyers had done was to obey the law passed by Congress.

If anyone doubts that FISA was intended to make such surveillances unlawful, I would urge you to read the 1978 HPSCI report of FISA. On page 34 it emphasizes that the term "agent of a foreign power" intentionally excluded "mere sympathizers, fellow-travelers, or persons who may have merely attended meetings of the group . . . ."[79]

I honestly don't know if FBI surveillance of Moussaoui prior to September 11, 2001, would have led to clues that might have prevented the attacks and saved 3000 lives. I do know that General Michael Hayden, who served as Director if the National Security Agency for more than six years starting in 1999 and has a reputation for the highest integrity, has publicly stated with respect to the Terrorist Surveillance Program so many legislators struggled so hard to destroy: "Had this program been in effect prior to 9/11, it is my professional judgment that we would have detected some of the 9/11 al Qaeda operatives in the United States, and we would have identified them as such."[80] He did not connect the dots and suggest that, once having identified al Qaeda terrorists in our midst we might have monitored their activities and even prevented the attacks, but that's not an unreasonable conclusion.

In 2004, Congress quietly amended FISA to address the "lone wolf" problem. Some might view that as a bit late – 3000 lives too late. In fairness, of course, no one in Congress expected that FISA would make it easier for foreign terrorist to slaughter thousands of innocent people in this country, and certainly no one in Congress wished for such a result. But one of the reasons John Locke explained that foreign affairs needed to

---

[78] Scott Dodd & Peter Smolowitz, *1983 Beirut Bomb Began Era of Terror*, DESERET NEWS, Oct. 19, 2003, available on line at: http://deseretnews.com/dn/view/0,1249,515039782,00.html (bold italics added). *See also.*, Brad Smith, *1983 Bombing Marked Turning Point In Terror: The U.S. reaction to the Beirut attack set off a chain of events, some say,* TAMPA TRIB., October 23, 2003.

[79] 1 H. REP'T NO. 95-1283 at 34.

[80] A copy of General Hayden's address to the National Press Club on January 23, 2006, can be found on line at: http://www.fas.org/irp/news/2006/01/hayden012306.html.

be entrusted to the executive was because it was not possible to anticipate all of the changed circumstances that might occur during negotiations, war, or other events by "antecedent, standing, positive laws" – and thus this business of necessity had to be entrusted to the executive "to be managed for the public good."[81]

Indeed, the congressional assault on presidential powers has given us textbook examples of this principle at work. In May 1973, Congress snatched defeat from the jaws of victory in Indochina (in the process consigning millions of human beings we had repeatedly pledged to assist by treaty and statute to death and tens of millions of others to a Communist tyranny that decades later still ranked among the "worst of the worst" human rights violators in the world) by cutting off all funds for combat operations "in the air, on the ground, or off the shores" of North Vietnam, South Vietnam, Laos or Cambodia. Two years later to the month, Cambodian forces seized the American merchant ship *S.S. Mayaguez* and took 42 crewmembers to an island. When Senator Frank Church was later asked whether he was upset that President Ford had repeatedly violated the amendment he had sponsored by using force in the air, on the ground, and off the shores of Cambodia to rescue those Americans, he explained that Congress had not "intended" to prevent something like *that*.

Then there was the statute that authorized the elder President Bush to use force in Operation Desert Storm in 1991. Congress carefully drafted the statute to prevent the president from using force for any objective beyond ejecting Iraqi forces from the territory of Kuwait. No one anticipated that General Norman Schwarzkopf would pull off a brilliant "left hook" that would leave Saddam's Revolutionary Guard fleeing across the desert with only minimal American casualties, and not a few congressional Democrats who had voted to deny Bush any authority to enforce the UN Security Council decision quickly denounced the president as a wimp for failing to go all the way to Baghdad to exploit the great victory and bring an end to Saddam's rule.

We don't have to go back years to find examples of serious harm being done to our national security by a Congress that usurped presidential power and then failed to anticipate the consequences of its actions. Time and again, the 1998 HPSCI report of FISA emphasized that that the new statute would only regulate "electronic surveillance conducted *within the United States* for foreign intelligence purposes."[82] The report explained: "The committee has explored the feasibility of broadening this legislation to apply overseas, but has concluded that certain problems and unique characteristics involved in overseas surveillance preclude the simple extension of this bill to overseas surveillance."[83]

And yet, if leaks in the newspapers are to be believed – and some are specifically attributed to congressional sources – changes in technology have led the FISA Court to declare that communications between bin Laden in Pakistan and his top lieutenants in Afghanistan can no longer be intercepted without a FISA warrant if they happen to pass

[81] JOHN LOCKE, SECOND TREATISE ON CIVIL GOVERNMENT § 147 (1689).
[82] H. REP'T NO. 95-1283 at 24. *See also, id.* at 26, 36, and other references.
[83] *Id.* at 27.

through an Internet switch in northern Virginia or Sillicone Valley. Because of this, we are reportedly getting twenty-five percent less intelligence this year than we got last year. Congress has not only usurped the constitutional powers of the president, but in the process it has given a special gift to al Qaeda by immunizing communications that clearly were not intended to be affected by FISA. And yet I am told that more than four House Democrats out of five voted to prevent this situation from being corrected.

If you want to find other horror stories about how Congress through FISA is undermining America's ability to protect the lives of our people, read the testimony and statements of Director of National Intelligence McConnell and other senior officials. Responding to a question from Senator Bond during his May 1 appearance before the Senate Select Committee on Intelligence, DNI McConnell declared that, "under the construct today, the way the definitions have played out and applied because technology changes, *we're actually missing a significant portion of what we should be gathering*." Kenneth Wainstein, the Assistant Attorney General for National Security, noted during that same hearing that the current interpretation of FISA prevents the government from collecting intelligence with non-U.S. persons who are temporarily visiting the United States and who we *know* have important foreign intelligence information that might well help us prevent terrorist attacks. But because we can't clearly connect that person – who might be a "tourist" from Pakistan or Iran – as an "agent" of a "foreign power," we are helpless. Does Congress really place greater value on the privacy interests of foreign visitors than it does on the lives of American citizens?

In his August 6 letter to Senators Reed and McConnell, the DNI noted that because of FISA the Intelligence Community was "diverting scarce counterterrorism analysts who speak the languages and understand the cultures of adversaries to compiling lengthy court submissions to support probable cause findings on an individualized basis by the FISA Court in order to gather foreign intelligence from foreign terrorists located overseas." He added: "This is an unacceptable and irresponsible use of Intelligence Community resources." We have a horrible shortage of skilled linguists, and rather than allow the DNI to prioritize their assignments Congress is taking them away from the task of trying to find bin Laden and prevent attacks on America so they can prepare paperwork to persuade the FISA Court that perhaps we ought to be keeping an eye on our enemies during a war that Congress has authorized. If you people were in business during World War II, I suspect we would all be speaking German or Japanese today.

Conclusions

Mr. Chairman, I have gone on far too long. I would not have done so were the stakes involved not so serious, and were not my frustration over the ignorance and misinformation that has clouded this debate so great. Let me try to make a few final observations and bring things to a close.

FISA Was Essentially a Gentleman's Agreement Between Congress and President Carter

When Congress enacted FISA in the face of unanimous views to the contrary by those who had expressed an opinion in the other two branches of our government, I'm sure most members believed their decision was "law" and would bind future presidents. But a careful reading of the hearing record suggests that that was not the view of the Carter Administration (which, as discussed, had taken the position that there was a foreign intelligence exception to the warrant requirements of the Fourth Amendment). Consider this excerpt from the HPSCI testimony of Attorney General Griffin Bell:

> [C]landestine intelligence activities, by their very nature, must be conducted by the executive branch with the degree of secrecy that insulates them from the full scope of these review mechanisms. Such secrecy in intelligence operations is essential if we are to preserve our society, with all its freedoms, from foreign enemies. . . .
> [T]he current bill recognizes no inherent power of the President to conduct electronic surveillance, and I want to interpolate here to say that *this does not take away the power of the President under the Constitution.* It simply, in my view, is not necessary to state that power, so there is no reason to reiterate or iterate it as the case may be. It is in the Constitution, whatever it is. *The President, by offering this legislation, is agreeing to follow the statutory procedure.*[84]

Now this statement may be subject to more than one interpretation, but it sounds to me like the Attorney General was asserting that the president had independent constitutional power to conduct foreign intelligence, and affirmed the truism that a mere legislative statute can not take away a constitutional power – precisely the unanimous conclusion of the FISA Court of Review nearly a quarter-century later. And then he goes on to say that the statute will nevertheless be followed because the president – despite his constitutional power to act outside of FISA – was "agreeing to follow the statutory procedure." There may be other interpretations, but that to me is the most reasonable one.

And if that interpretation is correct, then the foundation of FISA from the start was not a lawful and binding Act of Congress at all but rather a usurpation of presidential

[84] Testimony of Attorney General Griffin Bell, FOREIGN INTELLIGENCE ELECTRONIC SURVEILLANCE, HEARINGS BEFORE THE SUBCOMMITTEE ON LEGISLATION OF THE PERMANENT SELECT COMMITTEE ON INTELLIGENCE, HOUSE OF REPRESENTATIVES, January 10, 1978 at 14-15 (emphasis added).

constitutional power that as a matter of U.S. constitutional law was void, but which the sitting president had nevertheless agreed as a matter of policy to observe. If that is true, then if Congress insists on trying to control this area it must come up with language that the current president will also be willing to accept. For it is axiomatic that neither Congress by itself nor Congress in cooperation with a sitting president can amend the Constitution so as to deny future presidents the full use of their independent powers.

Why President's Like FISA

I've been out of the intelligence business for nearly twenty-four years, and while I have many friends still working in the Intelligence Community I don't pretend to speak for them. But my own sense is that most administrations basically *like* FISA. Certainly many prosecutors and law enforcement officials do, because if surveillance is carried out pursuant to a FISA judicial warrant and authorizing statute they don't have to worry as much about whether evidence acquired in the process will be found admissible in a criminal trials. And in a setting where speed and dispatch are not essential, it also adds another layer of review to ensure that the right thing is being done.

So even though I do not believe that Congress has the constitutional power to demand secret information from the president or to compel him to conduct foreign intelligence operations in accordance with the statute, with appropriate revisions I can see FISA being accepted and observed on the basis of an understanding that it is mutually convenient to do so. But if Congress continues to stonewall, and refused even to correct the obvious technical problems that are preventing NSA from monitoring communications between foreign terrorists outside of this country – communications FISA was clearly not intended to govern – in my view the president would be derelict in his duty if he did not authorize a more robust program of foreign intelligence collection outside of FISA. And if America gets hit again by a major terrorist attack before the next election, were I a legislator who had voted to undermine efforts by our Intelligence Community to gather intelligence on al Qaeda and its affiliates I think I might want to get my resume in order.

Confusing Law Enforcement Search Warrants and the Business of Foreign Intelligence Collection

With the caveat again that I have been out of the intelligence business for nearly twenty-five years, I must nevertheless say that I don't understand this insistence on imposing a warrant requirement, complete with "probable cause," on the collection of foreign intelligence information. In law enforcement, you have evidence that a crime has been committed or is about to be committed and you search for evidence to identify wrongdoers and bring them to justice. In that process, the Fourth Amendment quite properly limits the extent to which police or other government authorities may infringe upon the reasonable expectations of privacy of citizens and others in the community. Certain activities are prohibited in the absence of probable cause that an individual has committed or intends to commit a criminal act.

There are occasions in the intelligence business where a similar situation occurs and law enforcement personnel are brought in to try to collect the necessary evidence to win a conviction. But much of the time, the task of the Intelligence Community is to look around and try to identify individuals who may be foreign spies or agents. Historically, much of that difficult and often thankless task has involved trying to make associations – who spends a lot of time with a known spy or terrorist, who calls his telephone, who socializes with him time and again. No one is punished for telephoning a foreign agent or terrorist. Spies and terrorists do things other than steal secrets and blow up buildings, and there is not the slightest thing wrong with innocently but repeatedly communicating with an enemy spy you have no idea is a spy. Perhaps an eBay transaction will lead to a series of e-mails, or the illness of a mutual friend will prompt repeated phone calls. Our intelligence officers patiently look for and check out lead after lead, and sometimes they get lucky and identify another spy or terrorist.

Technology can greatly assist in this business. If NSA can get access to telephone records of millions and millions of customers, sophisticated programs can search and find which numbers are time and again connecting to numbers known or suspected to be used regularly by other terrorists. Again, no one is sent to jail for talking on the telephone with a covert enemy agent. Perhaps the calls are between teenagers in both houses who have fallen in love and are totally oblivious to the reality that one of their parents is a terrorist. They often lead to dead ends, but such leads are worth checking.

Professor Philip Bobbitt, a distinguished scholar and Director of the Columbia University Center for National Security, recently published an outstanding op-ed in the *New York Times* that is worth quoting. He explained:

> It made sense to require that the person whose communications were intercepted be a spy when the whole point of the interception was to gather evidence to prosecute espionage. This makes much less sense when the purpose of the interception is to determine whether the person is in fact an agent at all. This sort of communications intercept tries to build from a known element in a terror network — a person, a telephone number, a photograph, a safe house, an electronic dead-drop — to some picture of the network itself. By crosshatching vast amounts of information, based on relatively few confirmed elements, it is possible to detect patterns that can expose the network through its benign operations and then focus on its more malignant schemes.
>
> For this purpose, warrants are utterly beside the point.[85]

Philosophers sometimes ask whether a tree falling on a desert island makes a noise.[86] In a similar vein, one might ask whether a computer that in a nanosecond scans my

[85] Philip Bobbitt, *The Warrantless Debate Over Wiretapping*, N.Y. TIMES, Aug. 22, 2007 at A19.

[86] The answer, it has always seemed to me, depends upon whether one defines "noise" as a series of vibrations created by the falling tree, or the impulse transmitted to the human brain when the ear receives those vibrations. But that's not my point in making this comparison this morning.

anonymous telephone records to see if I have been communicating with known terrorists has violated my legitimate privacy rights? In more than 99.999 percent of the searches, no relationship will be found and no human being will be told anything about me. When in May of last year *USA Today* reported that some telephone companies had provided telephone records to the NSA – without any names, addresses, or content information about the calls – some civil libertarians went ballistic. Senator Patrick Leahy asked: "Are you telling me tens of millions of Americans are involved with al-Qaeda?"[87]

Obviously, Senator Leahy knows that no one is suggesting that every record searched belongs to a suspected Qaeda operative. He is either being silly about a very serious matter or playing partisan politics. We search millions of records to try to identify a small number that show a pattern of communicating with known or suspected terrorists in order to identify possible leads that may result in preventing the next major terrorist attack.

As I see it, this is no more a violation of my "privacy rights" than is the common practice (as I understand it) of having government computers scan my fingerprints – and they presumably have lots of them, starting with the ones I submitted while earning my Boy Scout fingerprinting merit badge half-a-century ago to my military records and the various times I was printed in connection with government jobs and security clearances – along with those of millions of other Americans. Am I really "injured" when their computer scans over my prints in trying to find a match to the ones found on a murder weapon? Unless there is at least a partial match, no human being even sees my name. I just don't see the problem here.

I stand in line patiently at airports because I want my government to make it difficult for terrorists to hijack my plane or blow it up. I am *glad* the FBI is scanning vast digital files that include my fingerprints when it searches for criminals, because I know searching more records should increase the chance of finding a match and I want to get criminals off the street. And I would be very glad to learn that the government is having a computer examine my phone and e-mail connection records if there is even a slight chance that the process will expose a real terrorist and prevent him from killing me, my family, or other innocent human beings.

Unless one is actually involved in criminal activity or terrorism, to say the privacy intrusion associated with these "searches" is *de minimis* is a gross overstatement. The Supreme Court held years ago that there is no reasonable expectation of privacy concerning such telephone records,[88] but even were there a recognized privacy interest it would obviously pale beside the government's interest in preventing terrorist attacks. Anyone who doubts that has forgotten the events of September 11, 2001. And when Members of Congress – or witnesses at congressional hearings, for that matter – make

---

[87] Susan Page, *NSA Secret Database Report Triggers Fierce Debate in Washington*, USA TODAY, May 11, 2006 at A1.

[88] *Smith v. Maryland*, 442 U.S. 735 (1979) (upholding the use of pen registers that record numbers of phones that communicate with a particular telephone without a warrant).

alarmist pronouncements calculated to anger the public they serve neither themselves nor their constituents. We have to make enough really difficult calls in trying to reach the right balance between privacy and safety without being led astray by unwarranted hysteria.

Revising FISA

I was absolutely shocked to read in *Newsweek* that 82 percent of House Democrats had voted against the "Protect America Act" prior to going on recess.[89] As I read the statute, it was an emergency six-month fix to permit our Intelligence Community to resume intercepting communications by foreign terrorists outside this country until Congress could return from a month-long recess and enact a more permanent fix. It may not have been perfect, but Congress was unwilling to stay in town long enough to try to make it perfect.

I'm not here as an expert on the details of proposed revisions to FISA. I'm sure you have had, or will soon have, an opportunity to discuss the details with people involved in the drafting who can give you much more authoritative answers that I could.

I have of course read the testimony of the DNI and Mr. Wainstein of the Justice Department, and I find both entirely compelling. Making FISA technology neutral and focusing our limited resources on protecting the civil liberties of U.S. persons in this country makes tremendous sense to me. The key issue ought to be who is being *targeted*, and the fact that bin Laden places a telephone call to Joe Sixpack in Peoria (about whom the government knows nothing) ought not require NSA monitors to unplug their headphones. If I telephone someone in this country whose phone calls the government has a lawful right to record – e.g., if they have a judicial criminal warrant – then my voice can lawfully be recorded. And if I begin the conversation by confessing to having committed a crime or announcing an intention to do so, the government can introduce that tape into court against me without needing a separate prior warrant in my name. My privacy rights are essentially "collateral damage" in the reasonable effort to get information on the target of the surveillance. Why on earth should we apply a more difficult standard to intercepting communications of foreign enemies who wish to murder large numbers of Americans than we do to white collar criminals in this country?

It seems to me that Congress ultimately has two choices. You can work with the president to try to find a mutually agreeable solution – one that will give him the benefit of knowing that foreign intelligence information will likely be admissible in a court of law, without in the process preventing him from taking the necessary measures to collect the intelligence needed to prevent the next catastrophic terrorist attack – or you can play hardball, intentionally preventing our Intelligence Community from collecting essential foreign intelligence information, until either we are attacked again and your constituents vote you out of office or the president simply decides to ignore FISA.

---

[89] Jonathan Alter, *I Know What You Did Last Summer*, NEWSWEEK, Aug. 27, 2007, available on line at: http://www.msnbc.msn.com/id/20226453/site/newsweek/.

In *Federalist* No. 41, James Madison cautioned:

> The means of security can only be regulated by the means and the danger of attack. They will, in fact, be ever determined by these rules, and by no others. It is in vain to oppose Constitutional barriers to the impulse of self-preservation. It is worse than in vain; because it plants in the Constitution itself necessary usurpations of power, every precedent of which is a germ of unnecessary and multiplied repetitions.[90]

In this instance, a decision by the president to ignore FISA would not involve a usurpation of power. For as I have demonstrated, he would merely be reclaiming authority that the Founding Fathers expressly said he had, that other presidents have exercised since the earliest days of our country, that Congress itself has recognized by statute to exist, and that every court to consider the issue – including a unanimous opinion by the appellate court Congress created to oversee FISA decisions – had affirmed. When the facts get out, this is not a fight that Congress is likely to win in the struggle for public opinion.

As a political matter, it is very much in your interest to fix permanently the inadvertent consequences of technological changes and outdated statutory language that prevents our Intelligence Community from listening to every word we can intercept from Osama bin Laden and his associates in other countries. If the American people learn what you have done, the approval rating of Congress –which the August 13-16 Gallup Poll reports has now dropped to 18 percent (a 38 percent drop since May), with a 76 percent disapproval rate[91] – may fall still further before next year's elections.

Mr. Chairman, lest there be any misunderstanding, I have the highest respect for this institution and its members. I worked as a staff member in the legislative branch for five years, and as a student of the Constitution I understand the critically important role assigned to Congress in maintaining our freedoms. If my testimony this morning seems critical of Congress, that is intentional. For the reasons I have tried to carefully explain, I believe Congress is violating the Constitution and endangering the safety of the American people. I come from the University of Virginia, whose founder, Thomas Jefferson, wrote in his *Summary View of the Rights of British America*: "Let those flatter who fear; it is not an American art."[92] America is at war, and the stakes in this debate are far too serious for anything short of honest and full candor.

Focus on Minimization Issues

I would leave you with but one final thought. As you seek to find a workable solution to this very difficult problem, consider the oath you took upon assuming the important

---

[90] THE FEDERALIST, No. 41 at 269-70 (Jacob E. Cooke, ed. 1961), available on line at: http://www.yale.edu/lawweb/avalon/federal/fed41.htm.

[91] A series of recent job rating polls on Congress may be found on line at: http://www.pollingreport.com/CongJob.htm.

[92] Available on line at: http://www.yale.edu/lawweb/avalon/jeffsumm.htm.

position of trust and honor that has been bestowed upon your by your constituents – a solemn oath to support our Constitution. It is our supreme law. And in this instance, it is absolutely clear that Congress has grossly usurped presidential power. In so doing, it has contributed to the success of one major terrorist attack and may soon bear responsibility for others if no quick solution is found.

My own recommendation is that you focus on the later stages of the intelligence process. At least with respect to activities outside this country, trying to ascertain the intentions and capabilities of our enemies in a war you have authorized, don't focus on how the president decides to *collect* intelligence. Just as in war there is inevitable "collateral damage" and lives are lost because of inaccurate intelligence or imperfect execution, accept the fact that to do its job effectively and protect our nation from catastrophic terrorist attacks some private information about innocent Americans will inevitably be swept up. That's not ideal, but it is okay – and it is far better that the alternative of allowing our enemies to kill thousands of our fellow citizens so that no U.S. person's privacy will be disturbed.

I would urge you instead to work with the DNI and others who understand these issues and focus on the *retention* and *dissemination* phases of the process. I don't have access to the latest minimization rules because they are presumably still at least in part classified. But having worked with those drawn up by Attorney General Levy when I served in the White House in the early 1980s, I can tell you that they work. And rather than compromise a vigorous collection effort, let's concentrate on making as certain as reasonably possible – consistent with operational success – that when information about specific U.S. persons that does not constitute legitimate foreign intelligence information is intercepted, it is identified, isolated, and ultimately destroyed.

Such measures may impose some costs on the Intelligence Community, as they will involve a certain number of man-hours over a continuing period of time. But my strong sense from reading the testimony of senior executive branch officials is that they favor these procedures, and they, too, are committed to trying to protect the civil liberties of U.S. persons.

The Stakes Are High for Congress Too

Admittedly, to date the president's critics have scored some major points by accusing him of being insensitive to civil liberties and charging him with breaking the law. Indeed, the administration has done a truly *atrocious* job of explaining its position in this struggle to the American people. But their case is a strong one – supported by revered names like Washington, Jefferson, Hamilton, Madison, Jay, and Chief Justice John Marshall himself – as well by past legislative statues and every court to address the issue, including the unanimous appellate court established by FISA itself.

If you refuse to seek a reasonable and workable compromise and the American people eventually learn the truth, you will lose. I think you will lose big. The American people may sometimes be uninformed and even misinformed, but they are not stupid. And they

will not likely forgive you if they learn that Congress has been playing politics with the lives and safety of their families and friends. If before this issue is resolved, America is hit by another catastrophic terrorist attack, maintaining your 18 percent public approval rating may prove to be but a pipe dream. The clock is running, our Intelligence Community is anxious to get back to business, and the ball is in your court.

Thank you, Mr. Chairman. That concludes my prepared statement.

Mr. CONYERS. Thank you, Dr. Turner.

We turn now to Morton Halperin, attorney, who served in Departments of Defense, State and the National Security Council during President Clinton, President Nixon and President Johnson, and was instrumental in the formulation of FISA in 1978.

He is currently Director of U.S. Advocacy for The Open Society Institute and a fellow at the Center for American Progress.

Welcome again to the Committee.

TESTIMONY OF MORTON H. HALPERIN, DIRECTOR OF U.S. ADVOCACY, OPEN SOCIETY INSTITUTE

Mr. HALPERIN. Thank you, Mr. Chairman. It is a great pleasure to be back.

I need to report that I have not acquired a law degree, although I still hope that is some time in my future.

It is a pleasure to be back here again before this Committee. I last testified on this subject before the Committee in a hearing in 1978 in which we debated exactly the same issues.

And I think I want to touch on this question of whether FISA is constitutional or not and whether it is appropriate or not.

The fact is every court that has considered FISA has held it to be constitutional. It continues to be the case that no court has found a warrantless tap for national security purposes to be unconstitutional because that question became moot with the enactment of FISA.

I think the real issue for me is to look at the Constitution and to note that it is based on a notion of separation of power. The Congress has a role. The President has a role. And the court has a role.

And the genius of FISA when it was enacted and reported out by this and other Committees with very broad, bipartisan support is that it took account of the obligations and responsibilities of the three branches and of the need both to protect the rights of American citizens and deal with the requirements of national security.

At the end of the day, the intelligence community leaders and many leaders of the civil liberties community said this bill has our support. It is an appropriate balance.

And that support from all those elements was, in my view, critical to the extraordinary success of FISA, which has been testified to by a succession of CIA directors, NSA directors, directors of national intelligence and other senior officials from every Administration since FISA was enacted.

FISA has permitted the intelligence community to do what it needed to do, but to do it in a way that had the support of the American people, that had the support of the courts. And the FISA court fulfilled its role by not always approving warrants, but by providing the support that was needed to enable this program to go forward.

We need to get back to that bipartisan support. We need to get back to a situation where most Americans support the Foreign Intelligence Surveillance Act because they understand what it does and they recognize that there is a court and a Congress monitoring the actions of the executive branch.

Where the system has fallen down now, in my view, Mr. Chairman, is in precisely ignoring all of these lessons which came out of the enactment of FISA.

The Administration has come forward and said, as we heard again this morning, we need to modernize FISA because FISA used to permit the acquisition of the overseas calls of foreign terrorists and now it requires a warrant because we want to intercept them within the United States.

I know no one who believes that the intelligence community should not be able to intercept these calls. All of us believe that the calls of a foreign terrorist can be intercepted, should be intercepted, and that the Government has the right to do so.

If FISA needs to be amended to make that clear, that amendment would have overwhelming support within the Congress. Indeed, a number of proposals were made by senior Members of the Intelligence Committees and the Judiciary Committees of both houses which would have granted to the intelligence community the authority to conduct surveillance for that purpose.

Those amendments were rejected. And in its place, we got the language which Congress, under substantial duress, enacted into law.

The fact is there is no public explanation, and I do not believe there is any private explanation, from the Administration about what the difference is between the language that people were prepared to enact and the language that the Administration, in the end, insisted on.

And I think that is where this process needs to begin. We need to know as much as we can publicly, and certainly the Congress privately, what the difference is between the language proposed by many others, which appeared to give the Government the authority it said it needed, and the language in the statute.

Is the difference simply that one doesn't want to bother going to a court because it is a burden? Or is the difference one that actually affects what you can intercept and what you can do with that interception?

If it is the latter, we need to understand what the difference is and why that difference is important. And I believe that everyone will then want to work to make sure that the intelligence community has the authority under FISA to do the surveillance that it needs to do.

But it needs to be done based on the principles which this Committee and others insisted upon when it enacted FISA and which gave us the support that the intelligence community needs to get the cooperation that it needs from the private community going forward.

And that means it must require that it be the sole means for conducting the surveillance. Whatever one believes about the inherent constitutional power, the President and the Congress can agree that this is the sole means. And I think that is essential for gaining public support and private support.

We also need to assure that the FISA court at the initiation of any surveillance authorizes the surveillance and finds that it is consistent with the statutory requirements.

We need to have appropriate procedures for the phone companies and the Internet service providers to be notified that they must cooperate.

FISA was based on a simple and important rule. If the surveillance fit within FISA—you either had a warrant or a very specific certification from the Attorney General—then the law was you had to cooperate, whether you were a landlord, whether you were a phone company.

You had an obligation to cooperate and you were fully protected from criminal or civil liability if you failed to cooperate.

On the other hand, if you cooperated without the warrant or the certification required by the statute, then you were subject to civil and criminal penalties from the State as well as from the Federal Government.

That is the way that the Congress can enforce exclusive means. And that must be restored in this bill. By making it clear to the telephone companies again that they only can cooperate when they have either a warrant or a certificate relating to very narrow circumstances where a warrant is not required.

The problem with this bill is it gives a totally open-ended authority to the Attorney General to tell the telephone companies to cooperate. Nobody in the world can understand under what circumstances the Attorney General is permitted to make that certification.

And certainly, the phone companies will have no basis for knowing whether they are supposed to cooperate or not, whether he has met those standards. That provision, in my view, needs to be rectified, along with other changes in the statute.

Mr. Chairman, in short, we have reached, in my view, a situation that is very dangerous for our national security as well as for our civil liberties.

We have a bill elected into law without the support of the senior leadership of one of our two political parties, with vigorous opposition from the entire civil liberties community, and with nobody in the American public able to understand what it is that Congress authorized and what it is that the executive branch needed to do.

That is a recipe for suspicion, for opposition, for the intelligence community and the private industry not being sure what they are supposed to do and what the rules of the game are.

And that is a recipe, as we discovered before FISA was enacted, for people to hold back because they fear they will be subject to civil and criminal penalties and for citizens to be fearful that their phones are being tapped and their e-mails are being read.

We need clear and simple rules that everybody understands and that everybody is committed to obey. Thank you.

[The statement of Mr. Halperin follows:]

PREPARED STATEMENT OF MORTON H. HALPERIN

Mr. Chairman,

It is a great pleasure for me to appear again before this committee with regard to the Foreign Intelligence Surveillance Act.

I need to be frank, however, in saying that I am deeply troubled by the amendments to FISA passed by the Congress before the August recess. I am troubled because Congress granted to the Executive branch broad authority, in violation of the Fourth Amendment, to intercept the phone calls and emails of persons in the United

States. Moreover, any person who is committed to the constitutional principle of checks and balances should be seriously concerned because:

> Congress enacted this legislation without any opportunity for hearings and debate and without the input of civil libertarians who are as dedicated to our security as they are to the protection of civil liberties and constitutional rights.
>
> Congress enacted legislation the meaning of which is simply not deducible from the words in the text. Clearly, the Administration insisted on this language and rejected a text offered by the congressional leadership because it wants to conduct interceptions not permitted under the alternative language. However, it has not explained why that surveillance is necessary nor what interceptions are permitted under the language as enacted but not under the alternative language.
>
> The legislation enacted by the Congress at the insistence of the President excludes the FISA court from any meaningful role in permitting the surveillance to go forward. Whether the Constitution always requires a warrant for intelligence surveillance remains an open question, but there is no question that the role of the FISA court has been critical in providing assurance to the intelligence community that it would get the cooperation it needs and to the public that the Constitution was being protected. Despite strong criticism from both the left and the right, the FISA court in my view has played the role that Congress intended it to play by forcing the administration to think carefully and by reviewing its actions.
>
> The telephone companies and ISPs are being sent a dangerous message that they should and must cooperate with a request to facilitate interception of messages simply on the say-so of the Attorney General.
>
> The legislation does not reaffirm that FISA is the sole means for intercepting conversations and emails in the United States for intelligence purposes.

Not included on this list of chief concerns is the accusation that the passage of the legislation will lead to the interception of phone calls and emails that the intelligence community should not be reading. I have no idea if that is the case or not but neither does anyone else in the public and most of the Congress. That very uncertainty is simply unacceptable and a threat to both our liberty and our security.

The bipartisan and strong public support of the FISA was ruptured by the Administration's tactics. This broad support was essential in creating a system which endured from one administration to another and which enjoyed strong congressional and public support.

Congress, working with leaders of the intelligence community and the public needs to restore the bipartisan support for an effective FISA and it needs to do so quickly.

The enactment of the initial FISA bill following the Watergate and intelligence scandals provides some important lessons which should guide the Congress in that process. Since I was deeply and continuously involved in those careful negotiations, I thought I could be most useful to the committee in describing some of that history.

The enactment of FISA was triggered in large part, as I believe these recent amendments were, by concerns expressed by the telephone company. In those long gone days, there was just one telephone company (and no internet). AT&T and the FBI had a simple arrangement. An official at the Bureau would simply call the AT&T security officer and give him a phone number. Nothing more was needed and the calls were flowing into the local FBI field office.

As the scandals broke, the FBI learned that some of these numbers were not the Soviet Ambassador, but White House and NSC officials and journalists as well as business leaders and civic leaders, including Martin Luther King, Jr. Some of those who learned that they were overhead (including me and my family) sued the phone company along with government officials. AT&T had had enough and warned the Justice Department that the days of blind cooperation were over.

Attorney General Levi on behalf of the Ford Administration came to the Congress and asked for legislation. Congress agreed to authorize interceptions for intelligence purposes under a different standard than for criminal wiretaps but only after insisting on four essential principles:

- surveillance could occur only after the FISA court issued an order or the situation fit into a few tightly drawn and fully specified exceptions to the warrant requirement.
- the phone company would be required to cooperate if given a court order or a certification by the Attorney General that the situation met one of the limited specified exceptions and that the requirements spelled out in FISA for such an exception had been fully satisfied.

- No U.S. person or any person in the United States would be the target of surveillance except if the FISA court found individualized probable cause about that person.
- The draft legislation needed to be subject to full public hearings as well as classified hearings at which the meaning of each phase in the legislation was fully explained and civil liberties groups were given an opportunity to testify.

We must go back to these core principles. The Congress must insist that senior officials of the intelligence community testify in public and in private before the Judiciary as well as the Intelligence Committees and explain in detail what meaning they attach to each of the new and arcane phrases in the bill. These officials should also explain why they seek this language to accomplish the objectives that they assert are what motivates the request for legislation. Administration officials must also explain in detail why the earlier bills drafted by the Congress in response to the described need did not accomplish these objectives.

Then there must be an opportunity for private citizens and groups to testify as to their understanding of the draft bill and the requirements of the Constitution. Then there should be private and public conversations to seek to arrive at a consensus that would restore the bipartisan and broad public support for FISA. Then the committees should conduct open mark ups and the bills should be debated on the floor of both houses and if necessary in a conference committee.

The final legislation should make clear that it is the sole means by which the executive branch can intercept communications in the United States or from Americans anywhere for intelligence purposes. It should enforce that assertion by directing the phone companies and ISPs to cooperate when they receive a court order or a certification that the surveillance is within the narrow exceptions to the warrant requirement specified in the statute. All private persons should be on clear notice that if they cooperate with surveillance in any other circumstances that they will be subject to state as well as federal civil and criminal penalties.

I have said almost nothing about the substance of what changes need to be made in FISA. I have not done so in part because I expect other witnesses will discuss these issues. More important I think it is premature. There is enough information in the public domain to know that Congress has given the Administration far more unchecked power than the Constitution permits or our security requires. At the same time, there is far from enough public information to know how to restore the balance that FISA had until last month and from which we all benefit.

Mr. Chairman, I once again want to express my appreciation to you and to the committee for inviting me to participate in this hearing and I would be pleased to respond to your questions.

Mr. CONYERS. Thank you very much.

Congressman Barr, Attorney Spaulding, Dr. Turner and Mort Halperin, I am very grateful to you for beginning our examination of FISA in this setting.

Mort Halperin, I not only want you to get your law degree, but I know a number of schools that would welcome you to teach law at these schools, and we thank you for your long experience.

We now begin the inquiry of the witnesses. And in my 5 minutes, I just want to ask this one question. Isn't it important that we reestablish that the sole means of intercepting any kinds of communications, conversations, or e-mail from United States citizens for intelligence purposes go through the FISA court or be specifically accepted from them under very clear terms by the FISA court?

And let's start with you, Dr. Turner. What do you feel about that?

Mr. TURNER. Well, I don't think it is possible for anyone, including the Congress and the President together, to prevent constitutional national security law searches.

The question is, do you always have to have a warrant in order to listen to a communication with an American? And the answer to that is clear.

Every court to consider it has basically said there is a foreign intelligence exception to the fourth amendment just as there are exceptions in so many other areas.

I came into this building today. They went through my bag. They made me go through a machine. Airports—these are searches under the Fourth amendment, but the way it is decided—the Supreme Court says you balance the infringement on privacy with the Government interest, and the court in *Haig v. Agee* said no governmental interest is more important than the national security.

Mr. CONYERS. Okay. Wait a minute.

Mr. TURNER. Sorry. Yes, sir.

Mr. CONYERS. Congressman Barr, what is your reaction to the question?

Mr. BARR. My reaction to the question, Mr. Chairman, is it is a very appropriate one that both this and prior Congresses have considered. The Chairman correctly identifies the gravamen of what we are talking about here, and that is the private communications of American persons in this country.

Under FISA, the Chairman's question was answered resoundingly with a yes. And courts have recognized that. It provides both an institutional and a constitutional framework that respects the privacy rights of our citizenry yet also affords very clear and robust mechanisms for the Government to acquire the foreign intelligence that it claims it needs.

That is the point where we were before this law was signed a month ago, and that is where we ought to return.

Mr. CONYERS. Thank you.

Attorney Spaulding?

Ms. SPAULDING. Mr. Chairman, as I said in my opening statement and my written testimony, I think it is vitally important that Congress get some affirmation, confirmation, from the executive branch that the President will, indeed, abide by the law.

I think this issue of Article II authority and the President's authority to ignore laws, or not abide by laws that the President determines unilaterally are unconstitutional, is one that really needs to be more fully discussed and debated and wrestled to the ground, frankly.

Mr. CONYERS. Mr. Halperin?

Mr. HALPERIN. There is no case holding that Congress cannot limit the President's power to conduct electronic surveillance for foreign purposes.

All of the cases that Mr. Turner refers to are cases dealing with the question of whether in the absence of congressional legislation either prohibiting or authorizing such surveillance the President has the authority to conduct that surveillance on his own initiative.

That remains an open question. But there is no authority at all propositioned that Congress cannot limit the President's power.

There are, indeed, cases in the court now which the Government is desperately trying to have dismissed because I think it fears they will lead to an opinion that says that if the Congress proposes a means to do this, the President must follow those means.

But at best, it is an open question and, in my view, almost an irrelevant question, because if the President agrees that he will follow these rules because that is the way to get the support of the

American people and of the phone companies, surely the President has the authority under the Constitution to decide that he will follow these procedures.

And that is the——

Mr. CONYERS. Well, we don't have any objection, do we, witnesses, that Americans, particularly on American soil, cannot be surveilled unless they go through the requirements of FISA law?

And there are existing exemptions that would allow them to be surveilled, but in the overwhelming majority of cases, they can't be surveilled. Does anybody want to refine their response to that question which I suggest is "yes"?

Mr. TURNER. Mr. Chairman, there are two sides to this. If we are targeting a foreign intelligence source—say, you know, bin Laden in Pakistan—and he is communicating with Joe Six Pack in Peoria, clearly the President has constitutional power to intercept that conversation.

As far as targeting an American citizen, I think it is unsettled, because if there is, in fact, as several courts have said, a national security or foreign intelligence exception to the fourth amendment, then if that American citizen were involved with foreign powers, you might well be allowed to have a warrantless wiretap.

The courts have not said that, but I think it certainly follows from some of the decisions we have.

Mr. CONYERS. I just want everyone to know that I have been in discussions with the Ranking Member, that there may be hearings that will be classified because of the nature of the discussions that will be happening. And that we are also considering inviting some of our colleagues who have opinions and advice to give us in the formulation of this law, maybe even to the extent of having a hearing solely of our other colleagues who are not Members of the Committee.

And with that, I recognize Lamar Smith.

Mr. SMITH. Thank you, Mr. Chairman.

Professor Turner, I have several questions, and I will try to keep them brief—if you can give me short answers as well.

I want to touch upon a subject that just has come up, and that is you clearly feel that the fourth amendment's protection of privacy is not implicated by a phone call from a foreign terrorist to someone who lives in the United States.

Do you want to, because of national security reasons, elaborate on your answer in any way?

Mr. TURNER. Well, just briefly, the general principle of wiretaps is if you have a legal wiretap for, say, somebody selling illegal guns, and I call him up, even though the Government has never heard of me, they can record every word I say and use it against——

Mr. SMITH. Right.

Mr. TURNER [continuing]. Me in court. In the same way, it is absolutely clear the President, certainly in time of war, when you have to engage in intelligence to find out even what to target, has independent and exclusive power to listen to al-Qaida in this case, and it is reinforced by the authorization for the use of military force.

Mr. SMITH. Right. Okay. Thank you.

Professor Turner, also, what kinds of information has the intelligence community not been able to gather over the last 20 years or 30 years because of changes in technology?

Mr. TURNER. Well, I have been out of this business for more than 25 years, or almost 25 years, but from the testimony of the DNI, we are told roughly 25 percent of the intelligence we used to get we are not getting now, and a lot of this is foreign known or suspect terrorists calling other terrorists outside this country.

Because those communications happen to transit a switch in northern Virginia or Silicon Valley, FISA is stopping us from listening to those, and people may die because of that.

Mr. SMITH. Okay. What additional changes do you feel should be made to FISA? And if so, why do you think those changes should be made?

Mr. TURNER. Well, FISA is only going to work if you have the agreement of the President. Griffin Bell himself said that is how this will work, because you can't take away the President's power.

Mort said there is no court case saying Congress can't do this. That is silly. The appeals court you set up under FISA, in the 2002 case, In re Sealed Case, said "FISA could not encroach on the President's constitutional power."

What authority do you want? That is a U.S. Court of Appeals that you set up to judge FISA. It is unanimous when you say you can't do this. So the way FISA is going to work—it is in the executive's interest to have FISA. Why? If they get a warrant, they can be sure they can get that evidence in court if they try to convict someone.

If they are doing it for foreign intelligence purposes, that is not a problem. Getting it into court—and they have got reasonableness tests and so forth.

They want to work with you. They have given you a bill that draws the distinction not where you intercept it, but is this a foreign power or are you targeting a U.S. citizen. That is an awfully good deal. I would take it.

Mr. SMITH. Okay. Professor Turner, also, why is the FISA process so burdensome?

Mr. TURNER. Well, they tried to streamline it, but the way it works—first of all, you have got, say, an NSA analyst. He says, "Hey, we need a warrant for this. We need a warrant."

They put together a package. They run it through the lawyers at NSA. They have got a lot of lawyers out there. They send it over to the Office of Intelligence Policy and Review, in what is now the national security division. They look at it.

And if they like it, then they run it by the Attorney General, who may be in Peoria today giving a speech. But when he gets back, he has to come up to the Hill and testify, but then he gets back on, say, Friday.

He signs it, and it goes over to the White House and gets signed by the national security advisor. Then it gets in line to be considered by the court.

These judges are wonderful. They are working all day long and on weekends. But there still is a several-day delay, and one of the most important principles in war is speed and dispatch.

If it takes you 4, 5, 10 days, 2 weeks to get a decision, the bomb may have already blown.

Mr. SMITH. Thank you, Professor Turner.

Let me go to former colleague Bob Barr and make a comment. And, Bob, you are welcome to respond if you want to. Thank you for your very articulate testimony—no surprise there.

At the outset of your testimony, though, you made the statement that Director McConnell had said that the mere debate of FISA was going to cost American lives. I think you came to that conclusion, which I think is a mischaracterization, because of the media.

And I notice in the A.P. report of his comments that was something that they concluded. And I will say that was an editorial comment on the part of the A.P. that I think was not appropriate.

But let me read you Director McConnell's exact words, and I think we will all agree that it wasn't the mere debate on FISA that was going to cost lives, it was the release of classified information that was going to cost lives.

"Part of this is a classified world. The fact that we are doing it this way means that some Americans are going to die." He was referring to the classified information, not the debate itself.

And it is understandable you said what you did, because that was the way the A.P. characterized it, but I don't think that that would be an accurate characterization. Just a comment.

Thank you, Mr. Chairman. And my time has expired.

Mr. CONYERS. Chairman Jerry Nadler?

Mr. NADLER. Thank you, Mr. Chairman.

Congressman Barr, I would like to ask a couple of questions about Ms. Spaulding's testimony. She writes that section 105(b) provides authority to the A.G. and DNI to collect intelligence information inside the U.S. so long as the information is about a person who happens to be outside the U.S. at the time, including a U.S. citizen.

It would appear, therefore, to authorize intercepting U.S. mail between two people inside the U.S. so long as the Government—without a warrant—so long as the Government reasonably believes the letter discussed, at least in part, someone outside the U.S.

Do you agree with that?

Mr. BARR. I think that is an accurate reading of the section 105(b).

Mr. NADLER. Thank you. She also says it would appear the A.G. could authorize the physical search of your home to find a letter from your son overseas or the family computer on which you stored his e-mails.

Do you think that that is a reasonable reading of this statute?

Mr. BARR. I do.

Mr. NADLER. Okay. Thank you. Thank you very much.

Ms. Spaulding, you talk about the provisions immunizing the telecommunications companies from liability.

We are being asked very insistently by the Administration to enact legislation now to immunize the telecommunications companies retroactively from any liability for the last 5 years since the President started ignoring the FISA act in 2001.

Why should we or shouldn't we do that, in your opinion?

Ms. SPAULDING. I think it would be a huge mistake, Congressman. As Mort Halperin has already testified, the current law already protects telecommunications carriers and others who provide assistance to the Government.

In this case, all they needed was a letter from the Attorney General certifying that this request for assistance was legal.

If they are now seeking immunity from liability, I can only assume they didn't even get that letter. And I think for Congress to say that is okay sends a very strong signal undermining our respect for the rule of law.

Mr. NADLER. Well, let me ask you this. The President's and the Attorney General's tapping people's phones without a warrant from the FISA court would appear to be a prima facie violation of the FISA act, which is a criminal statute.

If we are not prosecuting them, why should we let the telecom companies get off scot-free?

Ms. SPAULDING. Well, I think that is certainly a fair point. But I think the Attorney General, given the legal arguments from the Department of Justice, asserting that this warrantless surveillance in violation of FISA was nonetheless legal, certainly could have provided this letter to the telecommunications carriers.

And why, given that, if that is all they needed, they need immunity at this point is beyond me.

And I also think that they are an important, given the lack of transparency in this area, they are an important safeguard against Government abuse.

Mr. NADLER. Well, I must say that since the Government is interposing a state secrets defense on any lawsuit against the Government for illegal wiretapping, suing the telecommunications companies might be the only way of getting into court.

And I certainly agree with you. I don't like the abuse of the state secrets doctrine, but this may be somewhat of a way around that.

And absent that, if we were to give them that protection retroactively, there might be no way for anybody to get into court, and the executive would be completely scot free to ignore the law without any judicial accountability.

Mr. Halperin?

Mr. HALPERIN. Yes, the problem is the Government is asserting the state secrets privilege even when the telephone companies are sued. So I think that we need to find a way around that.

And I think Congress could do that by simply asserting that the justifications provided by the Government to the phone companies need to be made public. Those are documents that, I gather, Committees have sued for.

I think we are all entitled to see those. And I think one way to deal with the problem is to give the phone companies limited immunity based on a demonstration that they acted on a communication from the Attorney General that they reasonably relied on to believe that the surveillance was lawful.

We don't have any idea what the Government told the telephone companies. And to give them immunity without first finding out——

Mr. NADLER. I agree with you. Thank you.

Mr. Turner—or Professor Turner, I should say—you have written as to the President's expansive foreign relations powers, inherent powers.

I would like to ask you some questions with regard to the scope of those powers. If President Bush believed an American citizen in the United States were a spy for al-Qaida, could he authorize the burglary of that citizen's house to plant an eavesdropping bug without a wire?

Mr. TURNER. That is an interesting question. If the courts that have decided that there is a foreign intelligence exception to the fourth amendment, as there is in so many other areas—I don't know the answer to that, you know, but it at least would be arguable.

Mr. NADLER. And my last question. Could he be permitted in that circumstance to authorize the breaking into that individual's psychiatrist's office without a warrant to find evidence against him?

Mr. TURNER. I think it is a moot point. As I understand the Administration, they are saying they will get warrants for——

Mr. NADLER. No, no, but could they, under your interpretation of the law?

Mr. TURNER. It is an interesting question. I would really want to think about it. If you want an answer for the record, I will try to think about it. But that is an area of the law I don't teach in the general——

Mr. NADLER. Okay. Thank you.

Mr. CONYERS. The gentleman's time has expired.

Howard Coble, the gentleman from North Carolina and Ranking Member on the Subcommittee of Courts?

Mr. COBLE. Thank you, Mr. Chairman.

Good to have you all with us.

Professor Turner, we are working you overtime today. Let me put a two-part question to you.

What implication does the growth of mobile telephones have on FISA surveillance? And does this not require some flexible standard when our Government reasonably believes that the person is located outside the United States?

Mr. TURNER. It is a very good question. I may not be the right person to answer it, but my—again, when I last worked in this area, it was the early 1980's when nobody I knew could afford a portable telephone.

When FISA was written, telephones were carried by lines. Today most phone conversations, land line or mobile, I am told, are actually sent through other means.

So there are a lot of sort of technical amendments here. But one of the problems we have run into—the Patriot Act, for example, included a provision—the old way, you go to a judge.

You would say, "I have got a suspected—here is the probable cause. Here is his phone number." You would get a warrant to monitor that phone number.

Well, we have got drug dealers, terrorists and others who will buy a dozen cheap cell phones, use them for an hour, throw one away. Then the surveillance guy has to run back to the judge, "Hey, here is a new number."

When he gets back, he is three phones later. It doesn't work. The modern communications, from e-mail, cell phones and so forth, make the job of terrorists much easier. We have to adapt the law to make it possible for the people trying to stop them to keep up with them.

And again, the technology I can't tell you much about, especially the classified side, because I don't know about it, but my understanding is we are missing a lot of stuff.

Again, the DNI has said 25 percent we were getting a year ago because FISA and other laws have not kept up with the 21st century.

Mr. COBLE. Thank you, Professor.

Ms. Spaulding, what do you say about that, about flexible standard?

Ms. SPAULDING. Chairman Coble, I think there is certainly room for looking again at FISA to see whether it, in fact, ought to be modernized given changes in technology. And in fact, it has been a number of times, as you know, over the years.

And the example that Professor Turner gave of, you know, changing the cell phones, in fact, has been addressed through provisions that address roving wiretaps.

I think it is important to make sure, as I said at the outset, that these intelligence professionals have the tools that they need. I think it is equally important to ensure we have appropriate safeguards as we do that.

Mr. COBLE. Ms. Spaulding, thank you for elevating me to chairmanship. I am not aware of that, but thank you nonetheless.

Mr. Turner, let me come back to you. What do you believe was the Congress' intent with respect to FISA coverage of domestic communication involving foreign intelligence, domestic caller to domestic caller, versus international communications involving foreign intelligence, foreign caller to foreign caller?

Mr. TURNER. FISA clearly wanted to protect any U.S. person any, you know, domestic calls, basically, and it intentionally excluded—indeed, in the HPSCI report, they said, "We considered trying to cover foreign calls, and we decided it is just too complex, and it can't be done in this bill."

So it is very clear that FISA was not intended to place any limits on intercepting, you know, the calls of foreigners outside of this country or calls even of Americans outside this country.

Mr. COBLE. Let me talk to the Georgian for a minute and welcome him back to the Hill.

Mr. Barr, how burdensome, in your opinion, is the FISA process? And what modifications, if any, can be made to the process to expedite the process of applications?

Mr. BARR. In my experience, and I note in the same interview that the Ranking Member and I have a little bit of a disagreement about involving Director McConnell, he talks about the article here, that it takes 200 hours to assemble a FISA warrant on a single telephone number.

That certainly ought to be something that this Congress looks into to determine whether or not that figure is an accurate figure. If, in fact, it is an accurate figure and that much time is consumed

with virtually every FISA application, then it might be a question of resources that the Congress has to look into.

But the mechanism itself, I don't believe, is particularly burdensome. And with the growth of technology, it becomes actually much easier now than previously, in previous years and decades, to determine where a call is being made.

If you have two people using cell phones overseas, the Government, through the technology available even to private industry, knows exactly where those two people are calling.

So if you have two people using cell phones overseas, you don't need this massive rewrite of FISA that basically subjects every call that somebody in this country makes to somebody, anybody, whoever, overseas potentially subject to Government surveillance.

Mr. COBLE. Thank you, sir.

Mr. Turner?

Mr. TURNER. Just one quick point. In addition to the 200 hours—I don't know if that figure—I assume that figure is true. But also, a lot of those hours are spent by linguists who have the special ability—they are one of the most valuable commodities we have and one of our greatest weaknesses.

And taking people who understand the culture and the language of our enemy and making them review FISA requests, so they cannot be reviewing intercepts that might be talking about tomorrow's attack, is a very expensive price.

Mr. COBLE. My red light illuminates, and I yield back, Mr. Chairman.

Mr. CONYERS. Chairman Bobby Scott?

Mr. SCOTT. Thank you. Thank you, Mr. Chairman.

I thank all of our witnesses for their testimony.

Ms. Spaulding, you mentioned the new act had the word "concerning" in 105(b)—105(a) says encompass surveillance directed at a person reasonably believed to be located outside the United States.

But section (b) says acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States.

Could you restate what you think that difference in wording might mean?

Ms. SPAULDING. Well, it seems to me that section 105(a), in redefining electronic surveillance, when it uses the words "directed at" it means targeting. It means that that is the focus of your surveillance.

That is where you are directing your interest, as opposed to at the other parties with whom that target may be communicating.

Concerning persons—if they had meant the exact same thing, if they had meant targeting persons, I think they would have used the words "directed at." Concerning persons means something different, then.

And I think it could mean the communication merely mentions or is about, even just in part, someone who happens to be outside the United States, and that is a far different matter.

Mr. SCOTT. So if the communication is concerning someone outside, could that include communications domestic to domestic?

Ms. SPAULDING. Absolutely.

Mr. SCOTT. And do you think that—because we don't hear that mentioned very often, and these two words, as I have noticed, as you have, are different words and must mean different things.

Ms. SPAULDING. I would note that when we talk about communications between two individuals inside the United States, potentially coming within the scope of 105(b), there is the requirement that it not be electronic surveillance, which is why in my testimony I refer to letters or potentially stored e-mails, things that do not fall within the existing definition of electronic surveillance.

Mr. SCOTT. And you also mentioned that foreign intelligence—we keep hearing an al-Qaida member calling inside, but foreign intelligence includes more than terrorism, does it not?

Ms. SPAULDING. Absolutely. It is a very broad definition, one that has been broadened over the years.

Mr. SCOTT. And what kinds of things might be foreign intelligence?

Ms. SPAULDING. Really almost anything of interest to the foreign affairs and national defense of the United States.

In fact, most recently, it was broadened to include information that is at all relevant to potential sabotage or attack in the United States. So that might mean, for example, if you——

Mr. SCOTT. Well, that is terrorism. What about a trade deal?

Ms. SPAULDING. Well, it obviously includes trade deals. It includes all of the things that you think about the intelligence community monitoring and being interested in, and now they have added to their agenda global climate change.

They have long been interested in trade issues. There is a wide range of information that——

Mr. SCOTT. So if you are negotiating a global warming agreement with another country, that would constitute foreign intelligence.

Ms. SPAULDING. It might constitute foreign intelligence.

Mr. SCOTT. There is another little change here where it says significant purpose. That is not the primary purpose. If the primary purpose is not even foreign intelligence, what could the primary purpose be?

Ms. SPAULDING. The primary purpose could be anything that is presumably constitutional. You know, I think it would be limited, clearly, by the constitutional framework, but it could——

Mr. SCOTT. Partisan politics?

Ms. SPAULDING. It could be, because certainly, we know that it could be criminal prosecution.

Mr. SCOTT. Without probable cause of a crime.

Ms. SPAULDING. And it could be suspicion of, you know, subversion, which we know has been interpreted in ways that have proven very harmful in the past.

Mr. SCOTT. Now, Mr. Barr, is there anything under FISA that you can't do that you could do if you didn't have to worry about FISA? Or does FISA just require you to let the court know what you are doing?

Mr. BARR. No, FISA, under the very words of the statute and the way it has been interpreted over the years, is intended to and encompasses electronic surveillance for foreign intelligence purposes.

So if, in fact, that is, you know, the universe of information or persons involved in that that you are trying to gather evidence or information from, on or about, then FISA covers that.

Now, does that mean there——

Mr. SCOTT. But let me just——

Mr. BARR [continuing]. Isn't overlap with other areas?

Mr. SCOTT. We keep talking about balancing security and liberties. In fact, there is no balance at all because you can do any kind of wiretap you want under FISA. You just have to notify the court. Or without FISA, you just go ahead and do it.

But if it is legal, you can go ahead. There is no restriction on security created by requiring you to go to the FISA court, is there?

Mr. BARR. And that is correct, and that problem is made manifestly worse by the law that was signed 1 month ago.

Mr. SCOTT. And that is just on the—essentially the Attorney General and the director of intelligence can just authorize it.

Mr. BARR. Without any review by the courts at all.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. CONYERS. Thank you.

The gentleman from Virginia, Bob Goodlatte?

Mr. GOODLATTE. Mr. Chairman, thank you very much, and thank you for holding this hearing on this ongoing discussion.

The response by some to the Government's concerns has typically been we will give them more resources. That seems to me to miss a couple of basic points.

One, even if the department, the intelligence community, the FISA court had additional resources, would it make sense to expend them on taking surveillance of foreign terrorists operating overseas to the FISA court?

And second, at some point there is what I call a pyramid problem. Assuming that we could find more linguists to translate, more agents, more lawyers, all applications still have to go to the top of the department and would have to be certified by a Senate-confirmed official in the intelligence community, which is a good thing. There should be very high-level accountability for the decision.

If this high-level sign-off based upon an individualized showing of probable cause is needed, how will more resources provide the intelligence community with the speed and agility that is needed?

Mr. Turner, do you have any thoughts on that?

Mr. TURNER. Amen. I think you said it very well. I agree completely.

Mr. GOODLATTE. Mr. Halperin, do you have a——

Mr. HALPERIN. Yes, I do have some views on that. First of all, in terms of speed and agility, the solution in FISA is to permit emergency surveillances and still you get a warrant.

And I think the Administration has made a case that those emergency procedures are not flexible enough. And I think Congress ought to be willing to consider precise proposals to extend the emergency procedures.

For example, they could allow an NSA agency official to begin a surveillance based on guidelines established by the Attorney General and give him several days before he has to take it to the Justice Department.

In turn, the Justice Department could have several days before it had to take the matter to court if it determined that a court order was needed. So the——

Mr. GOODLATTE. But aren't we talking about enormous volumes of material that need to be worked through?

Mr. HALPERIN. Well, we don't have any idea, because we haven't been told what it is they want to hear.

If it is a question simply of saying, "We want to be able to conduct surveillance of phone conversations between two people overseas, but we want to intercept them in the United States," then I think everybody would support an amendment that said you do not need a court order to conduct a surveillance of two people outside the United States.

Mr. GOODLATTE. That leads to my next question, so I will go right to that.

Some have suggested this so-called foreign-to-foreign carve-out, but I wonder how workable that really is. After all, how is the Government going to know in advance who an overseas target is going to contact when they make——

Mr. HALPERIN. But that, of course, proves our point, not yours, which is to say the Government can't know that it is only intercepting the conversations of two people overseas. It may well be intercepting the conversations of many Americans.

And that is precisely why it should require a warrant, because it can't be sure of what it will encounter.

Mr. GOODLATTE. We are talking about thousands of these every single day. How can you have that problem that we just described to you work to adequately understand the intelligence information that is being gathered on a regular basis?

Now, as soon as it is determined that there is a U.S. citizen involved in the conversation, I absolutely agree with you.

Mr. HALPERIN. But that is what Congress—that was a provision in the alternative bill that the Administration insisted be taken out.

Exactly what needs to be added to the bill is language which says when you discover that this channel that you are listening to, which you thought was foreign to foreign, in fact picked up a significant number of conversations of U.S. citizens, then you have got to go back to the FISA court and get an appropriate warrant with appropriate minimization procedures.

That is exactly what this whole fight is about. If the Administration conceded that, we could get an agreement. It is resisting exactly that.

Mr. GOODLATTE. Well, let me ask Mr. Turner to respond to your comment.

Mr. TURNER. I don't know the modern technology, but my guess is it is going to be difficult to capture bin Laden's conversations with his top aides from Pakistan to Saudi Arabia, wherever, without occasionally intercepting some U.S. person communications.

I think the focus needs to be on minimization. That is to say, let them get what they need to stop the next 9/11, but have very firm processes so as soon as they determine that any U.S. person in the communication is not, in fact, working with the terrorists and talk-

ing about, "Yes, where do I go to pick up the explosive to knock off the capital?"

Then you do what they have always done, which is first to isolate the material so nobody can have it, make a record of it, and destroy it to protect the rights of Americans.

The idea that the risk they are going to pick up one of my e-mails or one of my phone calls means we should stop listening to bin Laden and let him kill anybody he wants to me is a very bad balance of those very important interests.

Mr. GOODLATTE. Thank you.

Let me ask Mr. Barr or Ms. Spaulding, anybody, with the advent of large fiber optic cables and other new technologies, should FISA cover situations where a call is routed to a United States facility, but involves two persons located outside the United States? Why or why not?

Mr. BARR. No, they should be exempt. And here again, if that is, in fact, the problem, as I believe it is, as articulated by the Administration, I believe there are certainly much more simple and focused ways to address that than the legislation that was signed a month ago.

Mr. GOODLATTE. Ms. Spaulding?

Ms. SPAULDING. Well, I think we are all in agreement on that point. You know, Professor Turner and you were discussing a much more challenging point, which is when you reasonably believe that you have got foreign to foreign, and your target is a foreign target, but you inadvertently pick up U.S. person communication.

I think where you don't know for sure what the other end of the call is, there ought to be an affirmative obligation, not just if you happen to discover, but affirmative obligation on the Government to have procedures in place to determine, even if after the fact, whether, in fact, a significant number of those communications are going into the United States and involve U.S. persons or people inside the United States.

And at that point, I think there does need to be some more rigorous process.

I agree with Professor Turner that I think a big part of the solution here lies in very strict, stringent minimization procedures of the kind that the executive branch now uses when the Attorney General unilaterally approves of a wiretap.

Mr. GOODLATTE. Thank you.

Thank you, Mr. Chairman.

Mr. CONYERS. Thank you.

Chairwoman Zoe Lofgren?

Ms. LOFGREN. Thank you, Mr. Chairman.

Before I ask my questions, I would like to yield—he said 5 seconds, but we won't be strict on that—to Mr. Scott for a point he wanted to make.

Mr. SCOTT. Thank you. Thank you.

And I appreciate you for yielding, because some people try to suggest that the requirement to get a FISA warrant means you can't listen to the conversation. You can listen to the conversation. You just have to get a FISA warrant.

So when you say these—listening to al-Qaida, if you have got a FISA warrant, you can't listen—of course you can listen. Thank you.

Ms. LOFGREN. Reclaiming my time, I would just like to ask Mr. Barr—and it is good to have you back in this Committee room. I read through your testimony, and I see this quite similarly to the way you do.

And I remember the years we served here on the Committee, we didn't always see every issue the same way, but often on constitutional issues we did. And I find that that is once again the case.

You mentioned that the—and I agree with you; I think we made this point quite clearly—that changes that would allow for the capture of communications from someone in a foreign country to someone in another foreign country that was routed technologically through the U.S.—there is no problem with it.

I think there is like almost unanimous agreement that that should not be precluded, and that you wouldn't need a FISA warrant. You shouldn't need a FISA warrant because the people that you are tapping are abroad.

However, supposedly there was a court decision that required a change in the law. It is a mysterious court decision. How much do we know—do you know what is in that court decision? I haven't seen the decision, as we have not been permitted to see it.

Mr. BARR. It is very interesting, because in the very interview that the Ranking Member and I were discussing with DNI Director Mike McConnell, he apparently knows, as he should, a great deal about it and actually discussed it, even though it is my understanding that the order or the opinion remains classified.

So it raises in my mind an interesting question about discussing classified information. But no, none of us do. I certainly haven't seen it. And I am not absolutely certain, therefore, and I don't think we ought to presume, that it is necessarily a good decision.

I would want to see it. I would think the Committee would want to see it.

Ms. LOFGREN. Well, you suggest that we should have more vigorous oversight in this activity, and I very much agree. And one of the things that I think has been a tremendous improvement in the 110th Congress is that the Judiciary Committee is now involved in this. It is not just the Intelligence Committee.

And we have our own backgrounds and set of skills to bring to this debate to enhance what the Intelligence Committee is doing.

And I am pleased, Mr. Chairman, that we are going to have some classified hearings, and I am hopeful that one element of that might be a review of the actual decision that supposedly set this whole circumstances on its merry way.

And if the DNI could talk about it on T.V., I would assume that Members of Congress who have signed an oath never to reveal classified information would be able to review it in a classified setting.

Now, for Ms. Spaulding, you know, one of the things you mention in your testimony has to do with the technology, and it was a point that I made on the floor with my colleagues, that for telecommunications, you know where calls are being initiated. At least you know enough to get the bill for them.

And so presumably, you wouldn't have the kind of rampant inadvertence that is referred to in terms of how would you ever know if a call was being initiated here or there.

You know, one of the concerns that I had is that we didn't have any technology experts with us to inform us. We had a lot of constitutional lawyers in the Congress, not that many technological wiz people.

Do you know whether any technology experts have really reviewed the statute? I have been reaching out to some in Silicon Valley. Have you been able to discover expertise that we could tap into on that aspect of this?

Ms. SPAULDING. First, I want to applaud you for reaching out to the technology experts outside the Government. As I said in my testimony, I think that is vitally important.

And I do think that technology allows us to narrow significantly that group of communications for which we don't know.

I think one of the greatest challenges, I would say, in that regard, is less phone calls than it is potentially either e-mail or—often times, what terrorists will do is draft an e-mail but not send it, and save it as a draft.

And then the intended recipient simply logs on as that user and goes to the saved draft file, for example. And you can't know the nationality, potentially, of the person who—so I think there are examples where it is extremely difficult, if not impossible, to know where the recipient of a communication resides.

But I think it is a very narrow band of communications, and technology experts can help us.

Kim Taipale is somebody—I am not sure I am pronouncing his last name correctly—is someone who has looked very carefully at both the technology and the law, and I would certainly recommend that you talk with him.

Ms. LOFGREN. Thank you, Mr. Chairman. My time has expired.

Mr. CONYERS. Our only California attorney general, Dan Lungren?

Mr. LUNGREN. Thank you very much, Mr. Chairman, our only Chairman of the Judiciary Committee at the present time. And I will treat you kindly, too, when you are the Chairman Emeritus.

First of all, I just find it passing strange that we would have someone on the majority side suggest that this bill is somehow a covert operation for us to gain information on global warming.

The only reason global warming is within the ambit of the intelligence community is that the majority party decided, in the reauthorization of the intelligence act, to put global warming within the ambit of the Intelligence Committee, requiring them to do not only short-term, but long-term 50-year studies on global warming, which I thought was nonsense. It ought not to be part of the Intelligence Committee.

But to use that now as a criticism of this bill is extraordinarily inventive.

Let's just, please, go back and understand why we are where we are. The DNI, Admiral McConnell, who was the NSA director under Bill Clinton, someone who I am unaware has any public political motivation, came to us and said two things.

One, he said we had increasing chatter from targets of our terrorism intelligence overseas similar to that increased chatter we had just before 9/11. He did not say that we were going to have a 9/11, but he said it would be irresponsible for us not to pay attention.

He said, secondly, because of a decision of the FISA court by a single FISA court judge, we had been blinded.

And I thought it was a classified piece of information as to how much we have been blinded, but you have suggested, Professor, that he has stated publicly on the record how much of our targets we used to get we can no longer get.

The judge said go to Congress to have it changed. He had to rule that way because the change in technology—the law had not come up to it. So that is where we are.

Why did we include it for all foreign intelligence? For the very reason articulated by Admiral McConnell. What is the worst scenario we could possibly have? It is al-Qaida or another transnational terrorist organization making common cause with a rogue state that has a nuclear weapon.

And he suggested perhaps the best way for us to find out about that is to target the other country rather than al-Qaida. That is why he expanded it, not so he could go into global warming information.

The other thing he told us was that if you merely defined it, as the Democratic bill did, the Democratic majority bill as presented to us, to say, "Look, as long as it is foreign to foreign, that takes care of it," he told us practically speaking that does not take care of the problem, because you don't know ahead of time whether there is going to be an inadvertent conversation into the United States because you are targeting a source outside the United States.

So balancing those things, how do you respond? The bill that we passed responds in this way.

It says because we have heard from Admiral McConnell that practically speaking it makes it impossible for us to respond to the law in the way articulated under the Democratic provision, because practically speaking it takes too much manpower, too much time, to go for an application in each instance—and he talked about how the fact we have to take analysts offline, linguists offline, to do that so they can't do the other, and the time requirements, as you suggested, Professor—he suggested the way to do it is the way we do in the criminal justice system.

When you wiretap a mafioso member, you don't know who he is going to call. As I said before, he could be calling his sainted mother, or his brother the priest or the pizza delivery guy. We bring in minimization.

And that is why I think, Professor, you are absolutely right. Where we ought to be concentrating our attention is the quality of the minimization as already articulated in the FISA statute. That didn't change with what we just put out.

The other thing is Admiral McConnell said as NSA director he took the minimization requirement so seriously because he said there was potential criminal liability for him. And he suggested that is the way you do it.

So, Professor, I would ask you this. What is essentially different between the minimization process that we have in place now where we inadvertently find an American in the United States, he is on one end of the conversation, and the minimization process we have used in the criminal justice system for years and years and years?

Mr. TURNER. The answer is I don't know enough about either one of those now. I know what it was 20 years, 25 years ago. But I think you are exactly right. I think that has to be the focus.

If I could pick up on one other issue here, and that is are we doing harm by holding hearings. Top sources of intelligence for our enemies, or the Soviets, used to be Aviation Week, which leaked things left and right, and the Congressional Record.

When you hold a hearing, you tell our enemies how our system works. The more you tell them, the more they can find—oh, they are not allowed to do this, let's direct our communications system through that, you know, free area they have given us.

And we are involved in a war against people that want to use WMD against us. I don't know if they are going to get nukes. I don't know if they are going to get some—you know, we know the Soviets were playing with a smallpox that was immune from known treatments.

If we don't take this seriously, if we don't allow our President to fight this war and protect our people, and if there is a bad consequence, people are going to want to know why they couldn't do that.

And my hope is the people in the intelligence community and elsewhere are going to say, "Well, Congress tied our hands. They were afraid we would inadvertently pick up communication with an American."

The answer: Let them get the communications. Let them extract the foreign intelligence from it. They don't want to listen to grandma talking to grandson.

When they find that conversation, they will isolate it, and they will destroy it. They will erase the recordings and so forth.

And if you tell Americans, you know, rather than overhearing grandma talking to grandson, we are going to stop listening to the enemies and stop finding out where they are planning to kill grandson, most Americans aren't going to understand that, and they shouldn't understand that.

Mr. LUNGREN. And as I understand it, even with the change we made in FISA, if, in fact, that person on the U.S. side does have information of a terrorist nature, we are going to follow it. At that point in time, we have to go in and get a FISA warrant to continue to follow that person.

Mr. TURNER. If the President accepts that. I think there is a strong case the President can act outside of FISA on that. It is in the President's interest to work with FISA.

Every Administration likes FISA because it then lets them prosecute these people. Work with them, but you have to be reasonable about it.

And if you tie their hands when it comes to getting intelligence on our enemies, and there are consequences, understand your constituents are going to ask about it.

Mr. CONYERS. The gentleman's time has expired.

The former prosecutor from the state of Massachusetts, Bill Delahunt?

Mr. DELAHUNT. Yes, thank you, Mr. Chairman.

And let me extend a welcome home to Congressman Barr. And it has been an excellent panel.

You know, I keep hearing about the delay and the cost and the burden, and that really seems to be the gravamen of many who debate this issue.

And let me just posit that no matter how much it costs, it is a cost that is well worth to protect our constitutional system and the relationship between the branches and individual liberties.

You know, there has been report after report emanating from a variety of agencies about wasteful spending. We still haven't accounted for $9 billion that was unaccounted for in Iraq during the first several months.

I dare say to protect the Constitution and what we are concerned about in terms of our own values, no price is too high, if that is really what it is about.

Because what I am hearing is well, we have to go here, we have to go there, and then we are talking about, you know, 3 days, we can make it 5 days, we can make it 7 days. We can work this out.

There is agreement that I am hearing today about foreign to foreign, and let's—I will use the term "modernize FISA" to deal with whatever has to be done to account for the newer technologies that exist.

And another issue that I would like to at least raise—because I have done a search and I can't find a single incident of information disseminating from a FISA court hearing that jeopardized the national security of the United States.

And I would just pose that to the panel. Has there been one single incident that has been reported that you are aware of that involved a leak—let me use that colloquial term—a leak from the FISA court that would jeopardize American national security?

Mr. BARR. Well, if I might respond to the gentleman from Massachusetts, I am not aware of any in the 30 years that the Foreign Intelligence Surveillance Court has been in existence.

The information, as I understand it, that has been discussed publicly regarding this particular case—which, by the way, the Government apparently was not sufficiently concerned about to seek an emergency review, which raises the question did they just want to use this as an excuse.

But the information that has been out there regarding this has been discussed by the director of national intelligence and at least one Member of this body, which raises interesting questions about leaks.

But no, I am not aware of any cases, orders, or opinions or deliberations that have been problematic in that regard.

Mr. DELAHUNT. Thank you.

Mr. Halperin?

Mr. HALPERIN. Yes. There have not been any such leaks. I also want to make——

Mr. DELAHUNT. Why can't we trust the judiciary?

Mr. HALPERIN. Well, we can, and I—if you look back at the hearing this Committee held in 1978 on this exact issue, you had all

of the same arguments made—we can't go to court, it will be too cumbersome, the information will leak, we have to move more quickly, it will take resources away.

And the fact was that Administration officials in every Administration since FISA is enacted have testified that they did far more surveillance after the enactment of FISA than they were able to do before the enactment of FISA.

And the reason was that officials in the Justice Department and the intelligence agencies were willing to do it because they knew that it was legal, because Congress had enacted it. The telephone company was willing to cooperate because they had a legal order from the Attorney General or from the court.

And so the number of interceptions went up enormously after FISA was enacted because it was done under a legal system. So the answer to the burden is that it has this payoff which the intelligence community is continuing to testify to.

What we need to do is to fix the rules so that we deal with this problem but without throwing away, as the bill that was enacted does, all the positive benefits of having a system that is broadly supported and broadly understood and that it has clear rules in it.

Mr. DELAHUNT. I think that in his testimony Congressman Barr references a quote from Judge Royce Lamberth, and I think it is particularly salient here today.

We have to understand that you can fight the war on terrorism and lose everything if you have no civil liberties left when you get through fighting the war.

What we have found in the history of our country is that you can't trust the executive. We still have to preserve our civil liberties.

With that, I yield back.

Mr. CONYERS. Thank you.

The gentleman from Indiana, Mike Pence?

Mr. PENCE. Thank you, Mr. Chairman.

And I want to thank these witnesses.

I want to welcome back, while in some disagreement on this issue, my esteemed colleague and friend, Congressman Barr. I appreciate the thoughtfulness of your presentation today.

And I really want to, in my time allotted, I want to see if we can reflect on first principles. I think Mr. Lungren did a very nice job of identifying kind of why we are here.

And the 6-month extension and the issues we are facing were not invented by the Congress.

The director of national intelligence came to the Congress and said there has been a court decision that is tying our hands, and it is affecting our ability to engage in the gathering of foreign intelligence necessary to protect the country.

And Congress was able to compromise on that this summer, and we are now back in an important debate.

I take a second chair to no one in my commitment to the constitutional liberties enshrined in the Bill of Rights, and I question the sincerity of no Member of this Committee or any Member of this body who raises issues in this debate.

But that being said, I would like to get Professor Turner to some first principles, and maybe invite a little discussion.

I am very provoked by your written testimony on the larger question here of where does the authority derive for the executive branch, and specifically the President of the United States, to engage in the gathering of foreign intelligence.

It seems to me—and I want to agree very strongly with your written testimony—that the Bush administration has done, in your words, an atrocious job of explaining their constitutional position in this matter. That, in fact, if I understand your testimony correctly, which I would encourage any American to look at in the record—is that, in fact, you know, Congress may no more usurp the constitutional powers of the President by statute than it can usurp the rights guaranteed to the people by enacting legislation contrary to the first amendment.

I think that was your thought, that the President's authority to gather foreign intelligence here is inherent in the powers of the executive. And this, as you forcefully articulate, was reflected by the likes of Thomas Jefferson and George Washington and other framers of the Constitution.

I was especially moved by the quote from Senator Fulbright, the late Senator Fulbright, who was a leading critic of the Vietnam War, who made a comment in which he explained "the preeminent responsibility of the President for the formulation of the conduct of American foreign policy is clear and unalterable," adding later that this also included the Central Intelligence Agency and all of the vast executive apparatus.

I believe, Professor Turner, you point out and emphasize the word "formulation" here. Then, in fact, Senator Fulbright himself said the President's authority was not merely to carry out policies established by Congress, as is the case of domestic policy, but it is the case to make policy in the gathering of foreign intelligence and protecting the Nation.

I also would point out that you quote favorably President Carter's Attorney General, Griffin Bell, who said that in the testimony involving the creation of the FISA court, he said the current bill recognizes no inherent power of the President to conduct electronic surveillance.

And I want to interpolate here that this does not take away the power of the President under the Constitution. He went on to say it is not necessary to state that power. There is no reason to reiterate it or to iterate it, as the case may be. It is in the Constitution, whatever it is. The President, by offering this legislation, is agreeing to follow statutory procedures.

I would like to raise that issue with you, Professor Turner, and then to anyone else on the panel, of where does this authority derive from. Can you expand on that further?

Because I think it is a backdrop of this debate that is largely lost, as millions of Americans, I think, believe the President's ability to engage in surveillance derives from the FISA act itself.

Mr. TURNER. Thank you. That is a very good question. It is almost as if during Vietnam we had a hard drive crash, and everybody forgot about the meaning of the executive power clause.

The term "executive power" was understood by the founding fathers, because they had read John Locke's Second Treatise on Civil

Government. They had read Montesquieu's Spirit of the Laws. They had read Blackstone's Commentaries on the Laws of England.

All of those, and many others, understood by its nature external business, foreign affairs, the conduct of war cannot be managed by large deliberative assemblies.

You have got to act with speed and dispatch. You have got to act with secrecy. Legislating bodies can't keep secrets. Thus, this is presidential business. This was part of the executive power.

In my testimony, I quote James Madison, Thomas Jefferson saying that—he quotes article II, section 1, the executive powers given to the President.

And then he said the transaction of business with foreign nations is executive altogether, and thus it belongs to the head of that department, except for those exceptions expressly vested in the Senate, which were to be construed narrowly.

Jefferson's chief rival in Washington's cabinet, Alexander Hamilton, made exactly the same point 3 years later as Pacificus. John Marshall, as a Member of the House of Representatives, said the President is the sole organ of the Nation in foreign affairs. He possesses the executive power.

I did a 1,700-page doctoral dissertation on separation of foreign affairs powers. I went through year by year and looked at congressional debates, looked at court opinions and so forth.

There was almost unanimity that certainly intelligence, certainly the conduct of diplomacy—in Curtiss-Wright in 1936, the Supreme Court said into the field of negotiations the Senate cannot intrude. Congress itself is powerless to invade it.

The same reason you don't get involved with negotiations is why you don't get involved in intelligence.

Now, the distinction is external and internal. John Marshall in *Marbury*—a great line. He talks about the President having certain powers under the Constitution that are confided to his discretion.

"Whatever opinion may be entertained on the manner in which executive discretion may be used, still there exists and can exist no power to control that discretion. Being entrusted to the executive, the decision of the executive is conclusive."

And to illustrate this, he mentioned in the next sentence the creation of the Department of Foreign Affairs, the presidential department, and he said courts cannot inquire into the official acts of the Secretary of State. This is a well-established principle that we lost about the time of the Vietnam debates.

And neither side mentioned this, but throughout our history it was understood the reason the President managed foreign affairs was because of the executive power grant.

And on intelligence, it was expressly discussed in the Federalist Papers. Congress can't keep secrets. Therefore, the Constitution has given the President power "to manage the business of intelligence as prudence might suggest."

And the gentleman from Massachusetts, who has left us, made the point of the importance of protecting the Constitution. I could not agree more. But what is being missed is Congress is usurping presidential powers.

Now, there is a gentleman's agreement here that I think works. If Congress can come up with a FISA that allows us to have an

extra check when they are talking about looking at American communications, I think that is wonderful.

But that will not be founded upon Congress directing the President to do something in the foreign intelligence area.

It will be founded upon the mutual interest of everyone wanting to protect the rights of individuals from unnecessary and unreasonable searches and Congress giving the President the flexibility he can do the job of protecting the country.

This is why I think it is so important that you work with the President, you are not dictating to him, because in reality you are trying to restrict his powers under the Constitution.

Mr. PENCE. I thank you.

I think my time has expired, unless there is other commentary on that, Mr. Chairman.

Ms. SPAULDING. Congressman, I would like to emphasize that the crux of the debate here, and certainly the crux of the FISA legislation, is not with respect to purely foreign affairs but, in fact, where it touches upon individual liberties of Americans inside the United States. That is the challenge with which we are wrestling.

And I would offer a more recent quote than those that Professor Turner was offering—Justice O'Connor in the Hamdan decision, who said that regardless of what authorities the President may have with respect to foreign affairs, surely when it comes to individual liberties—when individual liberties are at stake, it is clear that the Constitution envisioned a role for all three branches of Government.

Mr. BARR. If I might, at the gentleman's invitation, with the concurrence of the Chair, also respond briefly to that, with all due respect, the discourse between the gentleman from Indiana and the law professor is very interesting, but it is totally irrelevant to the gentleman from Indiana's question.

If he is inquiring about first principles, the first principles are that a United States citizen in this country is clothed with a sphere and aura of privacy that the Federal Government cannot invade, absent a good and sufficient reason, which there will be from time to time.

But that ought to be the focus of the debate here. We are not talking, I don't think, any of us here, about infringing the power of the President as the chief executive to gather foreign intelligence overseas or, under certain circumstances, in this country.

What we are talking about here, and the real problem with P.L. 110–55, is the fact that as Ms. Spaulding indicated, it implicates fundamental first principle constitutional liberties for citizens in this country who now, thanks to that law as signed by the President and passed with too much haste by this Congress—any call or e-mail—that is, any electronic communication—that a U.S. person has with anybody overseas, without any necessary hint of any association with a terrorist, is now subject to surveillance by the Government without any court supervision.

That is a violation of about as first principle as one can get. And I really think that that is where the debate ought to be, not on the intricacies of how far Article II might extend in foreign affairs.

Mr. PENCE. I appreciate that.

Just to conclude, Mr. Chairman, I appreciate the rebuttal remarks, but it is just imperative to me that as we reflect on the privacy rights of Americans, we also reflect on those long-term principles of separation of powers in Government that have served to protect the people of this country effectively over hundreds of years.

And with that, I yield back, grateful for the additional time.

Mr. CONYERS. Thank you.

The Chair observes that there were no hearings in the Judiciary on the amendments just recently passed that have a 6-month period before they expire, which now require us to begin to hold these hearings, which there was no opportunity to do in our haste before the recess.

The Chair is pleased to recognize the distinguished lady from Houston, Texas, Sheila Jackson Lee.

Ms. JACKSON LEE. Mr. Chairman, I want to take my first moment to thank you for your leadership and your complete commitment to the preservation of the Constitution.

I think that one of the things that we learned after 9/11—Mr. Chairman, you remember we went quickly to the steps of the United States Congress, purposely to show the American people that we would not be undermined and denied our liberty because of the horrific terrorist act of 9/11.

I remember singing "God Bless America," and it was really to show to the American people—Congressman Barr, you probably remember that we were not to be daunted in this enormous tragedy, in the face of this enormous tragedy.

And so, as I listened to the discourse between my good friend from Indiana and the distinguished professor from my alma mater, the University of Virginia School of Law—the Jeffersonian mission that that school has—I saw more than a reflection of this present underlying bill.

My recollection of Thomas Jefferson's original premise in the founding of this Nation was a healthy skepticism of authority does not mean that we don't have to have the laws necessary to protect America.

I have just left—and I apologize to the witnesses—the Homeland Security Committee which I am on and Secretary Chertoff discussing closing gaps on security in America.

And so we are not unmindful of that. But as I listen, Professor Turner—and I really just need a yes or no answer, because I hear an expanded view of the executive power.

So let me just read off to you the Bill of Rights, and I would like Professor Barr and the distinguished panelist to his right, Ms. Spaulding—I am sorry, I am being blocked out of your view—to also answer this in the context of this question.

And that is that the bill that was passed was under the premise of protecting America, and its premise was to surveil people overseas.

But frankly, what is happening, and I imagine has been discussed, is that it will weave its way into the bedroom, kitchen and other places of refuge for Americans.

This is, I think, the narrow focus of what we are trying to protect, and that is the basic underpinnings of civil liberties, while at the same time we promote the sharing of intelligence.

For those of us who are here, we remember the key underlying cause of 9/11—individuals in our intelligence community not talking to each other, not necessarily not having the right intelligence, but not talking to each other, with clear evidence of what might have been happening.

And so we were very cautious not to then take the terrorist act and terrorize Americans.

Professor, are you suggesting that executive powers during this very difficult time would then have the right to eliminate the freedom of press, the freedom of speech, to eliminate Americans' right to carry arms, of which—I happen to be someone who defines the second amendment differently, but America's right to carry arms, America's right to the protection against unreasonable search and seizure, America's right to due process, Americans' rights to a trial by jury?

Is that the expansive executive power that you are now promoting, that in times like these we, then, yield to the auspicious and, I might say, oppressive power of the executive and allow them to eliminate all these rights?

Is that your position today?

Mr. TURNER. I am always wary of yes or no questions. I stopped——

Ms. JACKSON LEE. But I asked for——

Mr. TURNER [continuing]. Years ago.

Ms. JACKSON LEE [continuing]. Is that your position today?

Mr. TURNER. Not at all. If you will read my testimony, the distinction is the President's, in many respects, exclusive power dealing with the external world, versus what you are talking about, internal.

The fourth amendment——

Ms. JACKSON LEE. And may I just——

Mr. TURNER [continuing]. Is just as enforced today as it is in peace time, but what is an unreasonable search may change when you are trying to stop a terrorist attack.

But certainly, I don't suggest at all that the President can suspend the Constitution or something like that. Quite the contrary.

Ms. JACKSON LEE. Thank you, Professor.

Congressman Barr, is it not possible to take the argument and the premise that the professor has made in his previous comments, including his testimony, even though he has now suggested the distinction of war time versus peace time. But if we don't look to provide some parameters for this warrantless wiretapping structure that does not invade improperly the civil liberties of Americans, is that not the possibility of the expansion of executive powers?

Mr. BARR. Well, it certainly is a possibility, and as a matter of fact a number of advocates for the Administration's policies regarding enemy combatants, regarding military tribunals, regarding foreign intelligence surveillance—all these areas and more—argue that the President has, in fact, in their view plenary authority under article II, sections 1 and 2, as commander in chief to do all of those things that you have enumerated.

Ms. JACKSON LEE. Ms. Spaulding?

Ms. SPAULDING. I think we have to be wary of expansion of executive authority and the skewing of our system of checks and balances, not just because we believe strongly in civil liberties, but there are also national security costs to that kind of avaricious accumulation of power and ignoring our system of checks and balances.

And I think it can be seen most clearly in the lessons we have learned from community policing. We are concerned about homegrown terrorism.

We are not likely to detect some young man sitting in his basement contemplating a terrorist attack through these expansive FISA powers, even as amended.

We are most likely to be able to successfully address homegrown terrorism by developing a close relationship with our communities, and particularly our Muslim-American communities.

They are deeply suspicious when the Government starts asserting this kind of broad power that infringes upon Americans' rights. And they know they are particularly vulnerable population, particularly in this context with this threat.

And I think it begins to drive a dangerous wedge and makes us less secure, not more secure.

Ms. JACKSON LEE. Mr. Halperin, would you comment?

Mr. HALPERIN. Yes. I think that we give up our liberty and do not gain our security. My basic point about FISA is that it has worked. The number of——

Ms. JACKSON LEE. That it is—I didn't hear you.

Mr. HALPERIN. Has worked. After it was enacted, the number of surveillances went up. Every director of central intelligence since has testified that they were able to conduct more surveillances and gain more information, because Government officials, officials of the phone company, landlords of people whose houses you needed to get into, all knew that they were doing something that was lawful, that Congress had authorized, that the courts had sanctioned, and that therefore they had an obligation to cooperate.

Before FISA, you had a situation in which you didn't have anywhere near as much cooperation and therefore much less surveillance.

The first leak that occurred of the foreign intelligence surveillance since the enactment of FISA was the leak of the President's program going beyond FISA and conducting surveillances outside of FISA.

And that leaked because some of the people involved did not believe it was lawful. We know one of the telephone companies refused to cooperate because their lawyers, I think properly, told them it was unlawful.

We now have the Government coming into the Congress desperately seeking new legislation because a court has said you violated FISA.

We protect our security, as we protect our civil liberties, by doing what this Congress did in 1978, which is enacting clear laws with clear obligations for everybody, with a clear role for the Congress and for the FISA court.

And when we break that rule, as we did in this legislation, we jeopardize our security as much as we jeopardize our civil liberties.

Ms. JACKSON LEE. I thank the Chairman.

Mr. CONYERS. I thank the gentlelady from Texas.

The Chair is pleased to recognize the Ranking Member of the Immigration Committee, the gentleman from Iowa, Steve King.

Mr. KING. Thank you, Mr. Chairman. I appreciate you holding this hearing here today and appreciate the testimony of the witnesses and I will say the expert perspective that is brought by each of you.

And I just have a few curiosities left. My colleagues have done a very good job, I think, of combing out a lot of the wrinkles that we have had here in this Committee.

And at first, I direct to Professor Turner. We passed the Protect America Act and completed into law August 5, and you understand the background for that. Would we have been better off not to have addressed this issue, in your opinion?

Did we take a step that was an improvement in the right direction? Should we back up a little bit? How would you summarize your recommendation, if there should be any changes made?

Mr. TURNER. Well, I think there is a consensus here that we are in a situation, as the Administration has explained—the DNI has explained—that new technology has made it—turned FISA on its head.

Things that used to be legal under FISA now can't be done because of the way the technology works. We need to have a technology-neutral FISA. And to me, the focus of FISA should be on protecting the rights of U.S. persons in this country.

The situation we were in before you acted—we were actually being told we could not listen if bin Laden called his number two across town in Pakistan somewhere because of Congress and the way you wrote this law. Which, again, proves the wisdom of Locke when he said you cannot manage these problems by antecedent, standing, positive laws because you cannot anticipate all the changes.

You know, the loss of a battle, the resignation of a minister might change a bad situation to a good one, and so Locke said those who preside must be left in position to act for the common good. This is a wonderful example when Congress gets into this area.

Now, I want to make it very clear, I have not suggested the President has any power to suspend the first amendment, or the fifth amendment or the second amendment. The distinction here is foreign-domestic.

There was a 1971 Committee of experts of the American Bar Association that said the President ought to be able to wiretap people in this country for foreign intelligence persons, but when the target is a domestic threat—in that case, it was a White Panther who worked for the Black Panthers, who had blown up the CIA building and was found with many pounds of dynamite and maps to American military bases.

The Supreme Court in the *Keith* case said you have to have a warrant. If it is an American threat, fourth amendment—you know, of course, fourth amendment applies all the time, but the

Supreme Court has carved out a number of safety-related exceptions to the fourth amendment, including the——

Mr. KING. I agree, Mr. Turner.

Mr. TURNER. And this is one of them.

Mr. KING. But you set up a question here, now, and that is these decisions that were made by the several judges that brought us into this situation—do you believe, then, that the executive powers of the United States should have been suspended with regard to intelligence gathering until Congress acted?

Mr. TURNER. No. I think Griffin Bell got it right. I think the President has the power to do this that is a higher power than your power to limit——

Mr. KING. Okay. Let me take you, then, if I might——

Mr. TURNER. Had you not passed this, I would have recommended the President just ignore FISA and continue listening to bin Laden. But I would rather see him work—I like FISA.

But FISA ought to be understood as an agreement, not as controlling the President, because in the end, he wins, because his constitutional power prevails in this act.

Mr. KING. Okay. And I appreciate your constitutional perspective, so I would ask this following question, and that is when there is a court decision that the executive believes runs contrary to the constitutional authority of the executive branch, then what is the duty—or the Congress, for that matter.

If we believe that there is a decision made by the court that is inconsistent with the Constitution, do we honor that decision and comply—and conform the law to match that decision of the judge? Or do we ignore that?

What is your recommendation on how Congress should act or the executive branch should act when we find ourselves in disagreement with the constitutional interpretation of a judge?

Mr. TURNER. This is an easy one. The Constitution is supreme. The courts have the supreme authority to interpret the Constitution. If a court says this is unconstitutional, you stop doing it, and if you disagree, you immediately appeal.

When the Supreme Court rules, that is final, except you can then try to amend the Constitution. Ultimately, the American people are the boss, but until they change the Constitution, it binds all the branches.

Mr. KING. Okay. But Ms. Spaulding quoted from the Hamdan case, a case where we clearly used article III, section 2 stripping language, and the Supreme Court was denied jurisdiction in that case. They heard it anyway.

And so are you suggesting, then, that for the Congress or the executive branch to maintain their authority in this balance of powers we would have to go to a constitutional amendment to remind the Supreme Court what the Constitution says in article III, section 2?

Mr. TURNER. That is an interesting question, and it is really a political question. But the basic point is ultimately the courts prevail on interpreting the Constitution. If you believe the courts violated the law, I am not sure what the answer to it is.

But if they—obviously, if it is an interpretation of the law—in fact, any time they say it has to do with the law, you just change

the law. If it deals with the Constitution, you accept it or you amend the Constitution.

Mr. KING. If I might, then, just very quickly conclude, and that is that each branch of Government—if we do not jealously protect the power and authority granted to us in the Constitution, we will lose it to another branch of Government.

I thank you very much for your testimony.

And I yield back.

Mr. CONYERS. The Chair is pleased to recognize the distinguished gentlelady from California, Maxine Waters.

Ms. WATERS. Thank you very much, Mr. Chairman. This has been an interesting and fascinating discussion. Sorry that I was not able to be here for all of it. We are looking at home foreclosures over in the Financial Services Committee.

But I was anxious to get back here, because I think that this is an issue that must be dealt with by the Congress of the United States.

As a matter of fact, I was disheartened with the passage of the Protect America Act when we left here on August 5, 2007. And I know that Congress is a very complicated place, and that often times actions are taken, decisions are made, based on the complication of the makeup of this body.

But I was not a very happy camper because that act was passed, even though it is temporary.

And I am so glad, Mr. Chairman, that you are revisiting this as quickly as could possibly be done and having us here today, because I know that there is going to be a coming together of both sides of the aisle eventually to deal with this, as demonstrated by my former colleague, Mr. Bob Barr, who is here today.

As Mr. Barr knows and many of you know, I disagree with him on a lot of things. But he has been absolutely spectacular on this issue.

And he and the ACLU literally have formed a partnership on the protection of civil liberties, and I have a real appreciation for that.

I am also pleased to hear the professor here today, because I know now why I am so frightened about the President of the United States and his ability to ignore the Constitution of the United States and to place American citizens under surveillance.

And I need to hear people like the professor explain why they think the way that they do, so it could help to keep me focused on why I must fight very, very hard to ensure that the President does not use the power of the presidency to spy on American citizens, or to ignore FISA, or simply to violate the Constitution, in my estimation.

Now, having said all of that—and I think this issue has been framed very well here today, and we probably all know where we stand on it. And we can wax eloquently about what the Constitution meant, and some can, I guess, emerge as strict constructionists, others more liberal.

But I want to get to what it really means for an American citizen to be spied on by their Government. And we have someone here today who is presenting as a witness, Mr. Mort Halperin, who was targeted as an enemy by the Nixon administration.

And I would like to hear from Mr. Halperin what you learned about surveillance of your family. I want to know why did the Government target you. What did you do about it? And help us put a face on this here in this Committee today.

Mr. HALPERIN. Well, thank you. I discovered that there was a warrantless electronic surveillance on my home phone. I sued the Government. The case went on for many, many, many years.

We took the depositions of vast numbers of people. All of them modestly assured us that they had nothing to do with the decision to put the tap on my home phone. Mr. Nixon, Mr. Kissinger, Mr. Haldeman, the deputy director of the FBI all insisted that somebody else had made the decision.

But the fact was that the FBI listened to my home phone conversations and those of my family for 21 months, learned at the end that according to General Haig, nothing suggested that I was a leaker of information.

They learned about the Muskie Presidential Campaign. They learned about Common Cause's campaign against the Vietnam War. They learned about my shopping habits, particularly what groceries I tended to buy, and other information relating to political activity that they had no business acquiring.

We sued, among other people, the telephone company. And I think that actually played an important role in getting us to FISA, because the phone company was starting to get sued by a number of people.

They had acted on the assumption that the Government always behaved in good faith. This tap was put on the way they all were put on. There was a phone call from an assistant director of the FBI to the security officer in the telephone company.

Now, of course, in those days, there was only a telephone company. It was very simple. And then they would provide all the phone calls to the FBI field office—in this case, the old post office building down on Pennsylvania Avenue—where they listened to the calls.

But I think the lesson there was that you can't trust the Government, that if the President has the power to pick up the phone and call the FBI and get a wiretap, he will do it on Martin Luther King, Jr. He will do it on steel company executives. He will do it on Government officials.

He will do it on newspaper men, as well as on the girlfriend of the Russian ambassador, and that therefore we needed rules. We needed clear rules for the phone company and for Government officials about when this was appropriate and when this was not appropriate.

And I think out of that came FISA, which I strongly supported, believed it was the right thing to do, and now strongly support amendments to make sure that we can listen to phone calls between two terrorists overseas but not do it in a way that allows the Government to acquire vast numbers of conversations of Americans.

Ms. WATERS. Can you regain the trust of your Government once you have been violated in the way that you have described, or are you forever looking over your shoulder, you are a little bit nervous about being spied on?

What does this do to an American citizen to find that their President has violated the law and the Constitution and spied on you?

Mr. HALPERIN. Well, I think, obviously, different people react different ways. My reaction was to say we have to fix the problem. We have to fix the problem by Congress enacting clear and firm rules.

We should not be in a position where an FBI official, or an NSA official, or CIA official, or the President or the Attorney General is not clear what the law permits him to do.

And that is why I thought that FISA was so important. I devoted much of my time for 3 or 4 years to the debate about FISA, because my view was there were some conversations that the Government had to be able to listen to.

At the same time, the American people needed to be assured that they would not be surveilled without a warrant.

And after 9/11, when people said to me, "I will bet they are listening in again to our conversations without a warrant," I said what the President said, "They can't do that. A court order and a warrant is required."

And then we found out the President was lying to us, that he was listening without a warrant to those conversations. And he destroyed the whole system of trust that had been built up in the enactment of FISA.

And then the Administration destroyed it again by demanding a bill without explaining what it meant or what it did in a way that people could understand.

And as I have said several times, my view is that threatens our security as much as it threatens our civil liberties. And it breaks the bond of trust that FISA created between our citizens and the Government, and we all know we what the rule were and we all knew that the rules would be enforced.

And I think Congress has to reestablish that system of trust, and it can do so in any way that gives the director of national intelligence access to the phone calls that he should be able to listen to.

Ms. WATERS. Thank you very much, Mr. Chairman.

Mr. CONYERS. Thank you so much.

The Ranking Member of the Constitution Subcommittee, the gentleman from Arizona, Mr. Trent Franks?

Mr. FRANKS. Well, thank you, Mr. Chairman.

And thank all of you at the panel here. You know, sometimes it is important just to kind of come back to earth a little bit.

And I am reminded that when 9/11 came upon America, there were over 2,500 Americans that were almost instantaneously stripped of their right to live, of their right to be free, and their right to pursue their dreams.

Almost everything that any of us hold dear was taken from them in an almost blinding instant.

And it reminded our Government that they have a profound responsibility to protect the citizens of the United States.

It also reminded them that they face a different kind of enemy than we have ever faced, an ideological one that lurks behind the shadows and is an asymmetric threat that is difficult to define and to ascertain where and what they are trying to do.

With that in mind, even intelligence becomes a critical and overriding issue. If we knew where every terrorist was in the world today and what they were planning, the war on terror would be over in 60 days. Our greatest challenge is intelligence.

So in the effort for all of us to protect the civil liberties of the United States and the people in it, we have to consider the importance also of foreign intelligence.

With that in mind, as I understand, Mr. Turner, let me just try to, if I can, walk through this a little bit, and you are welcome to say to the whole world where I am right and wrong.

But as I understand it, the Protect America Act essentially says that—like it was originally envisioned, that the foreign intelligence surveillance having to do with people not on this Nation's territory, could be done by the President largely without any kind of warrant, that he could listen to Terrorist A in Morocco and Terrorist B in Abu Dhabi and could make his own conclusions there as to whether or not they represented a threat to the United States, but that if someone in the United States was targeted, that there had to be a warrant.

And I understand that the rub comes when someone calls—a terrorist, perhaps, calls into the United States to someone that is not a targeted person under any warrant. And there are those of the majority that suggest that that is unconstitutional.

Is it not true, however, that if a terrorist calls someone in the United States, that of all considerations, of all calls that should be considered carefully, that that would be among the most important ones to consider?

And I understand that if there is some criminal discussion on the part of the person that is being listened to here in the United States as a result of listening to a terrorist phone from outside the United States that before that person can be targeted for any type of criminal investigation that they have to get a warrant to do that.

Is that correct, Mr. Turner?

Mr. TURNER. That is a good question, and I am not certain. It seems to me there are two regimes here. Going back to the ABA report in 1971, their argument was the President could do foreign intelligence wiretaps without a warrant.

That would include a foreign agent, a foreign government official, a terrorist—what have you—calling in.

They listen. If the American is not saying, "Hey, where do I get the explosive," but rather is trying to say, "Where do I send the lamp you bought on eBay," then the minimization procedures come in and they erase, you know, the tape and everything else.

The other issue is the FISA regime. I am not certain whether—I think FISA, if you are targeting the foreigner outside the country, where you have got every right—certainly, everybody agrees it is legal—the President has a duty to try to find them and target them or find out what they are doing.

I don't think you need a FISA warrant for the individual in this country. Certainly, you shouldn't. Certainly, the President should have a right to intercept that.

Mr. FRANKS. Well, that is as I understand——

Mr. TURNER. Yes.

Mr. FRANKS [continuing]. The situation, and I wanted to try to make that——

Mr. TURNER. That was before the latest interpretation over the technology that if it goes—now, anything that goes through a switch in this country——

Mr. FRANKS. Right. I think the technology, Mr. Chairman, is what made a lot of the challenge here—is that sometimes now those come through the United States, and that is what has caused the new discussion here.

And I will just close here, because I am about out of time. But the director of national intelligence has said that prior to the passage of the Protect America Act of 2007 that the intelligence community was "actually missing a significant portion of what we should be getting with respect to terrorist communication."

And, Mr. Chairman, I just am convinced that the Protect America Act does everything it possibly can—and I am open to making it better—to protect the civil liberties of those residing in the United States and still helps protect the country from those who are malevolent outside the United States.

And, Mr. Turner, if you would like to respond to that——

Mr. TURNER. Just one quick comment related to the Mort Halperin situation. I think everybody agrees that bug should not have taken place.

It is very clear under the *Keith* case in 1972 the Supreme Court has said you need a warrant to bug a person in this country, unless you have got reason to believe that person is tied to a foreign power, a foreign terrorist group or something like that.

So what happened there has already been taken care of by a Supreme Court ruling, quite properly.

Mr. FRANKS. And just for the record, Mr. Chairman, that is the case under the Protect America Act. Thank you.

Mr. CONYERS. The gentlelady from New York, Sue Sutton.

Oh, excuse me, the gentleman from Tennessee, Steve Cohen.

Mr. COHEN. Thank you, Mr. Chairman. I appreciate it.

Most of the questions, I guess, have been asked, but I do have a few thoughts and questions.

Congressman Barr, you were here—most of the discussion has been about foreign terrorists, and certainly that is our primary concern.

But before 9/11, our primary terrorist attack was some yahoos out in the Big 12 conference, Oklahoma, Colorado, Nebraska, wherever they were, and Oklahoma City.

After that attack in Oklahoma City, was there any discussion of changing the constitutional history of this country to have surveillance on domestic terrorists to protect us from that threat?

Mr. BARR. There were some discussions, for example, as the gentleman from Tennessee may recall—even though he wasn't in the Congress, I know he followed these issues.

There was some discussion in the initial antiterrorism legislation that was crafted in the wake of the Oklahoma City bombing that did—a number of us across the political spectrum believed did improperly infringe constitutional rights of our citizens, and at that time we defeated those. Those did not pass as part of that legislation.

Mr. COHEN. Did anything pass to give additional authority to the Government to intercept any conversations or documents of any sort?

Mr. BARR. No.

Mr. COHEN. Were the proposals ones that were tailored strictly to terrorist activity?

Mr. BARR. Some of the proposals went apparently far afield of the specific focus that a number of us believed should have been the focus of legislation to address the particular problem that manifested itself in Oklahoma City.

And here again, we were able to curtail those.

Mr. COHEN. And either you or Ms. Spaulding—this legislation that we passed was not strictly limited to terrorists, is that correct?

Mr. BARR. As the Chair, I think, is—or as the gentleman from Tennessee is implying here, the scope of P.L. 110–55, which is the Protect America Act, goes far beyond targeting terrorists.

Virtually any phone call or e-mail, any electronic transmission, communication, that a U.S. citizen in this country makes to anybody overseas, regardless of any connection whatsoever or even a mere suspicion that they are a terrorist or connected with a terrorist, is now subject to surveillance without court order, supervision or effective oversight by the Congress simply because that U.S. person is communicating with somebody overseas.

That goes far, far beyond anything reasonably necessary to address the problem of terrorism.

Mr. COHEN. And so, Ms. Spaulding, would you like to respond?

Ms. SPAULDING. Well, I was just going to respond to the argument that was made for why this bill was not limited to issues related to international terrorism.

And the example that was given, that suppose a terrorist group is talking with a foreign government about trying to purchase nuclear weapons or obtain other kinds of weapons of mass destruction—that still is related to international terrorism.

And an appropriately focused legislation that restricts itself to the threat posed by international terrorism could, indeed, encompass those kinds of threats.

Mr. COHEN. Do you have words of art that you could offer to the Committee?

Ms. SPAULDING. Congressman, I would be more than happy to work with the Committee to try to find the appropriate way to address all of these challenges.

Mr. COHEN. Thank you.

Do any of you know of any situations where the fact that some request for some surveillance went to the FISA court and had that time limit affected the security of this country?

Mr. TURNER. Mr. Chairman, I—or sorry.

Mr. COHEN. That is all right.

Mr. TURNER. Maybe later. Right. I don't know of any, but there is no reason I would, since all of that is classified.

Mr. HALPERIN. The Attorney General, I thought, in his testimony did lay out the situation which supposedly justified the terrorist surveillance program because there was not time to go to court.

I thought they did make out a case for why the emergency procedures needed to be lengthened in time in order to be able to deal with those particular surveillances.

The Administration seems to have lost interest in that amendment. It is not in their package anymore. I don't know how the problem went away, but I think it does need to be fixed.

Mr. COHEN. Thank you.

When this bill came up for vote, I voted no, as did most of my Democratic colleagues. There were lots of reasons to vote no, most of which are the subject matter and the concern of the fourth amendment, the courts, the tradition of American jurisprudence.

But one of the other reasons is because this bill gave a great deal of authority to the Attorney General of the United States.

This Committee, under our Chairman, had hearings which I think exposed certain problems in the Department of Justice and with our current Attorney General.

Because of the oversight of this Committee, as well as the oversight of the Senate, I believe issues were raised, responses were not given, that led to the resignation of our Attorney General, which will give this Congress and this congressman possibly more confidence in giving the Attorney General authority which he didn't have.

On that night when I voted no, I said that one of the reasons I voted no is because the American people did not trust this Attorney General with additional authorities, having seen what he had done with former Attorney General Ashcroft on his sick bed.

And I called on his resignation that night. I am pleased that he has announced his resignation. And I think this Committee, because of the hearings the Chairman has had—we have seen a hero emerge, and that was Mr. Comey. James Comey is an American hero.

And, Mr. Chairman, I have called in Memphis, Tennessee—and some of you may know it, but I believe if the President would appoint James Comey—or nominate him as Attorney General, we would feel a lot more comfortable with this law and the laws of this entire country.

And he would show that he was putting the country first, because he is a hero who will do what is right under the Constitution and the laws of the United States and not act as a political tool of any individual. And I would encourage the President to do so.

Thank you, Mr. Chairman.

Mr. CONYERS. Well, there are others on the Committee that share your view, Mr. Cohen.

I am pleased now to recognize Judge Louie Gohmert of Texas.

Mr. GOHMERT. Thank you, Mr. Chairman. I do appreciate this hearing.

And I do appreciate when we have a panel whose I.Q.s collectively enhance the I.Q. of the room itself, so we appreciate you all being here.

I would like to just ask some very basic questions so I know where everybody is. That helps me judge, you know, the credibility, weight, that kind of thing, for the testimony.

But first of all, I would like to ask a simple question to each.

Mr. Barr, you are looking at me sternly there—simple questions—but just to get an answer—and it should be yes or no. I am not trying to trick anybody, but just to find out where you stand.

First question: Are U.S. citizens located in foreign countries entitled to the rights in that country that are afforded under the United States Constitution?

Mr. Barr, if we could just go down the row?

Mr. BARR. In the context of the discussion regarding FISA, no.

Ms. SPAULDING. Most constitutional rights travel with Americans when they travel overseas vis-a-vis their relationship with the United States Government.

Mr. GOHMERT. So would that be——

Ms. SPAULDING. Yes.

Mr. GOHMERT [continuing]. A yes? Okay. Thank you.

Mr. TURNER. I think it is more complex than that, but I think most constitutional rights, you know, would carry over with respect to the U.S. Government, but I also agree with Mr. Barr with regard to some of the surveillance issues.

The question is whether they have a reasonable expectation of privacy, and I think one of the things you have to ask—the only country in the world that has a fourth amendment is the United States.

You go to France today, if you are a businessman—you had better be sure your briefcase is going to rifled while you are at lunch by the French intelligence.

And so, you know, the test in the fourth amendment—one, is there a reasonable expectation of privacy? If there is, is the search unreasonable?

Mr. GOHMERT. But going back to the question, you are saying there is no expectation of privacy by an American citizen in France, but nonetheless their constitutional rights have to be observed?

Mr. TURNER. Well, the answer there is the fourth amendment may not apply by virtue of the fact that they have to have an expectation of privacy for it to apply.

But most of the provisions certainly do apply to Americans overseas with respect to their relation to——

Mr. GOHMERT. Well, Professor, you have been so clear-spoken throughout your testimony. I think this is the most befuddling your answers have been so far in this hearing.

And I am still not clear where you stand on that question.

Mr. TURNER. Most constitutional rights do carry with them with respect to our Government with respect to——

Mr. GOHMERT. Even when there is no expectation of privacy.

Mr. TURNER. No. That is the key. The fourth amendment may apply, but if it does apply, they are probably excluded from its protections——

Mr. GOHMERT. But you just gave an example, France. You got no expectation——

Mr. TURNER. Yes, they don't have——

Mr. GOHMERT [continuing]. Of privacy.

Mr. TURNER [continuing]. An expectation of privacy. You know, that is the trigger for——

Mr. GOHMERT. So if you are a moron and you go into a country thinking you are going to have an expectation of privacy, even

though you clearly don't, then the fourth amendment follows you, is that——

Mr. TURNER. You know, I would have to research that one. I have never researched it, and the reason I am befuddled is because I am trying to think it through, and I don't——

Mr. GOHMERT. Okay.

Mr. TURNER [continuing]. Even know if there is any case law——

Mr. GOHMERT. Well, I really wasn't trying to be tricky here.

Mr. TURNER. Yes.

Mr. GOHMERT. Like I say, you have been pretty clear-spoken——

Mr. TURNER. I think I agree with Mort.

Mr. HALPERIN. Yes, he is going to agree with me.

Mr. GOHMERT. All right. Your answer?

Mr. HALPERIN. The Constitutional fully protects Americans against their own Government's actions whether they are at home or abroad.

The fourth amendment is situational both at home and abroad. For example, you are not protected against Government seizures of your conversations if you sit in your house and talk loudly enough for someone else to hear outside, because the court has said——

Mr. GOHMERT. Are we talking about in a foreign country? Because that was my question.

Mr. HALPERIN. No, but what I am saying is the fourth amendment applies equally in a foreign country as it does in the United States. Most——

Mr. GOHMERT. So expectation of privacy means nothing.

Mr. HALPERIN. No. It means something both in the United States and——

Mr. GOHMERT. But I am asking about a foreign country.

Mr. HALPERIN. Yes.

Mr. GOHMERT. And that is rather a subjective standard that you——

Mr. HALPERIN. But that is the one——

Mr. GOHMERT [continuing]. Have mentioned.

Mr. HALPERIN. It is the one the court has——

Mr. GOHMERT. And apparently it is a moronic offense if you are a moron and think you have got an——

Mr. HALPERIN. No, no.

Mr. GOHMERT [continuing]. Expectation of privacy.

Mr. HALPERIN. It is a reasonable person.

Mr. TURNER. That is the key.

Mr. HALPERIN. It is a reasonable person.

Mr. TURNER. It is a reasonable expectation.

Mr. GOHMERT. All right. All right. But this question is not—I didn't say constitutional rights with respect to intrusion by the United States Government.

Do they have a right to expect protections under the U.S. Constitution when they are in a foreign country?

Mr. HALPERIN. Against a foreign government?

Mr. TURNER. No.

Mr. GOHMERT. Right.

Mr. HALPERIN. Not at all.

Mr. TURNER. We all agree on that, I am sure.

Mr. GOHMERT. And is that your belief? As regards a foreign government, a U.S. citizen abroad has no expectation of the observation of U.S. constitutional rights? Is that fair?

Mr. TURNER. It is still more complex than that. For example, if a foreign government were to threaten the life of an American citizen abroad, that person would have an expectation that our Government would use its—you know, would make an effort to protect their, you know, safety and so forth.

Mr. GOHMERT. Okay. But then that raises other issues, and that would be unless it is an unborn child, and then you would have no expectation the U.S. Government would protect that life. But that is another issue.

Well, let me go to another question. Do you believe terrorists located in a foreign country who is of foreign citizenship is entitled to protections and rights afforded under the U.S. Constitution to U.S. citizens?

Mr. Barr? Foreign terrorists in a foreign country.

Mr. BARR. No connection with the U.S.

Mr. GOHMERT. No connection with the U.S.

Mr. BARR. No.

Ms. SPAULDING. No, that terrorist does not enjoy any constitutional rights.

Mr. TURNER. I am sure we all agree on that.

Mr. GOHMERT. Well, I just wanted to make sure, because I wasn't.

Mr. HALPERIN. Yes, we agree on that.

Mr. GOHMERT. Okay. And we got into—answer this question with regard to my first question—but are foreign intelligence agents in foreign countries trying to surveil foreign terrorists required to provide them with constitutional rights under the U.S. Constitution?

The answer apparently, from your last question, would be no, correct?

Mr. HALPERIN. Right.

Mr. GOHMERT. I appreciated my friend from California, Mr. Lungren, getting into the minimization issue. I have had some concerns that perhaps we have not had adequate—well, let me just mention this as a final comment. I see my time has expired.

I am very concerned that as we continue to have a lack of border security that in order to provide protections people want there is more and more usurpation of civil rights, and I would hope that we would have more border security to protect us there than have to keep encroaching, as apparently we have been going on some of the rights or perceived rights.

And I yield back. Thank you, Mr. Chairman.

Mr. CONYERS. You are welcome, Judge.

Several Members have allowed Debbie Wasserman Schultz of Florida to precede them, and we thank them for their courtesy.

The gentlelady is recognized.

Ms. WASSERMAN SCHULTZ. Oh, thank you so much, Mr. Chairman.

And to my colleagues, I appreciate the courtesy.

At the risk of dumbing down the very important and eloquent debate that has gone on and discussion that has gone on here today—I am not an attorney, and that is not an apology. It is just a fact.

And so because we have spent a lot of time speaking at a very high level, in very constitutional terms, in very legal terms, I want to ask my questions through the prism of someone who looks at an example like the following.

In my view, the FISA law that we just adopted, which I voted against—and Congressman Barr, I have to tell you that it is a privilege to be in the same room with you and not be yelling at you from my couch, which I did for many a year.

Mr. BARR. It is a privilege I share with you. I enjoy it.

Ms. WASSERMAN SCHULTZ. So I appreciate the opportunity to both agree with you, for once, and be in the same room.

But the question that I have for you—I would like you to comment on this, if you will, and Ms. Spaulding as well, and Professor Turner, if the time allows.

I look at this from this standpoint. The FISA law that we just passed would, in my estimation, allow the surveillance of an e-mail between my child and an Iraqi child communicating perhaps innocently, most likely innocently, about their views on the war, from an American child's perspective and an Iraqi child's perspective.

The Iraqi child would, you know, be someone in another country, would be—the discussion would possibly be related to foreigners or foreign affairs of the United States.

It seems to fit into the category of being eligible for surveillance and also, by almost every American you would ask, be an unreasonable communication to surveil.

Yet we would have no way of knowing whether the surveillance of that communication was reasonable, because there is no court review under this new version of the law, and there is no judge that is going to apply a reasonable standard or a constitutional standard to that surveillance.

Is that an accurate depiction or concern?

Mr. BARR. It is both an accurate depiction and ought to be a very major concern for certainly all of us.

Not only is the scenario that the gentlelady from Florida laid out a very accurate one, the fact of the matter is that the minimization procedures that are incorporated now in the FISA law as a result of P.L. 110–55 are dramatically different from earlier and other minimization procedures.

They are essentially just a sham. There is virtually no way that a court, even with the limits of review that it now has in this category of communication, could do anything more than simply pass judgment on whether the Government has made a clearly erroneous decision that somebody—that one of the parties is located overseas.

Ms. WASSERMAN SCHULTZ. I mean, and for those that would think that my question is an over simplification or is not reasonable to suspect that the Government might surveil that kind of communication, we do have Iraqi children blowing themselves up.

So I mean, there is a use of children in an entirely inappropriate and unacceptable way in that country and in other countries.

So it is not unreasonable to suspect or worry that innocent communications could be surveilled because of the difference in values or—well, values would be the best way to describe it, with how

children are treated in other countries—some other countries versus ours.

And thank you for your comment.

And, Ms. Spaulding?

Ms. SPAULDING. I think the example you gave is appropriate, and I would point out that by the example you gave, if the Government is targeting that Iraqi child and not your child, that they don't even have to be discussing foreign intelligence——

Ms. WASSERMAN SCHULTZ. Right.

Ms. SPAULDING [continuing]. That, in fact, it is simply taken entirely out of the definition of electronic surveillance. The only requirement is that the target be overseas.

Ms. WASSERMAN SCHULTZ. And the reason that I brought up this example is because it really—this is an insidious law, and it would be really—I have just been sitting here over the 3 hours thinking it would be really hard for most of our constituents, as individual Members of Congress, listening to this hearing, to grasp a lot of what we are talking about.

And not that we don't have smart constituents, we do, but you know, if you don't have a law degree, it is hard to follow what we are saying and apply it to your everyday situation and wonder and worry how the law that we changed in July would potentially impact you.

So I asked that question because I wanted to use an example of how an average, everyday person, not even an adult, but a kid could be impacted by this insidious law.

And, Professor Turner, I assume you will not agree with my characterization, so I would love to hear your opinion.

Mr. TURNER. I think it is a good question. I think the Supreme Court has told us in these kinds of cases your daughter has fourth amendment rights.

And in assessing the degree to which the Government can search—you know, can intrude upon your privacy, if you will, we balance the two interests. The strongest governmental interest of all is national security, protecting—preventing the next 9/11.

Now obviously, NSA doesn't have enough people to sit there and read the billions of e-mails that flow back and forth. Presumably—and I have been out of the business 23 years, so I don't know anything classified anymore.

But presumably, they have computer programs that scan e-mails and say who is talking to bin Laden, who is talking to here, who is using the words "blow up America" or whatever, and then maybe somebody looks at that, and so it is possible——

Ms. WASSERMAN SCHULTZ. But, Professor——

Mr. TURNER [continuing]. That somebody would spend 10 seconds scanning at your daughter's e-mail and trying to find the one that—the odds are good that would go through with no trouble at all.

Ms. WASSERMAN SCHULTZ. But my time has expired, but——

Mr. TURNER. Go ahead.

Ms. WASSERMAN SCHULTZ [continuing]. But kids use terms like that. Kids don't——

Mr. TURNER. I know.

Ms. WASSERMAN SCHULTZ [continuing]. I mean, kids talk about blow up and use——

Mr. TURNER. I know that, and——

Ms. WASSERMAN SCHULTZ. They use extreme words.

Mr. TURNER [continuing]. It is possible they might see that, and it would take them 2 or 3 seconds to say kids, ignore, and then minimization procedures would say protect her name, nothing goes to anybody on this, and the record gets destroyed.

And the question is is it so important when we are trying to find terrorists—you know, is this so offensive to her that somebody might look at this—I mean, every time we do a fingerprint search, Government computers search my fingerprint records.

They have got at least 10 copies. I was an Eagle Scout, and I sent them myself back in the 1950's, and then every security clearance they get a new set. You know, that is not, in my view, a violation of my privacy, the fact they have a computer scan through that.

The fact that NSA scans telephone records to find out what members are talking to terrorists—they probably scan my number. That is such a minor violation of any right I may have. It doesn't bother me in the least.

Ms. WASSERMAN SCHULTZ. But you are using words like "hopefully" and "probably." And the point is that without——

Mr. TURNER. Well, here is the key.

Ms. WASSERMAN SCHULTZ [continuing]. A court review, we really don't know.

Mr. TURNER. The alternative is if we say we don't want our Government seeing any e-mails that have U.S. persons on them without a warrant, what that means is bin Laden, every e-mail he sends he is going to copy some American person.

Maybe the way he will do it, the subject line will be "cheap Mexico Viagra," two pages of gibberish, and then pick up the explosives here and take them to the Capitol building.

Mr. BARR. With all due respect——

Mr. TURNER. If we say we have to have a warrant, we can't read that.

Mr. BARR [continuing]. That is a red herring. We are not talking about Osama bin Laden here.

Ms. WASSERMAN SCHULTZ. Right.

Mr. BARR. If the Government knows where Osama bin Laden is if he is talking on the phone, one would hope they would do something about it rather than listen in.

Mr. TURNER. But if we say they can't look at anything that has got U.S. person without a warrant, we are going to give him the easiest way to immunize his whole communication system.

Ms. WASSERMAN SCHULTZ. And a court review would resolve that. That is my point.

Mr. TURNER. In each case, you mean. Are we going to have the people—you know, what if——

Ms. WASSERMAN SCHULTZ. As the Chairman said, Professor Turner, a court review has never and would never stop the actual surveillance from occurring.

Mr. TURNER. Well, the old rule is if it is legal to intercept, say, a drug dealer, you know, who we have gotten a warrant for, we can listen to people who talk to him.

As soon as we find out they are unrelated to a drug deal, we erase it, but we can listen to it. And if they say, "I am calling to buy drugs," we can use it to prosecute them.

In the same way, it is perfectly legitimate to target bin Laden and probably to target just about any other foreign national we feel the need to do, and that means there is probably no reasonable expectation of privacy when you communicate.

But the reality is we don't have the time or the interest, you know, to read communications between little girls. That is to say—remember, NSA is overseen by 100 people in their office of inspector general.

Ms. WASSERMAN SCHULTZ. Professor Turner, I want to be respectful of my colleagues.

Mr. BARR. Is the professor saying——

Mr. TURNER [continuing]. There are protections.

Mr. BARR. If I might, is the professor suggesting that there is no reasonable expectation of privacy in any communication with a foreign person or somebody outside the country?

Mr. TURNER. The way we test that is to balance interests and ask whether society is willing to recognize an expectation of privacy——

Mr. BARR. No, that is not the test.

Mr. TURNER [continuing]. In each case.

Mr. BARR. Is that what you are saying, that you have no reasonable expectation of privacy if you simply call somebody or e-mail somebody overseas?

Mr. TURNER. If you are commissioning with someone who the Government has reason to believe is a foreign terrorist——

Mr. BARR. No, that isn't what I said.

Mr. TURNER [continuing]. I don't think anyone should have an expectation——

Mr. DAVIS. Mr. Chairman, could I ask the witnesses to yield to the Members?

Mr. TURNER. Sorry.

Ms. WASSERMAN SCHULTZ. I was enjoying it, Mr. Chairman, so it is perfectly okay with me.

Mr. TURNER. Former Member.

Mr. CONYERS. I am not sure if we can accommodate the gentlemen.

Ms. WASSERMAN SCHULTZ. I really appreciate my colleagues' indulgence.

And, Professor, my point is that this very discussion that we have been having for the last few minutes literally points out that the changes we made cry out for reform and that we cannot cast aside people's constitutional rights.

Mr. TURNER. But if there is no way to distinguish——

Ms. WASSERMAN SCHULTZ. I think my time has expired.

Mr. TURNER. If there is no way to distinguish, you are saying we shouldn't listen to the terrorists because we might pick up a communication involving a young American school girl. That is the issue.

Ms. WASSERMAN SCHULTZ. No. The issue is that we have a lot of innocent communication that we are capturing unreasonably and unconstitutionally and that the law should be reformed so that we don't do that, and people don't have to sit and wonder whether the Government is listening to them for no good reason.

And I appreciate it, and my time has expired.

Mr. CONYERS. Hank Johnson, Georgia?

Mr. JOHNSON. Thank you, Mr. Chairman.

And I would note for the record that my kids would, from time to time, place in an e-mail the fact that new Jay-Z is "blowing up," and so I guess that they would trigger a review of their e-mails.

But I am concerned about the interview that Director of National Intelligence Mike McConnell gave to the El Paso times, and you alluded to that interview, Congressman Barr, and you mentioned that Mr. McConnell stated that if we continue to debate this issue in Congress, then Americans are going to die.

And you were attacked in this hearing for alluding to that statement. And I have a copy of the transcript of the interview with Mr. McConnell, and I will just read that part for the record.

The question says, "So you are saying that the reporting and the debate in Congress means that some Americans are going to die?" The answer, "That is what I mean, because we have made it so public. We used to do these things very differently, but for whatever reason, you know, it is the democratic process, and sunshine is a good thing."

And so he definitely said that if Congress continues to discuss this then Americans are going to die.

And, Ms. Spaulding, I want to ask you, as a former CIA official and former executive director of the National Commission on Terrorism, can you tell us what your concerns would be about that statement that Mr. McConnell made in the context of the passage of this law that we are talking about today, the amendment to FISA?

Ms. SPAULDING. I think it is a most unfortunate comment on the part of Director McConnell. And we have discussed previously today the importance, not just to our civil liberties, but to our national security of having an open and robust and informed public discussion and debate.

The thing that I think is so tragic about comments like that of Director McConnell is that it does seem to reflect a fundamental lack of faith in the strength of our democratic system.

And I think it is important to remember, to always keep in mind, that this system of checks and balances was not created by a bunch of fuzzy-headed liberals.

This was a system that was created by hard-nosed pragmatists who had just fought a war and faced a time of great peril.

Mr. JOHNSON. These are the same——

Ms. SPAULDING. This was the way to keep the country strong.

Mr. JOHNSON [continuing]. Same founding fathers that have been cited repeatedly by Professor Turner.

And, Professor Turner, you would agree that our Constitutional sets up a separation of powers between the three branches of Government—presidential, legislative and judicial—correct? You would agree?

Mr. TURNER. I would agree, but some of those powers are not checked.

Mr. JOHNSON. Well, no, no, you would agree——

Mr. TURNER. That is to say, pardon power, for example, is unchecked.

Mr. JOHNSON. Well, listen to my question, now. And you answered—you agreed that we set up a separation of powers.

Mr. TURNER. With some checks.

Mr. JOHNSON. And then one of the things that makes that separation so important is because the three branches are co-equal, are they not?

Mr. TURNER. Well, they are co-equal, but they also——

Mr. JOHNSON. Thank you.

Mr. TURNER [continuing]. Have their own powers that are independent of the others.

Mr. JOHNSON. That is true. They are separate—separation of powers—co-equal. And the thing that gives substance to this co-equality is the concept of checks and balances.

Would you agree to that, Congressman Barr?

Mr. BARR. I would certainly agree with that.

Mr. JOHNSON. And, Congressman Barr, how can there be a check and balance on the executive branch if there is no judicial oversight or legislative input into an executive function?

Mr. BARR. It creates a nullity. There is none.

Mr. JOHNSON. What is your response to that, Professor Turner?

Mr. TURNER. It is fairly easy. And I document it briefly in my testimony. In the area of foreign affairs, the founding fathers, the people you are talking about——

Mr. JOHNSON. So you are saying that there is no check and balance——

Mr. TURNER. Well, to give you one example——

Mr. JOHNSON [continuing]. In foreign affairs?

Mr. TURNER [continuing]. Three days after Jefferson wrote his memo——

Mr. JOHNSON. Is that true or is that false? No check and balance——

Mr. TURNER. There are some checks.

Mr. JOHNSON [continuing]. In the President's conduct of foreign affairs?

Mr. TURNER. In Jefferson's memo, he said subject to the negatives given to the Senate. For example, the Senate can block an ambassadorial nominee. The Senate can block a treaty. The House, for example, in the——

Mr. JOHNSON. Well, we understand that, but we——

Mr. TURNER [continuing]. The House clearly can control that.

Mr. JOHNSON. I understand. And you have kind of graced us with a historical perspective as we have gone through this hearing, and I appreciate that. But my time is——

Mr. TURNER. Okay.

Mr. JOHNSON [continuing]. Running.

I did want to ask Mr. Barr, Congressman, if two Americans in the United States each sent—well, let me ask this question.

If there was an American soldier in Iraq that sent an e-mail to his girlfriend here in the United States, then under this new FISA

act that communication can be monitored because it concerns a person who is outside of the United States. Is that correct?

Mr. BARR. That is correct.

Mr. JOHNSON. And there is no need for a warrant?

Mr. BARR. That is correct, too.

Mr. JOHNSON. No judicial oversight is called for?

Mr. BARR. Correct.

Mr. JOHNSON. And that can be for a student who may be over in England somewhere and communicate back with a phone call to their parents. That phone call can be monitored.

Mr. BARR. That is correct.

Mr. JOHNSON. A doctor who is traveling overseas may call a patient here in the U.S., and that phone call can be monitored.

Mr. BARR. That is correct.

Mr. JOHNSON. That e-mail correspondence can be monitored.

Mr. BARR. Correct.

Mr. JOHNSON. And, Ms. Spaulding and Mr. Halperin, isn't it a fact that this new act would allow for the physical search of premises inside of the United States if it concerns a person located outside the United States?

Ms. SPAULDING. There are several criteria. For this, it would be under 105(b). And it has to concern a person outside the United States.

As I read it, it has to require the assistance of someone to gain access to a communication, which I can only assume the Government meant and was focused on electronic surveillance, but the language is unfortunate because it, as I have pointed out——

Mr. JOHNSON. Overly broad.

Ms. SPAULDING [continuing]. In my testimony, is much, much broader.

Mr. JOHNSON. Yes.

Ms. SPAULDING. But yes, assuming that it fit that fact pattern, the Government would be able to, because of the "notwithstanding any other law," use this authority to conduct a physical search.

Mr. JOHNSON. Thank you. I would——

Mr. HALPERIN. Can I just—Mr. Johnson, I don't think that that is correct, because the provision also says that it cannot be electronic surveillance. And I think the interception of the e-mail would be electronic surveillance.

But I think the important point is that this statute uses a whole set of new words. The "notwithstanding" language doesn't appear anyplace else. The "directed at" rather than "targeted at" doesn't appear anyplace else.

The "concerning a person overseas" doesn't appear anywhere else in the statute. And nobody has any idea what those words were intended to mean or what a court will interpret them to mean or what the Attorney General now thinks they mean.

And that is not a way to legislate when it involves the constitutional rights of Americans.

Mr. JOHNSON. Well, I agree, and I have confidence that under the oversight of this Chairman of this Committee we will consider legislation to amend this act and to correct these deficiencies.

And I want to applaud the Chairman for holding this hearing today. Thank you.

Mr. CONYERS. Thank you, Judge Johnson.

I am pleased now to recognize Betty Sutton of New York.

Ms. SUTTON. Ohio.

Mr. CONYERS. Ohio, I am sorry.

Ms. SUTTON. Love New York, but love my constituents in Ohio.

Mr. CONYERS. Excuse me.

Ms. SUTTON. That is okay. Mr. Chairman, thank you very, very much.

And thank you to the panelists for your testimony. It has been quite incredible to sit here and listen and take it all in.

I am taken by the testimony referencing the importance of the changes—words matter—words matter—the changes in the terms and the language that we find in this new act.

And I think that it is only heightened—the importance of those changes is heightened when we see some of the other things that we have heard discussed today here about the interview that Mr. McConnell has given.

And certainly, to characterize, I guess, carefully, suggestions that to have a discussion about this is in and of itself threatening to our security—I find that to be a very dangerous place for us in this country to be.

I would like to just begin—Mr. Turner, if you could just answer a question for me so that I understand where you are coming from.

Do you think that a warrantless interception of domestic-to-domestic mail by our Government on a belief that it concerns foreign intelligence does not violate the fourth amendment?

Mr. TURNER. The Supreme Court has left that open. The courts that have considered it—if the purpose is foreign intelligence—you know, the distinction the courts have drawn—the Supreme Court has said if it is a terrorist issue and the threat is not tied to a foreign power, it is—you know, it absolutely requires a warrant in every situation.

If it involves a foreign power, the Supreme Court punted. As I discussed—I actually discuss that case—we know how the judges favor, because one of the clerks has written about it, and it is fairly clear to me that had the *Keith* case been a foreign power case they would have gone the other way on it.

We know that Lewis Powell, who had been president of the American Bar Association, had set up and sat on this Committee that looked at this—had said that foreign intelligence wiretaps are part of an exception to the fourth amendment. You know, you can do it.

Now, the key to this is, again, if you wind up picking up—and it doesn't involve a terrorist threat or foreign intelligence, you need procedures to make sure that the privacy rights are protected. You know, we have been doing this for 30 years.

You need to make sure that any names of Americans and so forth are deleted, any communications about it—even if it has foreign intelligence value, you normally take the names of Americans out, unless they are terrorists or something like that.

But I think this is an issue—every court to decide it has said yes, the President has independent constitutional authority to engage in foreign intelligence wiretaps.

You know, again, we have got all sorts of supervision within the system for abuse. If the President were to say, "NSA, give me every conversation you can get from Ted Kennedy because he traveled to England and there is some foreign terrorists there," this would be in the Washington Post within an hour, probably, because there are 100 overseers just in the I.G. shop.

There are many people. And the people in the community don't want to violate the law. So this is not like it was in the 1960's. We have all kinds of internal checks.

Anybody in the intelligence community who believes something improper or illegal is being done can go directly to my old job. My job was to sit in the White House and try to make sure that all of the laws, including FISA, were being obeyed.

And although I thought it was unconstitutional, I said we are—you know, this is the law. We can challenge it but it will be obeyed. And we did obey it.

Go ahead, sorry.

Ms. SUTTON. Mr. Turner, I just—my question was, I think, much, much narrower than your response, and I am not really sure—maybe you were answering it, and I just didn't catch it. Okay. So your answer is you don't know. It may be that——

Mr. TURNER. Yes.

Ms. SUTTON [continuing]. A warrantless interception of domestic-to-domestic communication like that on the—because a belief that it concerns foreign intelligence may violate the fourth amendment, so something that provided for that may violate the fourth amendment.

Mr. TURNER. The only exception would involve foreign intelligence, and there we don't know. The Supreme Court has not ruled it. But if it did not involve foreign intelligence, it would require a warrant.

Ms. SUTTON. Okay. Thank you. Thank you, Mr. Turner.

I also just want to go back real quickly to Mr. McConnell's claim and some of the statements that he has made, specifically, the claim that 100 or less Americans have been targeted for surveillance.

First, at the same time that the Administration refuses to provide information on surveillance programs to Congress because it is classified, they seem to be selectively releasing classified information when they think it will help their position.

And that is a great concern to me. And for all the reasons that you all have articulated here today, I think it is concerning for the public and the trust of the public.

Second, that 100 or less number tells us absolutely nothing about the bigger and more disturbing question of how many Americans have had their phone calls listened to whether they were targeted or not.

Mr. Halperin, could you just tell me what you think about, you know, those concerns?

Mr. HALPERIN. Well, I think they are real, but I think they are very hard questions. And I think the only way to resolve what to do here is through serious good faith negotiations between the Committees of jurisdiction and the executive branch. And that is not what happened here.

I think on the one hand it is very easy. If it is a conversation between two Americans, you need a warrant based on probable cause.

If it is two foreigners talking to each other, you don't need a warrant, and even though the conversation runs through the United States, I think Congress should and would give the authority to do it.

The hard question, as you say, is you are targeting somebody abroad who you reasonably believe is not only abroad but is a terrorist—you are trying to collect terrorist information—and then they have conversations with Americans.

And the question is—and you have allowed the surveillance to go on without an individual warrant. Because if you get an individual warrant on bin Laden, for example, then it doesn't matter how many Americans he talks to.

You can listen to all of those conversations. You have to minimize the distribution of information about the Americans, unless it is necessary to understand the conversation. But that is all well understood.

The problem comes because the executive branch wants the authority to listen to these calls without a warrant or with a generalized warrant that says you can listen to all the calls, and then what happens if there are a lot of Americans?

And that is why I thought the direction that the Democrats were going in, and others in the Congress, which was to say the court has to be notified, the Congress has to be notified, of how many calls of Americans you are picking up on this particular surveillance—and at some point, if it is a significant number, then you have got to go back to the court and get a different kind of warrant.

That seems to me a reasonable balance that doesn't interfere with anything that the director said he needed to be able to do. And I think what we never got, as far as I can tell, was an explanation from the director as to why that was not okay.

What we got was it is not okay, and if you don't pass this, you are going to be responsible for the next terrorist attack.

What I think was the responsible answer was let me explain to you why that is too tightly written, or needs some more flexibility, or some greater time limits on it. But that has to be the way you solve the problem.

And the Administration, I think, has to be forced to engage, even if you say we are not extending this unless it does, to answering that question in a precise and serious way.

Ms. SUTTON. Thank you very much, Mr. Halperin.

Mr. CONYERS. Thank you very much.

The Chair recognizes the former assistant U.S. attorney from Alabama, Artur Davis.

Mr. DAVIS. Thank you, Mr. Chairman.

Mr. Turner, Professor Turner, let me begin with you in the limited time that I have today. One of the reasons why I think you have run into so much skepticism from this side of the aisle is there is an inherent contradiction that I want to point out to you.

On one hand, you, I think pretty accurately, describe the Administration's position on its authority. You describe an executive who essentially has untrammeled authority with respect to national se-

curity, and national security is essentially whatever the President decides it is.

You have said that several times. I think that it is a reasonably good summary of what the Administration has said in its pleadings.

So on the one hand, you have a very expansive view, and then when you talk about how this statute is going to be administered, all of a sudden you suggest that this Administration, which has such an expansive view of its power, is going to all of a sudden become very restrained.

You suggest, for example, that an Administration, this Administration, as it carries out this statute will take special care to make sure that it doesn't cross particular lines.

You suggest that the Administration will take special care to make sure that there is the strongest minimization process that we can contemplate. Those two don't work together.

And I say that, and my perspective is a little bit unique, Professor Turner, because I am the only person on this side of the aisle who is here today who actually voted for the bill that passed the House.

So as someone who agrees with more of what Dan Lungren said substantively than not, I am still troubled by a lot of what I have heard today. I am troubled by this expansive portrait of an executive and this theory that somehow that same executive will turn around and be restrained.

What I worried most about when I cast this vote was the following, that the Bush administration has no history whatsoever of executive restraint.

I cast the vote I did for one simple reason. After January 20th, 2009 there will be a different person in the White House. And I trust that the next person, frankly, will be much wiser in the use of those powers.

The next observation that I want to make is this one. Several times today you made the correct point that our country is facing an extreme threat. Several times today you made the correct point that these are unusual circumstances and they demand unusual measures.

But I want you to be cognizant of something else. What has made it near impossible to assemble bipartisan consensus around these issues is the following.

For the last 6 years, a lot of people on your side of these issues, frankly, on the President's side of these issues, have taken the position that if you don't agree that somehow you are not sufficiently zealous in your concern for American security.

On numerous occasions, the Administration has taken the position that, as the President famously said in 2004, you are either for us or you are for the terrorists.

The consequence of that kind of rhetoric is what you have now, a sharp partisan divide that very few of us cross, over issues that 6 years ago commanded a broad consensus.

The Patriot Act passed this House with an overwhelming vote. The reason every single subsequent vote on the boundaries of the fourth amendment—the reason they have all lost their bipartisan character is largely because of the rhetoric of the Administration,

and this rhetoric that suggests you have got to pick or choose, and if you don't follow this particular line you are not zealous enough about national security.

I don't buy that. As someone who voted with the Administration on this issue, I don't buy that. And it leads to my last observation.

If the Administration abuses this power, if the Administration takes this latest grant of authority and they treat it as cavalierly as they have treated the Patriot Act, or as cavalierly as they treated the authorization to go into Iraq, or as cavalierly as they have interpreted the authorization for force in Afghanistan, then I think I can safely represent to this entire panel and to the Administration, if it is listening to this, that it will be literally impossible to construct a bipartisan consensus around these issues.

We are down to 41 Democrats who crossed party lines in this last vote. If this authority is pushed in the way this Administration is eminently capable of pushing it, that number will shrink to nothing.

And that will be a cost not just on this particular term and this particular space in the political universe, but it will have a long-term cost on the relationship between the executive and the legislative.

And I will yield back, Mr. Chairman.

Mr. CONYERS. Thank you so much.

Mr. Barr, Attorney Spaulding, Dr. Turner, Mr. Halperin, your contribution really can't be appreciated sufficiently with words. And your endurance should also be taken note of as we conclude this hearing.

It has been an important way to begin the reexamination of FISA, and you have made the Committee and the Congress very proud of how we have put together our first record.

We thank you again and, of course, all the Members for their contributions.

The Committee stands adjourned.

[Whereupon, at 1:38 p.m., the Committee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON LEE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS, AND MEMBER, COMMITTEE ON THE JUDICIARY

SHEILA JACKSON LEE
18TH DISTRICT, TEXAS

WASHINGTON OFFICE:
2435 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-3816

DISTRICT OFFICE:
1919 SMITH STREET, SUITE 1180
THE GEORGE "MICKEY" LELAND FEDERAL BUILDING
HOUSTON, TX 77002
(713) 655-0050

ACRES HOME OFFICE:
6719 WEST MONTGOMERY, SUITE 204
HOUSTON, TX 77019
(713) 691-4882

HEIGHTS OFFICE:
420 WEST 19TH STREET
HOUSTON, TX 77008
(713) 861-4070

FIFTH WARD OFFICE:
3300 LYONS AVENUE, SUITE 301
HOUSTON, TX 77020

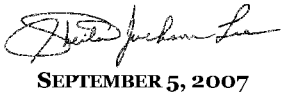
Congress of the United States
House of Representatives
Washington, DC 20515

COMMITTEES:
JUDICIARY
SUBCOMMITTEES:
COURTS, THE INTERNET, AND INTELLECTUAL PROPERTY
IMMIGRATION, CITIZENSHIP, REFUGEES, BORDER SECURITY, AND INTERNATIONAL LAW
CHAIR, TERRORISM AND HOMELAND SECURITY
HOMELAND SECURITY
SUBCOMMITTEES:
CHAIR
TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION
BORDER, MARITIME, AND GLOBAL COUNTERTERRORISM
FOREIGN AFFAIRS
SUBCOMMITTEES:
AFRICA AND GLOBAL HEALTH
MIDDLE EAST AND SOUTH ASIA
BOARD MEMBER:
DEMOCRATIC CAUCUS
THE
CONGRESSIONAL BLACK CAUCUS
CHAIR:
CONGRESSIONAL CHILDREN'S CAUCUS

CONGRESSWOMAN SHEILA JACKSON LEE, OF TEXAS

STATEMENT BEFORE THE JUDICIARY COMMITTEE

OVERSIGHT HEARING: "WARRANTLESS SURVEILLANCE AND THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: THE ROLE OF CHECKS AND BALANCES IN PROTECTING AMERICANS' PRIVACY RIGHTS"



SEPTEMBER 5, 2007

Thank you, Mr. Chairman for holding this hearing. Let me also welcome and thank our witnesses:

- Hon. Bob Barr, a former colleague and Representative of the 7th Congressional District of Georgia, and a former United States Attorney for the Northern District of Georgia;

- Ms. Suzanne Spaulding, Managing Director of the Harbour Group;
- Professor Robert F. Turner of the University of Virginia Law School;
- Mr. Morton Halperin, Director of U.S. Advocacy for the Open Society Institute.

Mr. Chairman, the purpose of this hearing is to consider the concerns of non-governmental organizations and actors regarding the contours of the "Protect America Act," P.L. 110-55, S. 1927, a short-term revision to the Foreign Intelligence Surveillance Act that was passed by the Congress in the waning hours before adjourning for the August district work period.

I strongly opposed that legislation. Had the Bush Administration and the Republican-dominated 109th Congress acted more responsibly in the two preceding years, Congress would not have been in the position of debating legislation that has such a profound impact on the national security and on American values and civil liberties in the crush of exigent circumstances. Mr. Chairman, the circumstances attending the development, debate, and deliberation of S. 1927 illustrates the truth of the saying goes that "haste makes waste."

S. 1927, the cleverly named but misleading, Protect America Act, Madam Speaker, purports to fill a gap in the nation's intelligence

gathering capabilities identified by Director of National Intelligence Mike McConnell, by amending the Foreign Intelligence Surveillance Act (FISA). But as I stated on the floor during general debate, in reality the bill eviscerates the Fourth Amendment to the Constitution and represents an unwarranted transfer of power from the courts to the Executive Branch and a Justice Department led by an Attorney General whose reputation for candor and integrity is, to put it charitably, subject to considerable doubt.

Mr. Chairman, the Foreign Intelligence Surveillance Act (FISA) has served the nation well for nearly 30 years, placing electronic surveillance inside the United States for foreign intelligence and counter-intelligence purposes on a sound legal footing and I am far from persuaded that it needs to be jettisoned or substantially amended. But given the claimed exigent circumstances by the Administration, let me briefly discuss some of the changes to FISA I would have been prepared to support on a temporary basis, not to exceed 120 days.

First, I was prepared to accept temporarily obviating the need to obtain a court order for certain foreign-to-foreign communications that pass through the United States. But I insist upon individual warrants, based on probable cause, when surveillance is directed at people in the

United States. The Attorney General must still be required to submit procedures for international surveillance to the Foreign Intelligence Surveillance Court for approval, but the FISA Court should not be allowed to issue a "basket warrant" without making individual determinations about foreign surveillance. During wartime, I accept the need for an initial 15-day emergency authority so that international surveillance can begin while the warrants are being considered by the Court. But there must be meaningful congressional oversight, requiring the Department of Justice Inspector General to conduct an audit every 60 days of U.S. person communications intercepted under these warrants, to be submitted to the Intelligence and Judiciary Committees. Finally, as I have stated, this authority must be of short duration and must expire by its terms in 120 days.

In all candor, Mr. Chairman, I must restate my firm conviction – shared by millions of Americans -- that when it comes to the track record of this President's warrantless surveillance programs, there is still nothing on the public record about the nature and effectiveness of those programs, or the trustworthiness of this Administration, to indicate that they require any legislative response, other than to reaffirm the exclusivity of FISA and insist that it be followed. This

could have been accomplished in the 109th Congress by passing H.R. 5371, the "Lawful Intelligence and Surveillance of Terrorists in an Emergency by NSA Act" (LISTEN Act)," which I have co-sponsored with the then Ranking Members of the Judiciary and Intelligence Committees, Mr. Conyers and Ms. Harman.

I think the record also should reflect that the Bush Administration has not complied with its legal obligation under the National Security Act of 1947 to keep the Intelligence Committees "fully and currently informed" of U.S. intelligence activities. Congress cannot continue to rely on incomplete information from the Bush Administration or revelations in the media. It must conduct a full and complete inquiry into electronic surveillance in the United States and related domestic activities of the NSA, both those that occur within FISA and those that occur outside FISA.

The inquiry must not be limited to the legal questions. It must include the operational details of each program of intelligence surveillance within the United States, including: (1) who the NSA is targeting; (2) how it identifies its targets; (3) the information the program collects and disseminates; and most important; (4) whether the program advances national security interests without unduly

compromising the privacy rights of the American people.

Given the unprecedented amount of information Americans now transmit electronically and the post-9/11 loosening of regulations governing information sharing, the risk of intercepting and disseminating the communications of ordinary Americans is vastly increased, requiring more precise — not looser — standards, closer oversight, new mechanisms for minimization, and limits on retention of inadvertently intercepted communications.

Mr. Chairman, we must never lose sight of the reason why we permit the Executive Branch to conduct foreign intelligence surveillance. Congress has authorized this activity to assist the Executive Branch in protecting the American people from foreign countries, organizations, agents, and actors who seek to harm our country and change our way of life. Americans rightly are proud of their way of life because, at bottom, it is made possible by adherence to a shared consensus regarding the values and beliefs that make our lives so rewarding, so fulfilling, and so special that ordinary men and women gladly don the uniform and willingly risk life and limb to preserve it.

Mr. Chairman, every day the brave and heroic men and women of

the Armed Forces stand on guard ready to defend their countrymen's liberty, including the right of privacy and their Fourth Amendment right to be secure in their persons, houses, papers, and effects. It would make a mockery of their devotion to preserving our way of life against foreign adversaries if this Congress voluntarily surrendered those rights by vesting in the Executive Branch more powers than are overbroad, unnecessary, and virtually unlimited. Mr. Chairman, the Executive Branch should have all the power necessary, but only the power necessary, to protect the American people from foreign adversaries.

It is worth recalling that this country was founded on the bedrock principle that governments exist to secure the inalienable rights of humankind – life, liberty, and the pursuit of happiness – and that government derives its just powers from the consent of the governed. Given their horrid experience living under the yoke of King George III, the Framers had a healthy concern for the abuse of power by those who wielded executive power. It is for that reason they subordinated the Executive Branch to the Legislative Branch; it is no mere coincidence that Congress is created and empowered in Article I of the Constitution and the Executive Branch is addressed in Article II. In the Declaration

of Independence Jefferson detailed the abuses, usurpations, and indignities suffered by the Colonies at the hand of an out of control executive. James Madison, the chief architect of the Constitution took great care to ensure that the Chief Executive would never be able to exercise the absolute powers of a monarch.

It is the American way, Mr. Chairman, to be wary of any attempt to aggrandize power in the hands of the Executive. My concern with the so-called Protect America Act is that it breaks faith with this long-standing and cherished American value. I believe that delegating to the Executive sweeping powers to eavesdrop on Americans without a warrant or constitutional probable cause will in the end sacrifice our liberty without increasing our security. I have reviewed the testimony of Mr. Barr, Ms. Spaulding, and Mr. Halperin and am aware that they share my concern. I am looking forward to discussing these matters in more detail with them. I also appreciate that the fourth witness, Professor Turner, holds a contrary view. I especially look forward to hearing his views in more detail.

Thank you, Mr. Chairman. I yield back the balance of my time.

PREPARED STATEMENT OF THE HONORABLE STEVE COHEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TENNESSEE, AND MEMBER, COMMITTEE ON THE JUDICIARY

STATEMENT OF REP. STEVE COHEN
HOUSE JUDICIARY COMMITTEE
SEPTEMBER 5, 2007

The Protect America Act (PAA), which I voted against, undermines the core purpose of the Foreign Intelligence Surveillance Act (FISA). Congress enacted FISA in the wake of revelations that the government had been engaged in the warrantless electronic surveillance of American citizens, including political opponents of the administration in power. FISA was supposed to act as a safeguard against such unfettered domestic surveillance by the government. The PAA substantially weakens that safeguard by redefining "electronic surveillance" to exclude an entire category of communications involving one non-U.S. based party. The danger is that, under the PAA, the government can engage in "reverse targeting," silently monitoring the American end of any communication regardless of whether the surveillance is nominally directed at a foreign target. Moreover, the PAA permits surveillance of almost any communication into and out of the U.S. and is not necessarily limited to the purpose of fighting terrorism. Additionally, there are constitutional concerns about the PAA's scope.

My hope is that today's witnesses can give us a good road map for crafting new legislation that will replace the PAA. While I recognize that we must update our laws from time to time to reflect changing technologies with respect to electronic communications and surveillance, we must do so in a way that does not undermine our fundamental beliefs about the limitations that should be imposed on the government's power to intrude in our lives.

II

Calendar No. 324

110TH CONGRESS
1ST SESSION

S. 1927

To amend the Foreign Intelligence Surveillance Act of 1978 to provide additional procedures for authorizing certain acquisitions of foreign intelligence information and for other purposes.

IN THE SENATE OF THE UNITED STATES

AUGUST 1, 2007

Mr. MCCONNELL (for himself and Mr. BOND) introduced the following bill; which was read the first time

AUGUST 2, 2007

Read the second time and placed on the calendar

A BILL

To amend the Foreign Intelligence Surveillance Act of 1978 to provide additional procedures for authorizing certain acquisitions of foreign intelligence information and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the "Protect America Act
5 of 2007".

1 **SEC. 2. ADDITIONAL PROCEDURE FOR AUTHORIZING CER-**
2 **TAIN ACQUISITIONS OF FOREIGN INTEL-**
3 **LIGENCE INFORMATION.**

4 The Foreign Intelligence Surveillance Act of 1978
5 (50 U.S.C. 1801 et seq.) is amended by inserting after
6 section 105 the following:

7 "CLARIFICATION OF ELECTRONIC SURVEILLANCE OF
8 PERSONS OUTSIDE THE UNITED STATES

9 "SEC. 105A. Nothing in the definition of electronic
10 surveillance under section 101(f) shall be construed to en-
11 compass surveillance directed at a person reasonably be-
12 lieved to be located outside of the United States.

13 "ADDITIONAL PROCEDURE FOR AUTHORIZING CERTAIN
14 ACQUISITIONS CONCERNING PERSONS LOCATED OUT-
15 SIDE THE UNITED STATES

16 "SEC. 105B. (a) Notwithstanding any other law, the
17 Director of National Intelligence and the Attorney Gen-
18 eral, may for periods of up to one year authorize the acqui-
19 sition of foreign intelligence information concerning per-
20 sons reasonably believed to be outside the United States
21 if the Director of National Intelligence and the Attorney
22 General determine, based on the information provided to
23 them, that—

24 "(1) there are reasonable procedures in place
25 for determining that the acquisition of foreign intel-
26 ligence information under this section concerns per-

1 sons reasonably believed to be located outside the
2 United States, and such procedures will be subject
3 to review of the Court pursuant to section 105C of
4 this Act;
5 "(2) the acquisition does not constitute elec-
6 tronic surveillance;
7 "(3) the acquisition involves obtaining the for-
8 eign intelligence information from or with the assist-
9 ance of a communications service provider, custo-
10 dian, or other person (including any officer, em-
11 ployee, agent, or other specified person of such serv-
12 ice provider, custodian, or other person) who has ac-
13 cess to communications, either as they are trans-
14 mitted or while they are stored, or equipment that
15 is being or may be used to transmit or store such
16 communications;
17 "(4) a significant purpose of the acquisition is
18 to obtain foreign intelligence information; and
19 "(5) the minimization procedures to be used
20 with respect to such acquisition activity meet the
21 definition of minimization procedures under section
22 101(h).
23 "This determination shall be in the form of a written
24 certification, under oath, supported as appropriate by affi-
25 davit of appropriate officials in the national security field

1 occupying positions appointed by the President, by and
2 with the consent of the Senate, or the Head of any Agency
3 of the Intelligence Community, unless immediate action by
4 the Government is required and time does not permit the
5 preparation of a certification. In such a case, the deter-
6 mination of the Director of National Intelligence and the
7 Attorney General shall be reduced to a certification as
8 soon as possible but in no event more than 72 hours after
9 the determination is made.

10 "(b) A certification under subsection (a) is not re-
11 quired to identify the specific facilities, places, premises,
12 or property at which the acquisition of foreign intelligence
13 information will be directed.

14 "(c) The Attorney General shall transmit as soon as
15 practicable under seal to the court established under sec-
16 tion 103(a) a copy of a certification made under sub-
17 section (a). Such certification shall be maintained under
18 security measures established by the Chief Justice of the
19 United States and the Attorney General, in consultation
20 with the Director of National Intelligence, and shall re-
21 main sealed unless the certification is necessary to deter-
22 mine the legality of the acquisition under section 105B.

23 "(d) An acquisition under this section may be con-
24 ducted only in accordance with the certification of the Di-
25 rector of National Intelligence and the Attorney General,

1 or their oral instructions if time does not permit the prep-
2 aration of a certification, and the minimization procedures
3 adopted by the Attorney General. The Director of Na-
4 tional Intelligence and the Attorney General shall assess
5 compliance with such procedures and shall report such as-
6 sessments to the Permanent Select Committee on Intel-
7 ligence of the House of Representatives and the Select
8 Committee on Intelligence of the Senate under section
9 108(a).

10 "(e) With respect to an authorization of an acquisi-
11 tion under section 105B, the Director of National Intel-
12 ligence and Attorney General may direct a person to—

13 "(1) immediately provide the Government with
14 all information, facilities, and assistance necessary
15 to accomplish the acquisition in such a manner as
16 will protect the secrecy of the acquisition and
17 produce a minimum of interference with the services
18 that such person is providing to the target; and

19 "(2) maintain under security procedures ap-
20 proved by the Attorney General and the Director of
21 National Intelligence any records concerning the ac-
22 quisition or the aid furnished that such person wish-
23 es to maintain.

1 "(f) The Government shall compensate, at the pre-
2 vailing rate, a person for providing information, facilities,
3 or assistance pursuant to subsection (e).
4 "(g) In the case of a failure to comply with a directive
5 issued pursuant to subsection (e), the Attorney General
6 may invoke the aid of the court established under section
7 103(a) to compel compliance with the directive. The court
8 shall issue an order requiring the person to comply with
9 the directive if it finds that the directive was issued in
10 accordance with subsection (e) and is otherwise lawful.
11 Failure to obey an order of the court may be punished
12 by the court as contempt of court. Any process under this
13 section may be served in any judicial district in which the
14 person may be found.
15 "(h)(1)(A) A person receiving a directive issued pur-
16 suant to subsection (e) may challenge the legality of that
17 directive by filing a petition with the pool established
18 under section 103(e)(1).
19 "(B) The presiding judge designated pursuant to sec-
20 tion 103(b) shall assign a petition filed under subpara-
21 graph (A) to one of the judges serving in the pool estab-
22 lished by section 103(e)(1). Not later than 48 hours after
23 the assignment of such petition, the assigned judge shall
24 conduct an initial review of the directive. If the assigned
25 judge determines that the petition is frivolous, the as-

1 signed judge shall immediately deny the petition and af-
2 firm the directive or any part of the directive that is the
3 subject of the petition. If the assigned judge determines
4 the petition is not frivolous, the assigned judge shall, with-
5 in 72 hours, consider the petition in accordance with the
6 procedures established under section 103(e)(2) and pro-
7 vide a written statement for the record of the reasons for
8 any determination under this subsection.

9 "(2) A judge considering a petition to modify or set
10 aside a directive may grant such petition only if the judge
11 finds that such directive does not meet the requirements
12 of this section or is otherwise unlawful. If the judge does
13 not modify or set aside the directive, the judge shall imme-
14 diately affirm such directive, and order the recipient to
15 comply with such directive.

16 "(3) Any directive not explicitly modified or set aside
17 under this subsection shall remain in full effect.

18 "(i) The Government or a person receiving a directive
19 reviewed pursuant to subsection (h) may file a petition
20 with the Court of Review established under section 103(b)
21 for review of the decision issued pursuant to subsection
22 (h) not later than 7 days after the issuance of such deci-
23 sion. Such court of review shall have jurisdiction to con-
24 sider such petitions and shall provide for the record a writ-
25 ten statement of the reasons for its decision. On petition

1 for a writ of certiorari by the Government or any person
2 receiving such directive, the record shall be transmitted
3 under seal to the Supreme Court, which shall have juris-
4 diction to review such decision.

5 "(j) Judicial proceedings under this section shall be
6 concluded as expeditiously as possible. The record of pro-
7 ceedings, including petitions filed, orders granted, and
8 statements of reasons for decision, shall be maintained
9 under security measures established by the Chief Justice
10 of the United States, in consultation with the Attorney
11 General and the Director of National Intelligence.

12 "(k) All petitions under this section shall be filed
13 under seal. In any proceedings under this section, the
14 court shall, upon request of the Government, review ex
15 parte and in camera any Government submission, or por-
16 tions of a submission, which may include classified infor-
17 mation.

18 "(l) Notwithstanding any other law, no cause of ac-
19 tion shall lie in any court against any person for providing
20 any information, facilities, or assistance in accordance
21 with a directive under this section.

22 "(m) A directive made or an order granted under this
23 section shall be retained for a period of not less than 10
24 years from the date on which such directive or such order
25 is made.".

1 **SEC. 3. SUBMISSION TO COURT REVIEW AND ASSESSMENT**
2 **OF PROCEDURES.**

3 The Foreign Intelligence Surveillance Act of 1978
4 (50 U.S.C. 1801 et seq.) is amended by inserting after
5 section 105B the following:

6 "SUBMISSION TO COURT REVIEW OF PROCEDURES

7 "SEC. 105C. (a) No later than 120 days after the
8 effective date of this Act, the Attorney General shall sub-
9 mit to the Court established under section 103(a), the pro-
10 cedures by which the Government determines that acquisi-
11 tions conducted pursuant to section 105B do not con-
12 stitute electronic surveillance. The procedures submitted
13 pursuant to this section shall be updated and submitted
14 to the Court on an annual basis.

15 "(b) No later than 180 days after the effective date
16 of this Act, the court established under section 103(a)
17 shall assess the Government's determination under section
18 105B(a)(1) that those procedures are reasonably designed
19 to ensure that acquisitions conducted pursuant to section
20 105B do not constitute electronic surveillance. The court's
21 review shall be limited to whether the Government's deter-
22 mination is clearly erroneous.

23 "(c) If the court concludes that the determination is
24 not clearly erroneous, it shall enter an order approving
25 the continued use of such procedures. If the court con-
26 cludes that the determination is clearly erroneous, it shall

1 issue an order directing the Government to submit new
2 procedures within 30 days or cease any acquisitions under
3 section 105B that are implicated by the court's order.
4 "(d) The Government may appeal any order issued
5 under subsection (c) to the court established under section
6 103(b). If such court determines that the order was prop-
7 erly entered, the court shall immediately provide for the
8 record a written statement of each reason for its decision,
9 and, on petition of the United States for a writ of certio-
10 rari, the record shall be transmitted under seal to the Su-
11 preme Court of the United States, which shall have juris-
12 diction to review such decision. Any acquisitions affected
13 by the order issued under subsection (c) of this section
14 may continue during the pendency of any appeal, the pe-
15 riod during which a petition for writ of certiorari may be
16 pending, and any review by the Supreme Court of the
17 United States.".
18 **SEC. 4. REPORTING TO CONGRESS.**
19 On a semi-annual basis the Attorney General shall
20 inform the Select Committee on Intelligence of the Senate,
21 the Permanent Select Committee on Intelligence of the
22 House of Representatives, the Committee on the Judiciary
23 of the Senate, and the Committee on the Judiciary of the
24 House of Representatives, concerning acquisitions under

1 this section during the previous 6-month period. Each re-
2 port made under this section shall include—
3 (1) a description of any incidents of non-compli-
4 ance with a directive issued by the Attorney General
5 and the Director of National Intelligence under sec-
6 tion 105B, to include—
7 (A) incidents of non-compliance by an ele-
8 ment of the Intelligence Community with guide-
9 lines or procedures established for determining
10 that the acquisition of foreign intelligence au-
11 thorized by the Attorney General and Director
12 of National Intelligence concerns persons rea-
13 sonably to be outside the United States; and
14 (B) incidents of noncompliance by a speci-
15 fied person to whom the Attorney General and
16 Director of National Intelligence issue a direc-
17 tive under this section; and
18 (2) the number of certifications and directives
19 issued during the reporting period.
20 **SEC. 5. TECHNICAL AMENDMENT AND CONFORMING**
21 **AMENDMENTS.**
22 (a) IN GENERAL.—Section 103(e) of the Foreign In-
23 telligence Surveillance Act of 1978 (50 U.S.C. 1803(e))
24 is amended—

1 (1) in paragraph (1), by striking "501(f)(1)"
2 and inserting "105B(h) or 501(f)(1)"; and
3 (2) in paragraph (2), by striking "501(f)(1)"
4 and inserting "105B(h) or 501(f)(1)".
5 (b) TABLE OF CONTENTS.—The table of contents in
6 the first section of the Foreign Intelligence Surveillance
7 Act of 1978 (50 U.S.C. 1801 et seq.) is amended by in-
8 serting after the item relating to section 105 the following:

"105A. Clarification of electronic surveillance of persons outside the United States.
"105B. Additional procedure for authorizing certain acquisitions concerning persons located outside the United States.
"105C. Submission to court review of procedures.".

9 **SEC. 6. EFFECTIVE DATE; TRANSITION PROCEDURES.**
10 (a) EFFECTIVE DATE.—Except as otherwise pro-
11 vided, the amendments made by this Act shall take effect
12 immediately after the date of the enactment of this Act.
13 (b) TRANSITION PROCEDURES.—Notwithstanding
14 any other provision of this Act, any order in effect on the
15 date of enactment of this Act issued pursuant to the For-
16 eign Intelligence Surveillance Act of 1978 (50 U.S.C.
17 1801 et seq.) shall remain in effect until the date of expi-
18 ration of such order, and, at the request of the applicant,
19 the court established under section 103 (a) of such Act
20 (50 U.S.C. 1803(a)) shall reauthorize such order as long
21 as the facts and circumstances continue to justify issuance
22 of such order under the provisions of the Foreign Intel-
23 ligence Surveillance Act of 1978, as in effect on the day

1 before the applicable effective date of this Act. The Gov-
2 ernment also may file new applications, and the court es-
3 tablished under section 103(a) of the Foreign Intelligence
4 Surveillance Act of 1978 (50 U.S.C. 1803(a)) shall enter
5 orders granting such applications pursuant to such Act,
6 as long as the application meets the requirements set forth
7 under the provisions of such Act as in effect on the day
8 before the effective date of this Act. At the request of the
9 applicant, the court established under section 103(a) of
10 the Foreign Intelligence Surveillance Act of 1978 (50
11 U.S.C. 1803(a)), shall extinguish any extant authorization
12 to conduct electronic surveillance or physical search en-
13 tered pursuant to such Act. Any surveillance conducted
14 pursuant to an order entered under this subsection shall
15 be subject to the provisions of the Foreign Intelligence
16 Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), as in
17 effect on the day before the effective date of this Act.

Calendar No. 324

110TH CONGRESS
1ST SESSION

S. 1927

A BILL

To amend the Foreign Intelligence Surveillance Act of 1978 to provide additional procedures for authorizing certain acquisitions of foreign intelligence information and for other purposes.

AUGUST 2, 2007

Read the second time and placed on the calendar

CRS REPORT FOR CONGRESS ENTITLED "P.O. 110–55, THE PROTECT AMERICAN ACT OF 2007: MODIFICATIONS TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT," AUGUST 23, 2007

Order Code RL34143

CRS Report for Congress

P.L. 110-55, the Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act

August 23, 2007

Elizabeth B. Bazan
Legislative Attorney
American Law Division

Prepared for Members and Committees of Congress

Congressional Research Service

P.L. 110-55, the Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act

Summary

On August 5, 2007, P.L. 110-55, the Protect America Act of 2007, was signed into law by President Bush, after having been passed by the Senate on August 3 and the House of Representatives on August 4. The measure, introduced by Senator McConnell as S. 1927 on August 1, makes a number of additions and modifications to the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended, 50 U.S.C. §§ 1801 *et seq.*, adds additional reporting requirements, and sunsets in 180 days. This report describes the provisions of P.L. 110-55, discusses its possible impact on and parallels to existing law, and summarizes the legislative activity with respect to S. 1927, H.R. 3356, and S. 2011.

The Foreign Intelligence Surveillance Act of 1978 was enacted in response both to the Committee to Study Government Operations with Respect to Intelligence Activities (Church Committee) revelations with regard to past abuses of electronic surveillance for national security purposes and to the somewhat uncertain state of the law on the subject. In creating a statutory framework for the use of electronic surveillance to obtain foreign intelligence information, the Congress sought to strike a balance between national security interests and civil liberties. Critical to an understanding of the FISA structure are its definitions of terms such as "electronic surveillance" and "foreign intelligence information." P.L. 110-55 limits the construction of the term "electronic surveillance" so that it does not cover surveillance directed at a person reasonably believed to be located outside the United States. It also creates a mechanism for acquisition, without a court order under a certification by the Director of National Intelligence (DNI) and the Attorney General, of foreign intelligence information concerning a person reasonably believed to be outside the United States. The Protect America Act provides for review by the Foreign Intelligence Surveillance Court (FISC) of the procedures by which the DNI and the Attorney General determine that such acquisitions do not constitute electronic surveillance. In addition, P.L. 110-55 authorizes the Attorney General and the DNI to direct a person with access to the communications involved to furnish aid to the government to facilitate such acquisitions, and provides a means by which the legality of such a directive may be reviewed by the FISC petition review pool. A decision by a judge of the FISC petition review pool may be appealed to the Foreign Intelligence Surveillance Court of Review, and review by the U.S. Supreme Court may be sought by petition for writ of certiorari.

The report will be updated should subsequent developments require it.

Contents

Introduction 1

Sec. 1. Short Title 2

Sec. 2. Additional Procedures for Authorizing Certain Acquisitions of Foreign Intelligence Information 2
New Section 105A of FISA, "Clarification of Electronic Surveillance of Persons Outside the United States" 2
To what extent would the new section 105A affect the scope of "electronic surveillance" as defined in section 101(f) of FISA? 3
New Section 105B of FISA, "Additional Procedure for Authorizing Certain Acquisitions Concerning Persons Located Outside the United States" 5
Effect on or parallels to existing law 11

Sec. 3. Submission to Court Review and Assessment of Procedures 13
New Section 105C of FISA. "Submission to Court Review of Procedures" 13
Comparison of this provision with court review 14
Other possible effects of new sections 105A, 105B, and 105C 14

Sec. 4. Reporting to Congress 18

Sec. 5. Technical Amendment and Conforming Amendments 18

Sec. 6. Effective Date; Transition Procedures 19
Effective Date 19
Transition Procedures 19

P.L. 110-55, the Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act

Introduction

In response to concerns raised by the Director of National Intelligence, Admiral Mike McConnell, that the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1801 *et seq.*, required modernization to meet the current intelligence needs of the nation, a number of bills were introduced in the Senate and the House of Representatives. Intense legislative activity with respect to proposed amendments to FISA in both bodies resulted in the enactment of the Protect America Act of 2007, P.L. 110-55 on August 5, 2007. The measure was introduced as S. 1927 by Senator McConnell, for himself and Senator Bond, on August 1, 2007. The bill was considered in the Senate on August 3, in conjunction with S. 2011, entitled The Protect America Act of 2007, introduced by Senator Levin, for himself and Senator Rockefeller. The Senate agreed by unanimous consent to an amendment to S. 1927 offered by Senator McConnell, for himself and Senator Bond, providing that sections 2, 3, 4, and 5 of the bill would sunset 180 days after its enactment.[1] As amended, S. 1927 passed the Senate the same day.[2] S. 2011 did not receive the requisite 60 votes, and was placed on the Senate calendar under general orders.[3]

That evening, the House considered H.R. 3356, the Improving Foreign Intelligence Surveillance to Defend the Nation and the Constitution Act of 2007, introduced by Representative Reyes for himself, Representative Conyers, Representative Schiff, and Representative Flake. After a motion to suspend the rules and pass H.R. 3356 fell short of the required two-thirds vote of the Members[4] on Friday night, the House took up S. 1927 the following day. At 10:19 p.m. Saturday night, August 4, the House passed S. 1927.[5] It was signed by the President on August 5, 2007.

This report discusses the provisions of P.L. 110-55 and their impact on or relationship with the prior provisions of FISA.

---

[1] S.Amdt. No. 2649 to S. 1927.

[2] Record Vote Number 309, 60-28 (August 3, 2007).

[3] Record Vote Number 310, 43-45 (August 3, 2007).

[4] The August 3, 2007, vote on the motion to suspend the rules and pass H.R. 3356 was 218 - 207 (Roll no. 821).

[5] The bill was passed by the Yeas and Nays: 227 - 183 (Roll no. 836).

Sec. 1. Short Title

Sec. 1 of S. 1927 states that the short title of the law is the Protect America Act of 2007.

Sec. 2. Additional Procedures for Authorizing Certain Acquisitions of Foreign Intelligence Information

Section 2 of the law contains its first substantive provisions. They are summarized in order below.

New Section 105A of FISA, "Clarification of Electronic Surveillance of Persons Outside the United States"

New Section 105A of FISA, as added by Section 2 of P.L. 110-55, states:

> Nothing in the definition of electronic surveillance under section 101(f) shall be construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States.

Section 101(f) of FISA, 50 U.S.C. § 1801(f), sets forth the definition of "electronic surveillance" under the statute. It provides:

> (f) "Electronic surveillance" means —
>
> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person[6] who is in the United

---

[6] As defined in section 101(i) of FISA, 50 U.S.C. § 1801(i),

> "United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

"Foreign power," as defined in section 101(a)(1), (2), or (3), 50 U.S.C. § 1801(a)(1), (2), or (3), means:

> (1) a foreign government or any component thereof, whether or not recognized by the United States;
> (2) a faction of a foreign nation or nations, not substantially composed of United States persons;
> (3) an entity that is openly acknowledged by a foreign government or

(continued...)

States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;
(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

To what extent would the new section 105A affect the scope of "electronic surveillance" as defined in section 101(f) of FISA? Absent the interpretation required by section 105A, two of the four definitions of "electronic surveillance" under section 101(f) of FISA, by their terms, appear to be broad enough to encompass electronic surveillance directed at a person abroad where the communications involved transcend U.S. borders.[7] Subsections 101(f)(2) and (f)(4) of FISA, on their face, appear to have the potential of reaching electronic surveillance of such communications targeted at a person outside the United States. In addition, it might be argued that the language of subsection 101(f)(4) might encompass the possibility of reaching some foreign to foreign communications in limited circumstances. This would suggest that, under FISA prior to the passage of section 105A of P.L. 110-55, some interceptions directed at a person abroad covered by the language of these subsections might have been regarded by the FISC as requiring court authorization.[8]

---

[6] (...continued)
governments to be directed and controlled by such foreign government or governments[.]

[7] Because new section 105A of FISA explicitly addresses electronic surveillance "directed at a person reasonably believed to be located outside the United States," it would not appear to affect subsection 101(f)(1), which deals with electronic surveillance of the contents of wire or radio communications acquired from an *intentionally targeted U.S. person within the United States* under specified circumstances. "Electronic surveillance" as defined in subsection 101(f)(3) of FISA involves the intentional acquisition of the contents of radio communications in specified circumstances *where the sender and all the intended recipients to the communication are in the United States*, so it would not seem to be impacted by new section 105A.

[8] *See*, Greg Miller, *Spy chief reveals details of operations*, L.A. Times, August 23, 2007, available at [http://www.latimes.com/news/nationworld/nation/la-na-intel23aug23,0,6229712.story?coll=la-home-center].

In pertinent part, "electronic surveillance," as defined by subsection 101(f)(2), covers acquisition of the contents of wire communications to or from a person in the United States where the acquisition occurs within the United States and no party to the communication has consented to the interception. Unlike subsection 101(f)(1), there is no express requirement that the person in the United States be known, that he or she be United States person, or that he or she be intentionally targeted by the electronic surveillance.

To the extent that an electronic surveillance under subsection 101(f)(2) intercepts communications between persons in the United States, it would not be impacted by section 105A of FISA, as added by P.L. 110-55, nor would section 105A affect electronic surveillance targeted at a person within the United States. However, to the extent that the language in subsection 101(f)(2) might encompass interception of communications between a person in the United States and one or more parties outside the United States, where the surveillance is targeted at a person outside the United States, section 105A would seem to restrict the previous reach of the definition of "electronic surveillance" in section 101(f)(2).

Subsection 101(f)(4) defines "electronic surveillance" under FISA to include "the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication,[9] under circumstances in which a person has a reasonable expectation of privacy and a warrant would be reqnired for law enforcement purposes." This subsection does not explicitly address the location of the parties to the communication or the location of the acquisition of the information involved. Thus, by its terms, it could conceivably be interpreted to cover some communications

---

[9] Section 101(l) of FISA, 50 U.S.C. § 1801(l), defines "wire communication" to mean:

> (l) "Wire communication" means any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications.

It does not have a separate definition of "radio communication." However, subsection 101(f)(4) of FISA appears to contemplate that communications can be transmitted using technologies other wire or radio. For example, in Title III of the Omnibus Crime Control and Safe Streets Act, as amended, 18 U.S.C. § 2510(12), "electronic communication" includes other technologies. Under § 2510(12), this term is defined to mean:

> any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include —
>
> (A) any wire or oral communication;
> (B) any communication made through a tone-only paging device;
> (c) any communication from a tracking device (as defined in [18 U.S.C. § 3117]); or
> (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds[.]

between parties in the United States, between a party in the United States and a party outside the United States, or between parties abroad, if the other requirements of the subsection were satisfied. The restrictions in this section are two-fold: the information must be acquired other than from a wire or radio communication; and the circumstances of the acquisition must be such that a person would have a reasonable expectation of privacy and a warrant would be required for law enforcement purposes. To the extent that "electronic surveillance" under subsection 101(f)(4) of FISA could have been or has been directed at a person or persons abroad, prior to the enactment of P.L. 110-55, new section 105A may also have the effect of limiting the scope of this subsection of the definition of "electronic surveillance" as it was previously interpreted.

New Section 105B of FISA, "Additional Procedure for Authorizing Certain Acquisitions Concerning Persons Located Outside the United States"

New section 105B(a) of FISA permits the Attorney General and the Director of National Intelligence, for periods of up to one year, to authorize acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States, if the Attorney General and the DNI determine, based on the information provided to them, that five criteria have been met. Under these criteria, the Attorney General and the DNI must certify that:

> (1) there are reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States,[10] and such procedures will be subject to review of the Court pursuant to section 105C of this Act;[11]

---

[10] The reporting requirements in Sec. 4 of the P.L. 110-55 require, in part, that the Attorney General report to the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, and the House and Senate Judiciary Committees regarding incidents of non-compliance by an element of the Intelligence Community with guidelines or procedures for determining that the acquisition of foreign intelligence authorized by the DNI and the Attorney General under section 105B "concerns persons reasonably [sic?] to be outside the United States."

[11] Section 105B(a)(1) states that the "procedures for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States" are to be submitted to the FISC for review pursuant to section 105C of FISA. There appears to be some ambiguity in the language of section 105B, particularly as compared with section 105C, as to what the procedures cover and what procedures are to be submitted to the FISC. The phrasing of section 105B(a)(1) on its face, seems to require submission to the FISC only of "reasonable procedures . . . for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States." This is the only mention in section 105B of procedures being submitted to the FISC. Thus, there is no mention in section 105B of creation of, or submission to the FISC of, procedures upon which the government bases its determination that the acquisition does not constitute electronic surveillance.

(continued...)

(2) the acquisition does not constitute electronic surveillance;
(3) the acquisition involves obtaining the foreign intelligence information from or with the assistance of a communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person of such service provider, custodian, or other person) who has access to communications, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications;
(4) a significant purpose of the acquisition is to obtain foreign intelligence information; and
(5) the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under section 101(h).[12]

---

[11] (...continued)

However, section 105C, by its terms, addresses only the submission by the Attorney General to the FISC of the procedures by which the government determines that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance, making no mention of the procedures referred to in section 105B(a)(1). In light of this apparent inconsistency, it is unclear what review, if any, the FISC is intended to give the procedures for determining that the acquisition of foreign intelligence information under section 105B "concerns persons reasonably believed to be located outside the United States." It is also not made clear in the language of either section by whom the procedures to be reviewed by the FISC under section 105C are to be promulgated.

On the other hand, section 105A provides that the definition of "electronic surveillance" shall not be "construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States." In light of this, it might be argued that the procedures by which the DNI and the Attorney General determine whether an acquisition of foreign intelligence information under section 105B concerns persons reasonably believed to be located outside the United States could be regarded as part of the FISC's analysis as to whether the procedures to determine that the acquisitions under 105B constitute electronic surveillance are clearly erroneous.

[12] Section 101(h) of FISA, 50 U.S.C. § 1801(h), defines "minimization procedures" for purposes of title I of FISA, dealing with electronic surveillance, to mean:

(h) "Minimization procedures", with respect to electronic surveillance, means —
(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;
(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and
(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802(a) of this title,

(continued...)

Except in circumstances where immediate government action is required and there is not sufficient time to prepare a certification, the determination by the Attorney General and the DNI that these criteria have been satisfied must be in the form of a certification, under oath, supported by affidavit of appropriate officials in the national security field appointed by the President, by and with the advice and consent of the Senate, or the Head of any agency of the Intelligence Community. Where imminent government action is required, the determination must be reduced to a certification as soon as possible within 72 hours after the determination is made.[13] The certification need not identify specific facilities, places, premises, or property at which the acquisition will be directed.[14]

A copy of a certification made under section 105B(a) must be transmitted under seal to the FISC as soon as practicable, there to be maintained under security measures established by the Chief Justice of the United States and the Attorney General, in consultation with the DNI. The copy of the certification must remain sealed unless needed to determine the legality of the acquisition involved.[15]

Where a certification has been prepared, an acquisition under section 105B of FISA must be conducted in accordance with that certification and minimization procedures adopted by the Attorney General. If a certification has not yet been prepared because of inadequate time, the acquisition must comply with the oral instructions of the DNI and the Attorney General and the applicable minimization procedures.[16] Section 105B(d) requires the DNI and the Attorney General must

---

[12] (...continued)

> procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

It may be noted that, while section 105B of FISA appears to be located in title I of FISA, which deals with electronic surveillance, the DNI and the Attorney General, under section 105B(a)(2) of FISA, are expressly required to certify that the acquisitions under section 105B do *not* constitute electronic surveillance. Similarly, the minimization procedures in section 101(h) of FISA, 50 U.S.C. § 1801(h), deal explicitly with minimization in the context of electronic surveillance, while, under subsection 105B(a)(5) of FISA, the DNI and the Attorney General must certify that "the minimization procedures to be used with respect to such acquisition[s] meet the definition of minimization procedures under section 101(h)." This seems likely to be intended to mean that the minimization procedures applicable to such acquisitions must set parallel standards to those applicable to electronic surveillance under the minimization procedures in section 101(h) of FISA, 50 U.S.C. § 1801(h).

[13] Protect America Act of 2007, P.L. 110-55, Sec. 105B(a), 121 Stat. 552 (August 5, 2007) (hereinafter P.L. 110-55).

[14] P.L. 110-55, Sec. 105B(b).

[15] P.L. 110-55, Sec. 105B(c).

[16] P.L. 110-55, Sec. 105B(d).

report their assessments of compliance with "such procedures"[17] to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence under section 108(a) of FISA, 50 U.S.C. § 1808(a).[18]

---

[17] In the context of the subsection 105B(d), the reference to "such procedures" might be seen to be susceptible of two possible interpretations. Perhaps the more likely and more limited interpretation would be that this may be a reference to the applicable minimization procedures referenced earlier in the subsection. Alternatively, a more expansive view might interpret this as a reference to the applicable minimization procedures plus the relevant certification, including the "reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States," or oral instructions regarding the acquisition at issue.

[18] Section 108 of FISA, 50 U.S.C. § 1808, provides:

> § 1808. Report of Attorney General to Congressional committees; limitation on authority or responsibility of information gathering activities of Congressional committees; report of Congressional committees to Congress
>
> (a) (1) On a semiannual basis the Attorney General shall fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, and the Committee on the Judiciary of the Senate, concerning all electronic surveillance under this subchapter [title I of FISA, 50 U.S.C. §§ 1801 *et seq.*]. Nothing in this subchapter [title I of FISA] shall be deemed to limit the authority and responsibility of the appropriate committees of each House of Congress to obtain such information as they may need to carry out their respective functions and duties.
>
> (2) Each report under the first sentence of paragraph (1) shall include a description of —
>
> (A) the total number of applications made for orders and extensions of orders approving electronic surveillance under this subchapter where the nature and location of each facility or place at which the electronic surveillance will be directed is unknown;
>
> (B) each criminal case in which information acquired under this chapter has been authorized for use at trial during the period covered by such report; and
>
> (C) the total number of emergency employments of electronic surveillance under section 1805(f) of this title and the total number of subsequent orders approving or denying such electronic surveillance.
>
> (b) On or before one year after October 25, 1978, and on the same day each year for four years thereafter, the Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence shall report respectively to the House of Representatives and the Senate, concerning the implementation of this chapter. Said reports shall include but not be limited to an analysis and recommendations concerning whether this chapter should be (1) amended, (2) repealed, or (3) permitted to continue in effect without amendment.

It may be noted that the reporting requirements under subsection 108(a) of FISA deal explicitly with electronic surveillance under FISA, and impose responsibility only upon the Attorney General. While section 105B has been added to title I of FISA, which deals with electronic surveillance, the DNI and the Attorney General, under subsection 105B(a)(2) are

(continued...)

In connection with an acquisition authorized under section 105B, the DNI and the Attorney General may issue a directive to a person to immediately provide the government with all information , facilities, and assistance needed to accomplish the acquisition in a manner which will protect the secrecy of the acquisition and minimize interference with the services provided by that person to the target of the acquisition.[19] The government must compensate the person furnishing such aid at the prevailing rate.[20] Any records that person wishes to keep relating to the acquisition or the aid provided must be maintained under security procedures approved by the DNI and the Attorney General.[21] P.L. 110-55 bars any cause of action in any court against any person for providing information, facilities or assistance in accordance with a directive under this section.[22] If a person receiving such a directive fails to comply therewith, the FISC, at the Attorney General's request, shall issue an order to compel such compliance if the court finds that the directive was issued in accordance with section 105B(e) and is otherwise lawful.[23]

A person receiving a directive under section 105B(e) may challenge its legality by filing a petition before the petition review pool of the FISC.[24] Under subsection

---

[18] (...continued)
required to certify, with respect to each acquisition under section 105B, that such acquisition "does not constitute electronic surveillance." The reporting requirement in section 105B(d) may be intended to direct the DNI and the Attorney General to include their assessments with respect to the procedures involved in the semiannual report of the Attorney General required by section 108(a), or it may be intended to require that the DNI and the Attorney General fully inform the House and Senate Intelligence Committees of their assessments on a semi-annual basis.

[19] P.L. 110-55, Sec. 105B(e)(1).

[20] P.L. 110-55, Sec. 105B(f).

[21] P.L. 110-55, Sec. 105B(e)(2).

[22] P.L. 110-55, Sec. 105B(l).

[23] P.L. 110-55, Sec. 105B(g). Service of process may be made upon such person in any judicial district in which he or she is found.

[24] Section 103(e)(1) of FISA, 50 U.S.C. § 1803(e)(1), established this pool. As amended by Sec. 5 of P.L. 110-55, section 103(e) provides:

> (e) (1) Three judges designated under subsection (a) of this section who reside within 20 miles of the District of Columbia, or, if all of such judges are unavailable, other judges of the court established under subsection (a) of this section as may be designated by the presiding judge of such court, shall comprise a petition review pool which shall have jurisdiction to review petitions filed pursuant to section *105B(h) or 501(f)(1)* of [FISA].
> (2) Not later than 60 days after March 9, 2006, the court established under subsection (a) of this section shall adopt and, consistent with the protection of national security, publish procedures for the review of petitions filed pursuant to section *105B(h) or 501(f)(1)* of [FISA] by the panel established under paragraph (1). Such procedures shall provide that review of a petition shall be conducted in camera and shall also provide for the designation of an acting presiding judge. [Emphasis added.]

(continued...)

105B(h)(1)(B) as written, the presiding judge of the Foreign Intelligence Surveillance Court of Review (Court of Review)[25] shall assign a petition filed with the petition review pool to one of the FISC judges in the pool. The assigned judge must conduct an initial review of the directive within 48 hours after the assignment. If he or she determines that the petition is frivolous, the petition is immediately denied and the directive or that portion of the directive that is the subject of the petition is affirmed. If the judge does not find the petition frivolous, he or she has 72 hours in which to consider the petition and provide a written statement for the record of the reasons for any determination made. A petition to modify or set aside a directive may only be granted if the judge finds that the directive does not meet the requirements of section 105B or is otherwise unlawful. Otherwise the judge must immediately affirm the directive and order its recipient to comply with it. A directive not explicitly modified or set aside remains in full effect.[26] Within seven days of the assigned judge's decision, the government or a recipient of the directive may petition the Foreign Intelligence Surveillance Court of Review for review of that decision. The Court of Review must provide a written statement on the record of the reasons for its decision. The government or any recipient of the directive may seek review of the decision of the Court of Review by petition for a writ of certiorari to the U.S. Supreme Court.[27]

---

[24] (...continued)
Subsection 103(a) requires the Chief Justice of the United States to publicly designate 11 U.S. district court judges from seven of the United States judicial circuits to become the FISC judges. The reference to section 501(f)(1) of FISA, 50 U.S.C. § 1861(f)(1), may be intended to be a reference to section 501(f), 50 U.S.C. § 1861(f). Section 501(f), as added to FISA by P.L. 109-177, § 106(f), was rewritten by P.L. 109-178, § 3. Current section 501(f)(1) of FISA contains two subsections, defining the terms "production order" and "nondisclosure order," respectively, for purposes of section 501.

[25] Section 105B(h)(1)(B) states that the "presiding judge designated pursuant to section 103(b) shall assign a petition filed under subparagraph (a) to one of the judge serving in the pool established by section 103(e)(1)." This may be intended to refer to the presiding judge of the FISC designated pursuant to section 103(a), rather than the presiding judge of the Foreign Intelligence Surveillance Court of Review designated pursuant to section 103(b). The petition review pool established by section 103(e)(1) is made up of FISC judges. *See* footnote 24, *supra*. Section 501(f)(2)(A)(ii) provides that, when a petition under that section is filed with the petition review pool of the FISC, "the presiding judge" shall immediately assign it to one of the judges in the pool. The rules, effective May 5, 2006, promulgated by the FISC under section 103(e)(2) of FISA are more explicit. Under title III, sections 8 and 9, of the "Procedures for review of Petitions filed pursuant to Section 501(f) of the Foreign Intelligence Surveillance Act of 1978, As Amended," the "Presiding Judge of the Foreign Intelligence Surveillance Court," where available, assigns petitions received under section 501(f) of FISA to one of the FISC judges in the petition review pool. If the Presiding Judge of the FISC is unavailable, the local FISC judge with the most seniority, other than the Presiding Judge, becomes Acting Presiding Judge, and assigns the petition to an FISC judge in the petition review pool. If no local judge is available, the most senior FISC judge who is reasonably available becomes the Acting Presiding Judge, and makes the assignment of the petition.

[26] P.L. 110-55, Sec. 105B(h).

[27] P.L. 110-55, Sec. 105B(i).

All judicial proceedings under this section are to be concluded as expeditiously as possible.[28]

All petitions under this section are filed under seal. Upon request of the government in any proceeding under this section, the court shall review ex parte and in camera any government submission or portion of a submission which may contain classified information.[29] The record of all proceedings, including petitions filed, orders granted, and statements of reasons for decision, must be maintained under security measures established by the Chief Justice of the United States in consultation with the Attorney General and the DNI.[30] A directive made or an order granted under this section must be retained for at least ten years.[31]

Effect on or parallels to existing law. Section 105B is a new section added to title I of FISA, 50 U.S.C. §§ 1801 *et seq*. It differs from the other provisions of title I of FISA in that it does not deal with electronic surveillance, but rather with acquisitions that do not constitute electronic surveillance. Because section 105B does not specify where such acquisitions may occur or from whom, it appears that such foreign intelligence information concerning persons reasonably believed to be outside the United States may be acquired, at least in part, from persons, including U.S. persons, who are located within the United States.[32]

Similar to electronic surveillance under section 102 of FISA, 50 U.S.C. § 1802, which may be authorized for up to one year by the President, through the Attorney General, without a court order if the Attorney General certifies in writing under oath that certain requirements are satisfied,[33] acquisitions under section 105B of FISA,

---

[28] P.L. 110-55, Sec. 105B(j).

[29] P.L. 110-55, Sec. 105B(k).

[30] P.L. 110-55, Sec. 105B(j).

[31] P.L. 110-55, Sec. 105B(m).

[32] It may be noted that the description of an acquisition under section 105B of FISA appears broad enough to encompass future collection of phone calling records for pattern analysis, but does not appear intended to address any past use of such investigative techniques. *Cf.*, Hepting v. AT&T Corp., 439 F. Supp. 2d. 974 (N.D. Cal. 2006); In re: National Security Agency Telecommunications Records Litigation, MDL No. 06-1791-VRW (March 13, 2007) (stipulation and order staying all cases except *Hepting* against AT&T Defendants); Hepting v. United States, Nos. 06-80109, 06-80110 (9th Cir. 2006) (order granting appeal).

[33] Section 102(a), 50 U.S.C. § 1802(a) provides:

> (a)(1) Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that —
>
> (A) the electronic surveillance is solely directed at —
>
> (i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801(a)(1), (2), or (3) of this title; or
>
> (ii) the acquisition of technical intelligence, other than the spoken

(continued...)

may be authorized by the DNI and the Attorney General without a court order if they certify in writing under oath that certain criteria are met. However, section 105B has no parallel to section 102(a)(1)(B)'s requirement that "there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party."

Similar to section 105B(d)'s reporting requirements, section 102(a)(2) requires electronic surveillance under that section to be carried out in accordance with the Attorney General's certification and applicable minimization requirements, and directs the Attorney General to assess compliance with "such procedures" and report his assessments to the House and Senate intelligence committees under the provisions of section 108(a) of FISA.

Section 102(a)(4), which permits the Attorney General to direct a specified communication common carrier to provide information, facilities, or technical assistance to the government needed to carry out the electronic surveillance involved and to compensate that communication common carrier at the prevailing rate for its aid, is structurally similar to section 105B(e) and (f). However, subsections 105B(e) and (g)-(i) permit the Attorney General and the DNI to direct "a person," rather than a "specified communication common carrier," to "immediately" furnish such aid; provide authority for the Attorney General to seek the aid of the FISC to compel compliance with such a directive; give the recipient of the directive a right to challenge the legality of the directive before the petition review pool of the same court; and permit both the government and the recipient of the directive to appeal that court's decision. The authority to challenge the legality of such a directive and to appeal the decision appears modeled, to some degree, after the process set forth in section 501(f) of FISA, 50 U.S.C. § 1861(f), dealing with challenges to the legality of production and nondisclosure orders.

Unlike electronic surveillance pursuant to a court order sought under section 104 of FISA, 50 U.S.C. § 1804, and authorized under section 105 of FISA, 50 U.S.C. § 1805, where the government provides the FISC with specific categories of substantive information about the electronic surveillance involved upon which the

---

[33] (...continued)

communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title;

(B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and

(C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 1801(h) of this title; and

if the Attorney General reports such minimization procedures and any changes thereto to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least thirty days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such minimization procedures and the reason for their becoming effective immediately.

court can base its determinations; the government submits certain procedures[34] for review to the FISC, but does not provide the court with substantive information about the acquisitions themselves.

Sec. 3. Submission to Court Review and Assessment of Procedures

Section 3 of the act creates a new section 105C of FISA, creating a review process for the procedures under which the government determines that acquisitions of foreign intelligence information from persons reasonably believed to be located outside the United States do not constitute electronic surveillance.

New Section 105C of FISA. "Submission to Court Review of Procedures"

Subsection 105C(a) requires the Attorney General, within 120 days of enactment of the act,[35] to submit to the FISC the procedures by which the government determines that acquisitions conducted pursuant to section 105B of the act do not constitute electronic surveillance.[36] The procedures are to be updated and submitted to the FISC annually. Within 180 days after enactment, the FISC must assess whether the government's determination under section 105B(1) of FISA that the

---

[34] Compare section 105B(a)(1) with section 105C.

[35] Under Sec. 6(a) of the act, except as otherwise provided, the amendments made by the act are to take effect immediately after the date of enactment of the act. Sec. 105C(a) states that it will take effect within 120 days of the effective date of the act. For purposes of Sec. 105C(a), that would be 120 days after enactment.

[36] Section 105B(1) on its face refers only to "reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States," and requires "such procedures [to be] subject to review of the [FISC] pursuant to section 105C of this Act." *See* footnote 11, *supra*, for further discussion of the seeming ambiguities in the statutory language of sections 105B and 105C with respect to the procedures to be reviewed by the FISC.

procedures are "reasonably designed to ensure that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance"[37] is clearly erroneous.[38]

If the FISC deems the government's determination not clearly erroneous, the court must enter an order approving the continued use of the procedures. On the other hand, if the government's determination is found to be clearly erroneous, new procedures must be submitted with 30 days or any acquisitions under section 105B implicated by the FISC order must cease.[39] Any order issued by the FISC under subsection 105C(c) may be appealed by the government to the Foreign Intelligence Surveillance Court of Review. If the Court of Review finds the FISC order was properly entered, the government may seek U.S. Supreme Court review through a petition for a writ of certiorari.[40] Any acquisitions affected by the FISC order at issue may continue throughout the review process.

Comparison of this provision with court review. The section 105C procedure review process is new and does not appear to have a parallel in the other provisions of FISA.

Other possible effects of new sections 105A, 105B, and 105C. The Terrorist Surveillance Program has been characterized as involving "intercepts of contents of communications where one . . . party to the communication is outside the United States" and the government has "a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda."[41] In a letter from the Attorney General to Senator Leahy and Senator Specter on January 17, 2007, the Attorney General indicated that, based upon classified orders issued by a judge of the Foreign Intelligence Surveillance Court (FISC), electronic

---

[37] There appears to be some ambiguity regarding the procedures referenced in section 105B(a) and section 105C of FISA. Section 105B permits the DNI and the Attorney General to authorize acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States if the DNI and the Attorney General determine, based upon information provided to them, "that — (a)(1) there are reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States, and such procedures will be subject to review of the Court pursuant to section 105C of this Act[.]" However, section 105C requires the Attorney General to submit to the FISC "the procedures by which the Government determines that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance." For further discussion, see 15, *supra*.

[38] Section 105C(b) of FISA, as added by P.L. 110-55, Sec. 3.

[39] Section 105C(c) of FISA, as added by P.L. 110-55, Sec. 3.

[40] Section 105C(d) of FISA, as added by P.L. 110-55, Sec. 3. If the Court of Review affirms the FISC order, the Court of Review must immediately prepare a written statement of each of the reasons for its decision. Should the government file a certiorari petition, that written record would be transmitted under seal to the U.S. Supreme Court.

[41] *See* Press Release, White House, Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (December 19, 2005).

surveillances previously carried out under the Terrorist Surveillance Program would thereafter be under the court's supervision. His letter stated, in part:

> I am writing to inform you that on January 10, 2007, a Judge of the Foreign Intelligence Surveillance Court issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization. As a result of these orders, any electronic surveillance that was occurring as part of the Terrorist Surveillance Program will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court.
> . . . .[42]

A question may arise as to whether new section 105A's interpretation of the definition of "electronic surveillance" under FISA, might impact the FISC's jurisdiction over some or all of the interceptions to which the Attorney General referred. Under section 103(a) of FISA, 50 U.S.C. § 1803(a):

> The Chief Justice of the United States shall publicly designate 11 district court judges from seven of the United States judicial circuits of whom no fewer than 3 shall reside within 20 miles of the District of Columbia who shall constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this chapter, except that no judge designated under this subsection shall hear the same application for electronic surveillance under this chapter which has been denied previously by another judge designated under this subsection. . . .

Section 102(b) of FISA, 50 U.S.C. § 1802(b), provides that:

> Applications for a court order under [title I of FISA, 50 U.S.C. §§ 1801 *et seq.*] are authorized if the President has, by written authorization, empowered the Attorney General to approve applications to the court having jurisdiction under section 1803 of this title, and a judge to whom an application is made may, notwithstanding any other law, grant an order, in conformity with section 1805 of this title, approving electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information, except that the court shall not have jurisdiction to grant any order approving electronic surveillance directed solely as described in paragraph (1)(A) of subsection (a) of this section unless such surveillance may involve the acquisition of communications of any United States person.

The answer to the jurisdictional question raised above would seem to depend on whether those interceptions were directed at the communications of a person reasonably believed to be located outside the United States. If so, then, by virtue of section 105A, such interceptions would not be construed to fall within the definition of "electronic surveillance" under FISA, and therefore a review of the underpinnings

---

[42] 153 *Cong. Rec.* S646-S647 (January 17, 2007) (Letter of Attorney General Alberto Gonzales to the Chairman and Ranking Member of the Senate Judiciary Committee ordered printed, without objection, in the *Record* during Senator Leahy's remarks on the FISA Program).

of such interceptions would not be within the FISC's jurisdiction in connection with an application to authorize electronic surveillance. If treated instead as acquisitions under new section 105B of FISA, then the FISC would seem to be limited to reviewing, under a clearly erroneous standard, the general procedures under which the Director of National Intelligence (DNI) and the Attorney General would make determinations that acquisitions did not constitute electronic surveillance;[43] and judges of the FISC petition review pool would have jurisdiction to consider petitions challenging the legality of directives to persons to furnish aid to the government to accomplish those acquisitions.[44]

Implicit in the previous discussion is the question what impact, if any, any possible narrowing of the interpretation of the definition of "electronic surveillance" under FISA might have upon the scope of "acquisitions" under new section 105B of FISA. In other words, if an interception of communications directed toward a person reasonably believed to be located outside the United States does not constitute "electronic surveillance" for purposes of FISA, regardless of where the other parties to the communication may be located or whether some or all of those other parties may be U.S. persons, could some or all such interceptions be deemed "acquisitions" under the provisions of section 105B?

For this to be the case, it would appear that the interception would have to be authorized by the DNI and the Attorney General under section 105B of FISA to acquire foreign intelligence information concerning persons reasonably believed to be outside the United States, and would have to satisfy the five criteria set forth in section 105B(a), including the use of minimization procedures.[45] If these requirements are met, then it appears that some communications to which U.S. persons located within the United States might be parties could be intercepted for periods of up to one year without a court order under section 105B.

This contrasts markedly with the detailed information to be provided by the government to the FISC in an application for a court order for electronic surveillance under section 104 of FISA, 50 U.S.C. § 1804,[46] and the level of FISC review

---

[43] Section 105C(a) of FISA, as added by P.L. 110-55, Sec. 3.

[44] Section 105B(h) of FISA, as added by P.L. 110-55, Sec. 2.

[45] Section 105B(a)(5) of FISA, as added by Sec. 2 of P.L. 110-55. For further discussion of minimization procedures in section 105B(a)(5), see footnote 12, *supra*, and accompanying text. Under section 105(f) of FISA, 50 U.S.C. § 1805(f), in approving an application for electronic surveillance under FISA, an FISC judge must find, in part, that the proposed minimization procedures applicable to that surveillance meet the definition of minimization procedures under section 101(h) of FISA, 50 U.S.C. § 1801(h). In authorizing an acquisition under section 105B, the DNI and the Attorney General must certify in writing under oath, in part, that "the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under section 101(h)."

[46] Section 104 of FISA, 50 U.S.C. § 1804, which deals with application for FISC court orders authorizing electronic surveillance, requires eleven categories of detailed information to be submitted by a federal office in writing under oath or affirmation to an FISC judge. Each application must be approved by the Attorney General based upon his finding that the

(continued...)

provided for such applications. To the extent that new section 105A circumscribes the previous interpretation of "electronic surveillance" as defined under section 101(f) of FISA, 50 U.S.C. § 1801(f), it could be argued that this might significantly diminish the degree of judicial review to which such interceptions might have heretofore been entitled. On the other hand, if the interpretation of the definition of "electronic surveillance" contemplated in new section 105A of FISA is consistent with prior practice, then this concern with respect to section 105A's impact would appear to be eliminated.

A somewhat closer parallel might be drawn between the statutory structure for acquisitions contemplated in section 105B and that for electronic surveillance under section 102 of FISA, 50 U.S.C. § 1802. The latter section permits the President, through the Attorney General, to authorize electronic surveillance for up to one year without a court order, if the Attorney General certifies in writing under oath that the electronic surveillance is solely directed at the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801(a)(1), (2), or (3) of this title;[47] or the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of such a foreign power. In addition, the Attorney General must certify that there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and that the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 1801(h) of this title; and he must comply with reporting requirements regarding those minimization procedures.

Subsection 102(b) of FISA denies the FISC jurisdiction to grant any order approving electronic surveillance directed solely at the acquisition of communications used exclusively between or among such foreign powers or the acquisition of such technical intelligence from property or premises under the exclusive and open control of such foreign powers, *unless such surveillance may involve the acquisition of communications of any United States person.* Section 105B provides the FISC no similar jurisdiction if an acquisition involves the communications of a United States person. Again, if the interpretation of the definition of "electronic surveillance" contemplated in new section 105A of FISA is consistent with prior practice, then this concern regarding section 105A's effect would appear to be eliminated.

To the extent that any intentional interceptions of communications which were previously deemed to be covered by the definition of "electronic surveillance" under FISA are now excluded from that definition, another question which may arise is whether any of those interceptions may now be found to fall within the general

---

[46] (...continued)
application satisfies the criteria and requirements set forth in title I of FISA. Section 105 of FISA, 50 U.S.C. § 1805, sets out the findings that a FISC judge must make in approving such an application.

[47] *See* footnote 6, *supra*, for the definition of "foreign power" under section 101(a)(1), (2), or (3) of FISA.

prohibition against intentional interception of wire, oral, or electronic communications under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, 18 U.S.C. § 2511. Under 18 U.S.C. § 2511(2)(f), "electronic surveillance," as defined in section 101 of the Foreign Intelligence Surveillance Act, is an exception to this general prohibition.[48] If such interceptions were deemed to violate 18 U.S.C. § 2511, then the intentional use or disclosure of the contents of such communications, knowing that the information was obtained through the interception of a wire, oral, or electronic communication in violation of 18 U.S.C. § 2511 would also be prohibited under that section.

Sec. 4. Reporting to Congress

Section 4 of P.L. 110-55 requires the Attorney General to inform the Senate Select Committee on Intelligence, the House Permanent Select Committee on Intelligence, the Senate Judiciary Committee and the House Judiciary Committee semi-annually concerning acquisitions "under this section"[49] during the previous six-month period. Each report is to include descriptions of any incidents of non-compliance with a directive issued by the DNI and the Attorney General under section 105B, including noncompliance by an element of the Intelligence Community with guidelines or procedures for determining that "the acquisition of foreign intelligence authorized by the Attorney General and the [DNI] concerns persons reasonably to be outside the United States,"[50] and incidents of noncompliance by a specified person to whom a directive is issued under section 105B. The report is also required to include the number of certifications and directives issued during the reporting period.

Sec. 5. Technical Amendment and Conforming Amendments

Section 5(a)(1) and (a)(2) make technical amendments to section 103(e)(1) and (2) of FISA, 50 U.S.C. § 1803(e)(1) and (2), to reflect the jurisdiction of the FISC petition review pool over petitions under section 105B(h) of FISA, dealing with challenges to the legality of directives issued under section 105B(e) of FISA to a

---

[48] If there are any types of intentional interceptions of communications previously covered by FISA's definition of electronic surveillance, which may now be prohibited under 18 U.S.C. § 2511, this, in turn, might give rise to the question whether, if the President were to carry out such interceptions under an assertion of his constitutional authority under Article II, the application of Title III's prohibition to those interceptions would be found by a court to be unconstitutional, or whether the application of this prohibition to such interceptions would withstand constitutional scrutiny. *Cf.*, In re Sealed Case, 310 F. 3d 717, 742, 746 (U.S. Foreign Intell. Surveillance Ct. Rev. 2002).

[49] This appears to be a reference to section 105Bof FISA, as added by P.L.110-55, Sec. 2.

[50] This may be intended to read "the acquisition of foreign intelligence *information* authorized by the Attorney General and Director of National Intelligence concerns persons reasonably *believed* to be outside the United States." (Emphasis added.)

person by the Attorney General and the DNI, and over petitions under section 501(f)[51] of FISA, 50 U.S.C. § 1861, dealing with challenges to production orders or nondisclosure orders issued by the FISC under section 501(c) of FISA, 50 U.S.C. § 1861(c).

Section 5(b) makes conforming amendments to the table of contents of the first "section"[52] of FISA, 50 U.S.C. § 1801 *et seq.*, to reflect the additions of new sections 105A, 105B, and 105C of FISA.

Sec. 6. Effective Date; Transition Procedures

Effective Date

Under Section 6(a) of P.L. 110-55, the amendments to FISA made in the act are to take effect immediately after its enactment except as otherwise provided.

Transition Procedures

Section 6(b) of P.L. 110-55 provides that any order issued under FISA in effect on the date of enactment of P.L. 110-55 (August 5, 2007) shall remain in effect until the date of expiration of the order, and, at the request of the applicant for the order, the FISC shall reauthorize the order as long as the facts and circumstances continue to justify its issuance under FISA as in effect the day before the applicable effective date of P.L.110-55. This appears to refer to orders and applications for orders under FISA authorizing electronic surveillance,[53] physical searches,[54] pen registers or trap

---

[51] Sec. 5(a)(1) and (2) of the act refer here to section "501(f)(1)," rather than to section "501(f)," of FISA. The reference to section 501(f)(1) of FISA, 50 U.S.C. § 1861(f)(1), may be intended to be a reference to section 501(f), 50 U.S.C. § 1861(f). Section 501(f), as added to FISA by P.L. 109-177, § 106(f), was rewritten by P.L. 109-178, § 3. Current section 501(f)(1) of FISA contains two subsections, defining the terms "production order" and "nondisclosure order," respectively, for purposes of section 501. For further discussion, see footnote 24, *supra*.

[52] This appears to be intended to refer to the title I of FISA, dealing with electronic surveillance.

[53] Applications for electronic surveillance are covered by section 104 of FISA, 50 U.S.C. § 1804, while orders authorizing such surveillance are addressed in section 105 of FISA, 50 U.S.C. § 1805. These sections were not amended by P.L.110-55.

[54] Applications for physical searches are addressed in sections 302(b) and 303 of FISA, 50 U.S.C. §§ 1822(b) and 1823, while orders authorizing such physical searches are addressed in section 304 of FISA, 50 U.S.C. § 1824. These sections were not amended by P.L.110-55.

and trace devices,[55] or production of tangible things and related nondisclosure orders.[56]

Section 6(b) provides further that the government may also file new applications and the FISC shall enter orders granting such applications pursuant to FISA, as long as the application meets the requirements set forth in FISA as in effect on the day before the applicable effective date of P.L. 110-55. This seems to indicate that pre-existing authorities under FISA remain available in the wake of P.L. 110-55's enactment. At the applicant's request, the FISC shall extinguish any extant authorizations to conduct electronic surveillance or physical searches pursuant to FISA. Any surveillance conducted pursuant to an order entered under subsection 6(b) of P.L. 110-55 is to be subject to the provisions of FISA as in effect before the effective date of P.L. 110-55.

Under Section 6(c) of P.L. 110-55, sections 2, 3, 4, and 5 of that act sunset 180 days after the date of enactment of the act, except as provided in section 6(d). Under section 6(d), any authorizations for acquisition of foreign intelligence information or directives issued pursuant to those authorizations issued under section 105B shall remain in effect until their expiration. Section 6(d) also provides that such acquisitions shall be governed by the applicable amendments made to FISA by P.L. 110-55, and shall not be deemed to constitute electronic surveillance as that term is defined in section 101(f) of FISA.[57]

---

[55] Applications for installation and use of pen registers and trap and trace devices are addressed in subsections 402(a), (b), and (c) of FISA, 50 U.S.C. § 1842(a), (b), and (c); while orders authorizing installation and use of such pen registers and trap and trace devices are covered by subsection 402(d), 50 U.S.C. § 1842(d). No amendments to these subsections were made in P.L. 110-55.

[56] Applications for orders "requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution" are addressed in subsections 501(a) and (b) of FISA, 50 U.S.C. § 1861(a) and (b). Production orders are covered in subsection 501(c) of FISA, 50 U.S.C. § 1861(c), while related nondisclosure orders are addressed in subsection 501(d) of FISA, 50 U.S.C. § 1861(d). These subsections were not amended by P.L. 110-55.

[57] The provisions in section 6(c) and (d) were added by Senate amendment 2649 to S. 1927, proposed by Senator McConnell, for himself and Senator Bond. It was agreed to by unanimous consent on August 3, 2007. As amended, the bill passed the Senate by Yea-Nay vote, 60-28 (Record Vote Number 309), 153 *Cong. Rec.* S10861-S10872 (August 3, 2007).

LETTER FROM DENISE A. CARDMAN, ACTING DIRECTOR, AMERICAN BAR ASSOCIATION (ABA), DATED SEPTEMBER 14, 2007, TO CHAIRMAN JOHN CONYERS, JR., AND RANKING MEMBER LAMAR S. SMITH

GOVERNMENTAL AFFAIRS OFFICE

DIRECTOR
Robert D. Evans
(202) 662-1765
rdevans@staff.abanet.org

DEPUTY DIRECTOR
Denise A. Cardman
(202) 662-1761
cardmanda@staff.abanet.org

SENIOR LEGISLATIVE COUNSEL
C. Lawson Fridley
(202) 662-1763
fridleyc@staff.abanet.org

Gillian B. Gaskin
(202) 662-1766
gaskinb@staff.abanet.org

LEGISLATIVE COUNSEL
Kristi Galinsky
(202) 662-1762
galinskyk@staff.abanet.org

Kenneth J. Gradillas
(202) 662-1763
gradillask@staff.abanet.org

Steve M. Lawrence
(202) 662-1767
lawrencesteve@staff.abanet.org

Elisa Avi Bernoff
(202) 662-1767
bernoffe@staff.abanet.org

F. Bruce Nicholson
(202) 662-1769
nicholsonb@staff.abanet.org

DIRECTOR, GRASSROOTS OPERATIONS/LEGISLATIVE COUNSEL
Julie M. Strandlie
(202) 662-1764
strandlij@staff.abanet.org

INTELLECTUAL PROPERTY LAW CONSULTANT
Hayden Gregory
(202) 662-1772
gregoryh@staff.abanet.org

STAFF LEGISLATIVE COUNSEL
Rita C. Aguilar
(202) 662-1760
aguilarr@staff.abanet.org

EXECUTIVE ASSISTANT
Julie Paul Inman
(202) 662-1776
paulinenjx@staff.abanet.org

STAFF DIRECTOR FOR INFORMATION SERVICES
Sharon Greene
(202) 662-1614
greenes@staff.abanet.org

EDITOR WASHINGTON LETTER
Brenda L. McMillan
(202) 662-1577

AMERICAN BAR ASSOCIATION

Governmental Affairs Office
740 Fifteenth Street, NW
Washington, DC 20005-1022
(202) 662-1760
FAX: (202) 662-1762

September 14, 2007

The Honorable John Conyers
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Lamar Smith
Ranking Republican Member
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Conyers and Rep. Smith:

Thank you for holding a hearing considering the impact of the recently-passed amendments to the Foreign Intelligence Surveillance Act ("FISA") included in the Protect America Act ("PAA"). The ABA welcomes your leadership in exploring the legal, operational and constitutional consequences of this significant statutory change.

One of the witnesses at the September 5, 2007 hearing, Dr. Robert F. Turner, repeatedly referenced the work of the American Bar Association in the area of electronic surveillance as part of his written and oral testimony. During the late eighties and early nineties, Dr. Turner dedicated his time as a volunteer leader in the ABA and the organization greatly values his contributions, particnlarly to our Committee on Law and National Security. I write today to clarify the position of the ABA on these matters to ensure that the hearing record reflects a full picture of the ABA's current policies with regard to surveillance for foreign intelligence purposes.

In his testimony, Dr. Turner cited the First Edition of the ABA Standards for Criminal Justice on Electronic Surveillance, which was originally adopted in 1971 prior to the adoption of FISA. Specifically, Dr. Turner referenced the report's endorsement of warrantless surveillance "in cases involving threats from a 'foreign power' or 'to protect military or other national security information against foreign intelligence activities.'"[1]

In 2001, the ABA issued the Third Edition of the Standards, which "abandons the minimal attempt made in the First and Second Edition of the Standards to regulate

[1] Testimony of Professor Robert F. Turner, U.S. House of Representatives, Committee on the Judiciary Hearing on Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights at http://judiciary.house.gov/media/pdfs/Turner070905.pdf.

electronic surveillance relating to foreign intelligence activities."[2] The Introduction to the Standards notes that the committee had received "comments expressing grave concerns about retaining this Standard"[3] and that the standard at issue was "beyond the scope" of the group's expertise.[4] Furthermore, it stated that the question of "whether the ABA should make more specific recommendations about how the President and Congress should set standards for and supervise foreign intelligence surveillance is more properly the subject of a separate inquiry."[5]

Last year, the ABA established an entity to consider the legal and constitutional issues relating to electronic surveillance conducted for foreign intelligence purposes. In February 2006, the ABA House of Delegates adopted as policy the unanimous recommendations of the Task Force on Domestic Surveillance in the Fight Against Terrorism. The Task Force was a bipartisan panel of distinguished lawyers that included a former Director of the Federal Bureau of Investigation, a former General Counsel of the National Security Agency and the Central Intelligence Agency, the National Institute of Military Justice General Counsel, and others with deep knowledge of national security law. For your ready reference, I have attached a copy of our policy and explanatory report, in the hope that it may be beneficial to you as you seek to legislate on these important policy matters.

Specifically, our policy calls upon the President to abide by the limitations that the Constitution imposes on a president under our system of checks and balances. As such, this policy states the Association's opposition to any future electronic surveillance inside this country by any U.S. government agency for foreign intelligence purposes that does not comply with FISA. The policy also urges the President to seek appropriate amendments or new legislation if he believes that FISA is inadequate to safeguard national security. Further, it urges Congress to conduct a comprehensive review of our intelligence operations and limitations before taking any further action to permanently rewrite FISA to ensure that all Members of Congress appreciate why any proposed changes are necessary, justified and consistent with the system of checks and balances required by the U.S. Constitution.

The ABA applauds the Judiciary Committee for its oversight work on the impact of these new legal standards for intelligence gathering.

Sincerely,

Denise A. Cardman
Acting Director

cc: Dr. Robert F. Turner

---

[2] AMERICAN BAR ASSOCIATION STANDARDS FOR CRIMINAL JUSTICE, ELECTRONIC SURVEILLANCE, THIRD EDITION, SECTION A: ELECTRONIC SURVEILLANCE OF PRIVATE COMMUNICATIONS, *Introduction* at 5.
[3] *Id.*
[4] *Id.* at 6.
[5] *Id.*

REPORT OF THE TASK FORCE ON DOMESTIC SURVEILLANCE IN THE FIGHT AGAINST TERRORISM, THE AMERICAN BAR ASSOCIATION (ABA), FEBRUARY 13, 2006

AMERICAN BAR ASSOCIATION

ADOPTED BY THE HOUSE OF DELEGATES
February 13, 2006

RESOLVED, that the American Bar Association calls upon the President to abide by the limitations which the Constitution imposes on a president under our system of checks and balances and respect the essential roles of the Congress and the judicial branch in ensuring that our national security is protected in a manner consistent with constitutional guarantees;

FURTHER RESOLVED, that the American Bar Association opposes any future electronic surveillance inside the United States by any U.S. government agency for foreign intelligence purposes that does not comply with the provisions of the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801 et seq. (FISA), and urges the President, if he believes that FISA is inadequate to safeguard national security, to seek appropriate amendments or new legislation rather than acting without explicit statutory authorization;

FURTHER RESOLVED, that the American Bar Association urges the Congress to affirm that the Authorization for Use of Military Force of September 18, 2001, Pub.L. No. 107-40, 115 Stat. 224 § 2(a) (2001) (AUMF), did not provide a statutory exception to the FISA requirements, and that any such exception can be authorized only through affirmative and explicit congressional action;

FURTHER RESOLVED, that the American Bar Association urges the Congress to conduct a thorough, comprehensive investigation to determine: (a) the nature and extent of electronic surveillance of U.S. persons conducted by any U.S. government agency for foreign intelligence purposes that does not comply with FISA; (b) what basis or bases were advanced (at the time it was initiated and subsequently) for the legality of such surveillance; (c) whether the Congress was properly informed of and consulted as to the surveillance; (d) the nature of the information obtained as a result of the surveillance and whether it was retained or shared with other agencies; and (e) whether this information was used in legal proceedings against any U.S. citizen.

FURTHER RESOLVED, that the American Bar Association urges the Congress to ensure that such proceedings are open to the public and conducted in a fashion that will provide a clear and credible account to the people of the United States, except to the extent the Congress determines that any portions of such proceedings must be closed to prevent the disclosure of classified or other protected information; and

FURTHER RESOLVED, that the American Bar Association urges the Congress to thoroughly review and make recommendations concerning the intelligence oversight process, and urges the President to ensure that the House and Senate are fully and currently informed of all intelligence operations as required by the National Security Act of 1947.

REPORT

"Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent. . . ."

***Olmstead v. United States*, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting).**

A. Introduction

On December 16, 2005, the New York Times reported that the President had "secretly authorized the National Security Agency (NSA) to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without the court-approved warrants ordinarily required for domestic spying, according to government officials."[1]

The New York Times revelation has created a major national controversy. The NSA program has drawn severe critics and staunch defenders; dozens of newspaper editorials and op-ed pieces have published, it has been a "hot topic" on hundreds of blogs, and both Democrat and Republican members of Congress have called for hearings.[2]

A number of terrorism defendants have filed legal challenges to their previous pleas of guilty or convictions,[3] and a lawsuit has been filed in Detroit against the NSA by the American Civil Liberties Union (ACLU), the National Association of Criminal Defense Lawyers (NACDL), the Council on American Islamic Relations (CAIR) and named individual plaintiffs -- including several lawyers -- seeking declaratory and injunctive relief demanding the NSA cease and desist warrantless interception of Americans' electronic and telephone conversations because such interceptions "seriously compromise the First Amendment's guarantees of the freedoms of speech, of the press, and of association, and the Fourth Amendment's prohibition on warrantless searches and seizures."[4]

---

[1] *See* James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," New York Times, December 16, 2005.

[2] The first of what is expected to be several Senate Judiciary Committee hearings, with Attorney General Alberto Gonzales as the sole witness for a full day, was held on February 6, 2006, and the Senate Intelligence Committee will soon follow with its own hearings on the NSA program.

[3] *See* Jerry Markon, "Spying Cited in Bid To Erase Terror Plea," Washington Post February 4, 2006.

[4] See NACDL News release, January 19, 2006, "When the Government Becomes a Lawbreaker, Part 2," available at: http://www.nacdl.org/public.nsf/newsreleases/2006mn001?OpenDocument

In light of the importance of these issues, ABA President Michael S. Greco appointed a Task Force on Domestic Surveillance in the Fight Against Terrorism[5] to "examine the legal issues surrounding federal government surveillance conducted inside the United States relating to the investigation of potential terrorist activities" and bring a preliminary report with recommendations to the ABA House of Delegates at the February 2006 Midyear Meeting. In his appointment letters, President Greco stated:

> Recent revelations about the National Security Agency's domestic surveillance program remind us that we must continually and vigilantly protect our Constitution and defend the rule of law.

While the Task Force was operating under intense time pressures, it benefitted from the fact that substantial analyses of the legal issues had already been undertaken by a wide and diverse variety of sources. For example, the Department of Justice issued a 42 page "white paper," an Assistant Attorney General sent a strong letter responding to congressional inquiries, and the Attorney General delivered a major address on the issue at the Georgetown Law Center. Each, as expected, vigorously defended what the Administration is calling a "terrorist surveillance program" (as opposed to "domestic surveillance" or "warrantless eavesdropping"), as being entirely lawful and within the President's constitutional and statutory authority. [6]

On the other side of the issue, a variety of constitutional law scholars and former government officials have released letters and memoranda decrying the NSA program as a violation of FISA, and the Constitution,[7] and several Web sites have collected documents related to the NSA

---

[5] The Task Force is chaired by **Neal R. Sonnett**, and includes **Mark D. Agrast**, **Deborah Enix-Ross**, **Stephen A. Saltzburg**, **Hon. William S. Sessions**, **James R. Silkenat**, and **Suzanne Spaulding**. **Dean Harold Hongju Koh** and **Dean Elizabeth Rindskopf Parker** serve as Special Advisers, and **Alan J. Rothstein** was named Liaison to the Task Force from the New York City Bar, whose members have contributed substantially to this Report. A short biography of each appears in an Appendix to this Report.

[6] *See, e.g.*, Letter to House and Senate Intelligence Committee Leaders from Assistant Attorney General William E. Moschella on Legal Authority for NSA Surveillance, December 22, 2005, available at http://www.fas.org/irp/agency/doj/fisa/doj122205.pdf; DOJ Legal Authorities Supporting the Activities of the National Security Agency Described by the President, January 19, 2006, available at www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf; Prepared Remarks for Attorney General Alberto R. Gonzales at the Georgetown University Law Center, January 24, 2006, available at: http://www.usdoj.gov/ag/speeches/2006/ag_speech_0601241.html

[7] Letter to Congress from14 Constitutional Law Professors and Former Government Officials, January 9, 2006, available at: http://www.fas.org/irp/agency/doj/fisa/doj-response.pdf.

domestic surveillance issues.[8]

The bipartisan Congressional Research Service issued three reports: a report on the legislative history of the AUMF issued on January 4, 2006; a lengthy report issued on January 5, 2006, analyzing the NSA program, and another report on January 18, 2006, regarding the statutory reporting procedures required in intelligence matters.[9]

The Task Force unanimously agreed that the President should abide by the limitations which the Constitution imposes on a president under our system of checks and balances and respect the essential roles of the Congress and the judicial branch in ensuring that our national security is protected in a manner consistent with constitutional guarantees. There was also consensus that any electronic surveillance inside the United States by any U.S. government agency for foreign intelligence purposes must comply with the provisions of FISA and that, if the President believes

---

[8] *See, e.g.*, Findlaw at: http://news.findlaw.com/legalnews/documents/archive_n.html#nsa; Bill of Rights Defense Committee, at: http://bordc.org/threats/spying.php; Federation of American Scientists, at: http://www.fas.org/irp/agency/doj/fisa/; Electronic Privacy Information Center, at: http://www.epic.org/privacy/terrorism/fisa/.

[9] *See* "Authorization For Use Of Military Force in Response to the 9/11 Attacks (P.L. 107-40): Legislative History," Congressional Research Service January 4, 2006, at: http://www.fas.org/sgp/crs/natsec/RS22357.pdf; "Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information," Congressional Research Service, January 5, 2006, at: http://www.fas.org/sgp/crs/intel/m010506.pdf; "Statutory Procedures Under Which Congress Is To Be Informed of U.S. Intelligence Activities, Including Covert Actions," Congressional Research Service, January 18, 2006, at: http://news.findlaw.com/hdocs/docs/nsa/crs11806rpt.pdf.

that FISA is inadequate to safeguard national security, he should seek appropriate amendments or new legislation rather than acting without explicit statutory authorization.

The Recommendation also urges the Congress to conduct a thorough, comprehensive investigation of the issues surrounding the NSA domestic surveillance program, with proceedings that are open to the public and conducted in a fashion that will provide a clear and credible account to the people of the United States, except to the extent the Congress determines that any portions of such proceedings must be closed to prevent the disclosure of classified or other protected information.

The Task Force also calls for the Congress to thoroughly review and make recommendations concerning the intelligence oversight process, and urges the president to ensure that the House and Senate are fully and currently informed of all intelligence operations as required by the National Security Act of 1947.

B. Electronic Surveillance for Foreign Intelligence Purposes Conducted Within the United States Should Comply with FISA

The Administration concedes that its secret NSA electronic surveillance program entails "electronic surveillance" of "United States persons" as those terms are defined by the Foreign Intelligence Surveillance Act ("FISA"). The Administration maintains, however, that Congress, in enacting the Authorization for the Use of Military Force on September 18, 2001 ("AUMF"), Pub. L. No. 107-40, 115 Stat. 224, authorized the President to conduct such foreign intelligence electronic surveillance without obtaining the court orders required by FISA.

As we explain, FISA is a detailed and comprehensive statute that was enacted to strike a balance between the recognized need to conduct foreign intelligence surveillance and the need to protect fundamental civil liberties. FISA makes specific provision for exceptions to its requirements in emergencies and in the event of war. Moreover, following 9/11, FISA was amended by the Patriot Act, at the behest of the President, to provide the greater flexibility the administration argued was needed to address the enhanced threat of international terrorism so tragically dramatized by the 9/11 attacks. The Patriot Act amendments, however, left intact FISA's explicit provisions making FISA procedures the exclusive means for conducting electronic surveillance for foreign intelligence purposes in the United States.

There is nothing in either the language of the AUMF or its legislative history to justify the assertion that the general grant of authority to use "all necessary and appropriate force" against Al Qaeda and those affiliated with or supporting it, was intended to amend, repeal or nullify the very specific and comprehensive terms of FISA. Nor, under our system of checks and balances, is there any serious constitutional issue concerning Congress' power to regulate electronic surveillance for foreign intelligence purposes where it intercepts the communications of persons within the United

States, to assure that the Nation has the necessary means to combat terrorism while also assuring that those means are not abused to unjustifiably infringe civil liberties, through invasions of privacy that not only violate the Fourth Amendment but chill the freedom of speech and association protected by the First Amendment.

1. The FISA Statutory Framework

In 1967, the Supreme Court held for the first time that as a general matter wiretapping was subject to the Fourth Amendment's protections against unreasonable searches and its requirement of a warrant in most circumstances. *Katz* v. *United States*, 389 U.S. 347 (1967). The Court left open, however, the question of whether the Fourth Amendment applied to wiretapping conducted to protect national security. *Id.* at 358.

Subsequently, in 1972, the Court held that wiretapping conducted for domestic security purposes was subject to the Fourth Amendment and required a warrant. *United States* v. *United States District Court*, 407 U.S. 297, 313-14, 317, 319-20 (1972). It left open the question, however, whether electronic surveillance for foreign intelligence purposes was subject to the Fourth Amendment's requirement of a warrant issued by a court authorizing the surveillance. *Id.* at 308.

There followed a period in which lower courts differed on this question. During this same period, following the Watergate scandal and revelations of abuses of wiretapping during the Nixon administration, and with the support of both Presidents Ford and Carter, a Senate Select Committee, headed by Senator Frank Church (the "Church Committee"), undertook a comprehensive investigation of government wiretapping and other surveillance procedures conducted by the Executive branch without a warrant.

The Church Committee exposed substantial abuses of this purported authority. *See* S. Rep. No. 94-755 (Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities) 94th Cong., 2nd Sess., Book II at 5-20 (1976). It therefore recommended congressional legislation to provide the government with needed authority to conduct surveillance to protect national security but to protect against the abuses of that authority and the serious infringements of civil liberties disclosed by the investigation. *Id.* at 296-341. FISA was enacted to carry out these recommendations. Pub. L. 95-511, 92 Stat. 1783 (1978).

The bill, as enacted, had the full support of President Carter and the Executive branch. *See* S. Rep. No. 95-604 (Judiciary Committee) 95th Cong., 1st Sess., Part 1 at 4 (1977). President Carter's Attorney General, Griffin Bell, testifying in support of the bill, emphasized:

> In my view this bill . . . sacrifices neither our security nor our civil liberties, and assures that the abuses of the past will remain in the past and that the dedicated and patriotic men and women who serve this country in intelligence positions . . . will

> have the affirmation of Congress that their activities are proper and necessary.

Id. at 4. *See also* S. Rep. No. 95-701 (Intelligence Committee), 95th Cong., 2nd Sess., 6-7 (1978).

When President Carter signed FISA into law, he said in his signing statement:

> The bill requires, for the first time, a prior judicial warrant for *all* electronic surveillance for foreign intelligence or counterintelligence purposes in the United States in which communications of U.S. persons might be intercepted. It clarifies the Executive's authority to gather foreign intelligence by electronic surveillance in the United States. It will remove any doubt about the legality of those surveillances which are conducted to protect our country against espionage and international terrorism. It will assure FBI field agents and others involved in intelligence collection that their acts are authorized by statute and, if a U.S. person's communications are concerned, by a court order. And it will protect the privacy of the American people.
>
> In short, the act helps to solidify the relationship of trust between the American people and their Government. It provides a basis for the trust of the American people in the fact that the activities of their intelligence agencies are both effective and lawful. It provides enough secrecy to ensure that intelligence relating to national security can be securely required, while permitting review by the courts and Congress to safeguard the rights of Americans and others.

See Statement on Signing S.1566 Into Law, October 25, 1978, available at: http://www.cnss.org/Carter.pdf.

FISA applies to "electronic surveillance" which, among other things, would include the electronic acquisition, within the United States, of the content of communications to or from the United States or of communications of a "United States person" located in the United States. 50 U.S.C. § 1801 (f). A "United States person" includes, among others, U.S. citizens or permanent resident aliens. The Administration has never questioned, and in fact, has conceded, that the NSA surveillance program meets FISA's definition of "electronic surveillance."[10]

With certain exceptions, FISA requires that to conduct "electronic surveillance" the government must obtain a court order from a special, secret court created by FISA known as the FISA court. To obtain such an order, a federal officer must certify that "a significant purpose" of the

---

[10] Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005), available at: www.whitehouse.gov/news/releases/2005/12/20051219-1.html.

surveillance is to obtain foreign intelligence information and provide a statement describing, among other things, the basis for the belief that the information sought is foreign intelligence information. 50 U.S.C. § 1804 (a)(4) and (7). The court will issue an order authorizing the surveillance upon making a series of findings, including that there is probable cause to believe that a target of the electronic surveillance is a foreign power or agent of a foreign power and that the surveillance is directed at facilities used, or about to be used, by a foreign power or agent of a foreign power. *Id.* at § 1805 (a) and (b). A "foreign power" includes international terrorist groups and an "agent of a foreign power" includes a person other than a United States person engaged in international terrorism. *Id.* at §1801(a)(4) and (b)(1)(C).

FISA provides a number of exceptions, two of which are of particular significance. First, it permits electronic surveillance without first obtaining a court order, in situations certified by the Attorney General as an emergency, provided that an order is sought within 72 hours of the authorization of the surveillance by the Attorney General. *Id.* at §1805(f). Second, recognizing the exigencies created by war, the President through the Attorney General, may authorize electronic surveillance without a court order for a period of 15 days after a declaration of war by Congress. *Id.* at § 1811.

This provision was intended to provide time to enable Congress to amend FISA if it was determined necessary to do so to meet special war-time needs. H.R. Conf. Rep. No. 95-1720, 95th Cong., 2nd Sess., 34 (1978). Notably, Congress rejected a request to make this exception extend for one year after a declaration of war, indicating that 15 days should be sufficient to make any necessary amendments. *Id.*

Congress made explicit its intention that FISA is the exclusive means by which electronic surveillance for foreign intelligence purposes may be conducted. 18 U.S.C. §2511 provides in part: "[T]he Foreign Intelligence Surveillance Act of 1978 [50 U.S.C. § 1801 *et seq.*] shall be the exclusive means by which electronic surveillance, as defined in Section 101 of such Act [50 U.S.C. §1801] . . . may be conducted." FISA also makes it a criminal offense "to engage in electronic surveillance under color of law except as authorized by statute." 50 U.S.C. § 1809 (a).[11]

Following the attacks of September 11, 2001, the Administration asked Congress to enact legislation to enhance its ability to protect the nation against such attacks by Al Qaeda and other international terrorists. Congress responded promptly to that request, enacting the USA PATRIOT

[11] Two separate statutes regulate electronic surveillance: FISA governs electronic surveillance for foreign intelligence purposes; Title III of the Crime Control and Safe Streets Act, 18 U.S.C. §§ 2510 *et seq.*, 2701 *et seq.*, and 3121 *et seq.*, governs domestic electronic surveillance. 18 U.S. C. § 2511 expressly makes these two statutes the exclusive means for conducting electronic surveillance for foreign intelligence or domestic purposes.

Act in October and the Intelligence Authorization Act in December.

Those laws amended FISA in a number of respects, including expanding the period for emergency electronic surveillance from 24 hours to 72 hours and reducing the requirement that the government certify that the foreign intelligence gathering was a "primary purpose" of the electronic surveillance to a showing only that it was "a significant purpose." *See* Intelligence Authorization Act for Fiscal Year 2002, Pub. L. No. 107-108, § 314(a)(2)(B), 115 Stat. 1394 (Dec. 28, 2001); USA PATRIOT Act, Pub. L. 107-56, § 218, 115 Stat. 272 (Oct. 26, 2001).[12]

In sum, FISA is a comprehensive and exclusive procedure for conducting foreign intelligence electronic surveillance in the United States. It anticipates emergencies and the exigencies of war, and it was specifically amended at the Administration's request to make it more responsive to the need to combat international terrorism following the attacks of September 11, 2001. Nevertheless, the Administration concedes that NSA conducted electronic surveillance for a period of four years without complying with FISA's procedures.

2. The AUMF Does Not Create an Exception to FISA

The argument that Congress implicitly authorized the NSA program when it enacted the Authorization for Use of Military Force (AUMF) against al Qaeda, Pub. L. No. 107-40, 115 Stat. 224 (September 18, 2001), is unpersuasive. There is nothing in the text or the history of the AUMF to suggest that Congress intended to permit the Executive to engage in any and all warrantless electronic surveillance in the United States without judicial approval or a showing of probable cause as required by FISA.

The argument put forward by the Executive assumes that Congress intended to remove all restraint on electronic surveillance currently mandated by FISA or Title III, at least with regard to the fight against terrorism. The history of FISA demonstrates a congressional commitment to regulate the use of electronic surveillance and to assure that there is a judicial check on Executive power. Nothing in the AUMF suggests that Congress intended to unleash the Executive to act

[12] Indeed, Congress has amended FISA a total of five times since 1999 in response to requests from the Department of Justice. In addition to those set forth above, FISA amendments related to: court orders for pen registers, trap and trace devices, and certain business records of suspected agents of a foreign power, P.L. 105-272, §§ 601, 602 (1999); definition of "agent of a foreign power" to include people working for a foreign government who intentionally enter the United States with a fake ID or who obtain a fake ID while inside the US, P.L. 106-120, § 601 (2000); which federal officials could authorize applications to the FISC for electronic surveillance and physical searches, P.L. 106-567, §§ 602, 603 (2001); eliminated requirement that non U.S. persons be acting on behalf of a foreign power in order to be targeted, P.L. 108-458, § 6001 (2004).

without judicial supervision and contrary to standards set by Congress in conformity with the Constitution.

The Executive's argument rests on an implicit, unstated inference from the AUMF. Such an inference is directly contrary to the explicit text of FISA. The Supreme Court has stated that specific and carefully drawn statutes prevail over general statutes where there is a conflict. *Morales v. TWA, Inc.*, 504 U.S. 374, 384-85 (1992) (quoting *International Paper Co. v. Ouelette*, 479 U.S. 481, 494 (1987)).

FISA contains a section entitled "Authorization during time of war," which provides that "[n]otwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information *for a period not to exceed fifteen calendar days following a declaration of war by the Congress*." 50 U.S.C. § 1811 (emphasis added). One need not parse the language to determine Congressional intent, because the plain meaning of the language is indisputable: i.e., When Congress declares war, the President may permit the Attorney General to authorize electronic surveillance without a court order under FISA for 15 days. Thus, Congress limited the Executive power to engage in electronic surveillance without judicial supervision to 15 days **following a formal declaration of war**. It is inconceivable that the AUMF, which is not a formal declaration of war, could be fairly read to give the President more power, basically unlimited, than he would have in a declared war.

The legislative history of § 1811 demonstrates that Congress intended that the Executive seek legislation if it concluded that there was a need for electronic surveillance not authorized by FISA for more than 15 days: "The Conferees intend that this [15-day] period will allow time for consideration of any amendment to this act that may be appropriate during a wartime emergency. . . . The conferees expect that such amendment would be reported with recommendations within 7 days and that each House would vote on the amendment within 7 days thereafter." H.R. Conf. Rep. No. 95-1720, at 34 (1978).[13]

The Executive's argument distorts FISA and makes meaningless18 U.S.C. § 2511(2)(f), the provision that identifies FISA and specific criminal code provisions as "the *exclusive* means by which electronic surveillance . . . may be conducted" because the argument assumes that the

[13] The House version of the bill would have authorized the President to engage in warrantless electronic surveillance for the first year of a war, but the Conference Committee rejected so long a period of judicially unchecked eavesdropping as unnecessary.

Executive may treat any congressional act as authorizing an exception from Title III and FISA. Were the argument accepted, the Executive could justify repeal or suspension of FISA and Title III restrictions in statutes appropriating money for federal agencies or virtually any other legislation that, in the sole judgment of the Executive, would be rendered more effective by greater electronic surveillance.

The argument that the AUMF implicitly creates an exception to FISA and is therefore consistent with § 2511(2)(f) strains credulity. It rests on the notion that Congress, although it never mentioned electronic surveillance or FISA in the AUMF, nevertheless implicitly intended to create an undefined, unrestrained exception to FISA and give the Executive unlimited power to engage in unlimited electronic surveillance with no judicial review.

In an area as heavily regulated and as important to basic notions of privacy as electronic surveillance, it is inconceivable that Congress would have ceded greater unfettered power and discretion to the Executive in dealing with al Qaeda than it would in a declared war.

Moreover, the Attorney General has essentially conceded that no reasonable person would conclude that Congress intended to cede such power to the Executive: "We have had discussions with Congress in the past—certain members of Congress—as to whether or not FISA could be amended to allow us to adequately deal with this kind of threat, and we were advised that that would be difficult, if not impossible." See Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005), available at http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html. In light of this concession, the claim that Congress granted the Executive this authority under the AUMF is not credible.

The administration has argued that its position is supported by the Supreme Court's opinion in *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004), but this is also unpersuasive. A plurality of the Court in *Hamdi* held that the AUMF authorized military detention of enemy combatants captured on the battlefield abroad as a "fundamental incident of waging war." *Id.* at 519. When Congress authorizes the use of force, it clearly contemplates that the enemy will be killed or captured. There can be little doubt that those who are captured on the battle field may be held while the battle is fought. Typically, those captured are deemed prisoners of war. But, in *Hamdi*, the question was whether a captured individual could be held as an enemy combatant. The plurality expressly limited its affirmative answer to individuals who were "part of or supporting forces hostile to the United States or coalition partners *in Afghanistan and who engaged in an armed conflict against the United States there*." *Id.* at 516 (emphasis added).

It is not a fair reading of the *Hamdi* case to suggest that AUMF repeals all limitations on Executive power previously contained in any federal statute as long as the Executive in its sole discretion deems additional power useful in the general fight against terror.

The Hamdi plurality agreed "that indefinite detention for the purpose of interrogation," even of conceded enemy combatants, "is not authorized" by the AUMF. *Id.* at 2641. If Congress did not provide the Executive with the right to detain enemy combatants for intelligence purposes, it is inconceivable that Congress intended to permit the indefinite eavesdropping and invasion of privacy of American citizens who are neither enemy combatants nor suspected of criminal activity.

3. The Government's Interpretation of the AUMF Is Not Required to Avoid a Constitutional Question

The Administration mistakenly argues that its construction of the AUMF is required to avoid a serious constitutional question. First, the canon of avoidance only comes into play if there is an ambiguity in a statute. *See United States* v. *Oakland Cannabis Buyers' Coop.*, 532 U.S. 483, 494 (2001).

But neither FISA nor the AUMF are ambiguous on the question of electronic surveillance. FISA explicitly makes its procedures the exclusive means for conducting electronic surveillance. Meanwhile, the AUMF contains no reference to electronic surveillance, and as indicated above, nothing in the history or circumstances suggests that the AUMF was intended to authorize electronic surveillance.

In any event, the constitutional question must be serious and substantial. The Administration claims that unless its construction of the AUMF is accepted, a serious constitutional question would be raised as to whether FISA unconstitutionally encroaches on inherent powers of the President as Commander-in-Chief. That question is neither serious nor substantial. Even assuming that, after FISA, the President retains inherent authority to conduct electronic surveillance without a warrant to acquire foreign intelligence – a question that has never been decided – that does not mean that Congress lacks authority to regulate the exercise of that authority to prevent its abuse and unnecessary intrusions on civil liberties.

It should be noted that both President Ford and President Carter supported legislation to regulate the conduct of foreign intelligence surveillance, and as noted, FISA was enacted with the full support of President Carter. As the Senate report accompanying the bill that became FISA noted:

> The basis for this legislation is the understanding – concurred in by the Attorney General – that even if the President has an "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.

S. Rep. (Judiciary Committee) No. 95-604, 95th Cong., 1st Sess., Part 1 at 16 (1977). As Congress observed, this analysis was "supported by two successive Attorneys General." H.R. Rep. No. 95-1283, 95th Cong., 2nd Sess., Part 1 at 24 (1978).

The analysis is plainly correct. Whatever inherent authority the President may have to conduct foreign intelligence surveillance, Congress also has the authority under Article I to regulate the exercise of that authority. *See* Article I, Section 8, Cl. 1, 14 (power to provide for the common defense), Article I, Section 8, Cl. 3 (power to regulate commerce).

Here, through FISA, Congress has exercised its Article I powers to regulate electronic surveillance for foreign intelligence purposes in great detail and made it the exclusive means for conducting such surveillance. The NSA domestic surveillance program is in direct conflict with this detailed statutory scheme. Under the criteria set forth in Justice Jackson's famous concurring opinion in *Youngstown Sheet and Tube Co.* v. *Sawyer*, in these circumstances the President's inherent power is at its "lowest ebb." 343 U.S. 579, 637 (1952). To sustain the President's power here a court would have to find that such power was "beyond control by Congress." *Id.* at 640. In other words, the President's authority must be not just inherent but exclusive.

Such a conclusion would be at odds with the principles of separation of powers and our cherished system of checks and balances and faces a particularly high hurdle where, as here, individual liberties are at stake. As Justice O'Connor observed in *Hamdi* v. *Rumsfeld,* 542 U.S. 507, 536 (2004):

> Whatever power the United States Constitution envisions for the Executive in its exchanges with other nations or with enemy organizations in times of conflict, it most assuredly envisions a role for all three branches when individual liberties are at stake.

Id.. (quoting *Mistretta* v. *United States*, 488 U.S. 361, 380 (1989) (it was "the central judgment of the Framers of the Constitution that, within our political scheme, the separation of governmental powers into three coordinate Branches is essential to the preservation of liberty").

The government argues that prior presidents have exercised their inherent authority to conduct electronic surveillance without a warrant for foreign intelligence purposes and that courts have consistently upheld the exercise of that power.

But FISA was enacted precisely because, prior to FISA, prior presidents had repeatedly abused that power. *See* S. Rep. (Judiciary Committee) No. 95-604, 95th Cong., 1st Sess., Part 1 at 7-8 (1977) ("[The Church Committee] has concluded that every President since Franklin D. Roosevelt asserted the authority to authorize warrantless electronic surveillance and exercised that authority. While the number of illegal or improper national security taps and bugs conducted during

the Nixon administration may have exceeded those in previous administrations, the surveillances were regrettably by no means atypical . . . [and were] 'often conducted by illegal or improper means' . .").

In enacting FISA, Congress was concerned not only with violations of the Fourth Amendment, but the chilling effect that abuses of electronic surveillance had on free speech and association. As the Senate Report accompanying FISA explained:

> Also formidable – although incalculable – is the "chilling effect" which warrantless electronic surveillance may have on the constitutional rights of those who were not targets of the surveillance, but who perceived themselves, whether reasonably or unreasonably, as potential targets. . . . The exercise of political freedom depends in large measure on citizens' understanding that they will be able to be publicly active and dissent from official policy, within lawful limits, without having to sacrifice the expectation of privacy that they rightfully hold. Arbitrary or uncontrolled use of warrantless electronic surveillance can violate that understanding and impair that public confidence so necessary to an uninhibited political life.

Id. at 8.

Moreover, the cases upholding the President's inherent authority all preceded the enactment of FISA. No court has ever held that Congress was without power to regulate electronic surveillance for foreign intelligence purposes to protect against the abuse of such surveillance. The government incorrectly relies on a statement in *In re Sealed Case*, 310 F.3d 717 (FISA Court of Review 2002), that: "We take for granted that the President does have [inherent authority to conduct warrantless searches to obtain foreign intelligence] and, assuming that is so, FISA could not encroach on the President's constitutional power." *Id.* at 742. But this statement is dictum, made without any analysis, in a case which raised no issue about the President's inherent authority or the constitutional power of Congress to regulate the President's exercise of that authority under FISA.

To the contrary, the issue in *Sealed Case* was whether FISA's criteria for the issuance of court orders authorizing electronic surveillance satisfied the requirements of the Fourth Amendment. The Court of Review held that they did. Moreover, the cases cited by the Court of Review for the proposition that the President had inherent authority to conduct warrantless surveillance all addressed surveillance predating the enactment of FISA and hence, have no bearing on whether any inherent authority the President had survives FISA, i.e., whether the President has not just inherent but exclusive authority to order warrantless surveillance of Americans.

Finally, if there is any serious constitutional question, it is raised by the government's construction of the AUMF. It would give the President unfettered discretion, subject neither to regulation by Congress nor scrutiny by a court, to conduct warrantless electronic surveillance of Americans, based on the President's (or his designees') unilateral determination that there is reason to believe that one of the parties to the communication is a member of Al Qaeda or of groups affiliated with or supporting Al Qaeda.

While the Supreme Court has never addressed the question of whether such warrantless electronic surveillance would meet the requirements of the Fourth Amendment, and a conclusive assessment of that question would require a careful analysis of the facts, which the secrecy surrounding this program precludes. The government maintains that such surveillance fits within a "special needs" exception to the Fourth Amendment's requirement of a warrant or other court order authorizing a search and that given the post 9/11 circumstances its electronic surveillance without a court order was not an "unreasonable search" within the meaning of the Fourth Amendment. But the "special needs" exception is a narrow doctrine. The doctrine has usually been invoked to protect law enforcement officers from concealed weapons, prevent the destruction of physical evidence like illegal drugs, or permit testing for drugs or alcohol to regulate the safety of schools, workplaces or transportation. *See*, e.g., *O'Connor* v. *Ortega*, 480 U.S. 709 (1987); *New York* v. *Burger*, 482 U.S. 691 (1987), *Griffin* v. *Wisconsin*, 483 U.S. 868 (1987), *Skinner* v. *Railway Labor Executives' Ass'n*, 489 U.S. 602 (1989). None of these cases involved government acquisition of the content of private communications, where the intrusion into privacy has a chilling effect on freedom of speech and association. It was for that very reason that the Supreme Court rejected government claims that it had a special need for warrantless electronic surveillance of communications for domestic security purposes. As the Court explained:

> National security cases . . . often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime . . . . 'Historically, the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power.' [Citation omitted.] History abundantly documents the tendency of Government – however benevolent and benign its motives – to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs.

United States v. *United States District Court*, 407 U.S. 297, 313-314 (1972). These considerations also apply to electronic surveillance of persons in the United States for foreign intelligence purposes.

Thus, even if there were a "special needs" exception for warrantless surveillance of Americans, it is likely that a court would construe it extremely narrowly, subject to the Fourth amendment, and available only in extraordinary circumstances unforeseen by Congress and in which

there is no time to seek amendment to the law. It is highly unlikely that a court would uphold the exercise of such authority for four years, let alone indefinitely. The government has not shown that resort to FISA's procedures is impractical, nor has it provided any explanation as to why in the more than four years since 9/11 it has not asked Congress for any amendments to FISA – beyond those sought and obtained under the USA PATRIOT Act – to address any alleged inadequacy of FISA.

The government's argument that the President and the NSA have limited the program to circumstances where they have "reason to believe" that at least one party to the communication is a member of Al Qaeda or organizations affiliated with or supporting Al Qaeda does not provide reasonable protections against unjustified invasions of the privacy of innocent persons or a safeguard against abuse from a long-term program. The "very heart" of the Fourth Amendment requirement is that the judgment of whether the evidence justifies invasion of a citizen's privacy be made by a "neutral and detached magistrate." *United States* v. *United States District Court*, 407 U.S. at 316 (quoting *Coolidge* v. *New Hampshire*, 403 U.S. 443, 453 (1971)). As the Court there explained:

> 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. . . . The Fourth Amendment contemplates a prior judicial judgment . . . , not the risk that executive discretion may be reasonably exercised. This judicial role accords with our basic constitutional doctrine that individual freedoms will best be preserved through a separation of powers and division of functions among the different branches and levels of Government.

Id. at 317 (internal citations omitted).

Thus, warrantless electronic surveillance in the United States for foreign intelligence purposes would raise very serious and substantial Fourth Amendment questions.

C. The Need for Additional Congressional Investigation and Oversight

There are important questions about the nature, scope, and operation of the NSA domestic surveillance program that remain unanswered and which have not been examined by the Congress. For example, it has been reported that serious dissension existed within the administration over the expansive authority granted to the NSA, that then-Deputy Attorney General James Comey, acting in the absence of Attorney General John Ashcroft who was in the hospital with a serious pancreatic condition, once refused to reauthorize the NSA program, causing a high level delegation of White House Counsel Gonzales and chief of staff Andy Card to visit Ashcroft in the hospital to appeal Comey's decision.[14]

The questions about the scope of the NSA's electronic surveillance are highlighted by conflicting statements made by government officials. While the Administration now argues that only calls by suspected terrorists emanating from outside the United States have been monitored, the San Francisco Chronicle reported on December 22, 2005 that:

> White House Press Secretary Scott McClellan said National Security Agency surveillance ordered by the president after the Sept. 11 attacks four years ago might have inadvertently picked up innocent conversations conducted entirely within the United States by Americans or foreigners.
>
> That would violate what McClellan called Bush's requirement that one party to the communication had to be outside the United States and raised the possibility that NSA surveillance of terror suspects had morphed into surreptitious monitoring of some communications strictly within the United States without court approval.
>
> In Congress, Rep. Peter Hoekstra, R-Mich., chairman of the House Intelligence Committee, told a news conference that White House officials had acknowledged during briefings for congressional leaders that U.S.-to-U.S. communications might be inadvertently intercepted during NSA's worldwide quest for al Qaeda-related conversations between terror suspects in the United States and overseas.

See Stewart M. Powell, "White House acknowledges some taps wholly domestic," Hearst Newspapers, December 22, 2005, at: http://sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2005/12/22/MNGOHGBM9N1.DTL

---

[14] *See* Daniel Klaidman, Stuart Taylor Jr. and Evan Thomas, "Palace Revolt," Newsweek, February 6, 2006, at: http://www.msnbc.msn.com/id/11079547/site/newsweek.

Moreover, public statements made well after the NSA program was underway raise issues that should be examined by Congress. When James A. Baker, the Justice Department's counsel for intelligence policy, testified before the Senate Select Committee on Intelligence on July 31, 2002, he stated that the Administration did not support a proposal by Senator Mike DeWine (R-OH) to lower the legal standard for electronic surveillance "because the proposed change raises both significant legal and practical issues," might not "pass constitutional muster," and "could potentially put at risk ongoing investigations and prosecutions." He added:

> We have been aggressive in seeking FISA warrants and, thanks to Congress's passage of the USA PATRIOT Act, we have been able to use our expanded FISA tools more effectively to combat terrorist activities. It may not be the case that the probable cause standard has caused any difficulties in our ability to seek the FISA warrants we require, and we will need to engage in a significant review to determine the effect a change in the standard would have on our ongoing operations. If the current standard has not posed an obstacle, then there may be little to gain from the lower standard and, as I previously stated, perhaps much to lose.

See Dan Eggen, "White House Dismissed '02 Surveillance Proposal," Washington Post, January 26, 2006. Interestingly, these paragraphs no longer appear in the official version of Baker's testimony.[15]

Senator Russell Feingold recently accused Attorney General Gonzales of "misleading the Senate" during his confirmation hearings in his answer to a question about whether the president could authorize warrantless wiretapping of U.S. citizens. As the Washington Post reported:

> Gonzales said that it was impossible to answer such a hypothetical question but that it was "not the policy or the agenda of this president" to authorize actions that conflict with existing law. He added that he would hope to alert Congress if the president ever chose to authorize warrantless surveillance, according to a transcript of the hearing.

See Carol D. Leonnig, "Gonzales Is Challenged on Wiretaps," Washington Post, January 31, 2006, at: http://www.washingtonpost.com/wp-dyn/content/article/2006/01/30/AR2006013001318.html.

---

[15] *See* Chris Anderson, "NSA, FISA, and the 'Missing 3 Paragraphs,'" IndyMedia, January 27, 2006, at:http://nyc.indymedia.org/en/2006/01/63921.html.

Even the President has come under attack for potentially misleading statements. In a speech in Buffalo, NY, on April 20, 2004 – more than two years after the NSA program had been authorized – President Bush stated:

> Now, by the way, any time you hear the United States government talking about wiretap, it requires -- a wiretap requires a court order. Nothing has changed, by the way. When we're talking about chasing down terrorists, we're talking about getting a court order before we do so.

See "President Bush: Information Sharing, Patriot Act Vital to Homeland Security," Remarks by the President in a Conversation on the USA Patriot Act, Kleinshans Music Hall, Buffalo, New York, April 20, 2004, at: http://www.whitehouse.gov/news/releases/2004/04/20040420-2.html

Thus, the Task Force Recommendations also urge the Congress to conduct a thorough, comprehensive investigation to determine: (a) the nature and extent of electronic surveillance of U.S. persons conducted by any U.S. government agency for foreign intelligence purposes that does not comply with FISA; (b) what basis or bases were advanced (at the time it was initiated and subsequently) for the legality of such surveillance; (c) whether the Congress was properly informed of and consulted as to the surveillance; and (d) the nature of the information obtained as a result of the surveillance and whether it was retained or shared with other agencies.

We also believe that these hearings should be open and conducted in a fashion that will provide a clear and credible account to the people of the United States, except to the extent the Congress determines that any portions of such proceedings must be closed to prevent the disclosure of classified or other protected information.

Finally, the Congressional Research Service report of January 18, 2006, "Statutory Procedures Under Which Congress Is To Be Informed of U.S. Intelligence Activities, Including Covert Actions," [16] makes it clear that Congress needs to thoroughly review and make recommendations concerning the intelligence oversight process, to ensure that the House and Senate are fully and currently informed of all intelligence operations as required by the National Security Act of 1947.

D. <u>Conclusion</u>

The American Bar Association has stood shoulder to shoulder with the president in the fight against terrorism. Every member of the Task Force – indeed, every member of this great Association – wants the president to use all appropriate tools to defeat these enemies of democracy.

---

[16] See Fn. 9, *supra*.

However, as President Greco said in creating the Task Force, "We must continually and vigilantly protect our Constitution and defend the rule of law." And, as Supreme Court Justice Murphy warned in a case arising during World War II:

> [W]e must be on constant guard against an excessive use of any power, military or otherwise, that results in the needless destruction of our rights and liberties. There must be a careful balancing of interests. And we must ever keep in mind that "The Constitution of the United States is a law for rulers and people, equally in war and in peace, and covers with the shield of its protection all classes of men, at all times, and under all circumstances."

Duncan v. Kahanamoku, 327 U.S. 304, 335 (1946) (Murphy, J., concurring).

We simply cannot allow our constitutional freedoms to become a victim of the fight against terrorism. The proposed Recommendations should be adopted by the ABA House of Delegates in order to strike a proper balance between individual liberty and Executive power.

Respectfully submitted,

NEAL R. SONNETT, Chair
ABA Task Force on Domestic Surveillance
in the Fight Against Terrorism

February 2006

APPENDIX

ABA Task Force on Domestic Surveillance in the Fight Against Terrorism
Biographies

Chair

Neal R. Sonnett

Mr. Sonnett is a former Assistant United States Attorney and Chief of the Criminal Division for the Southern District of Florida. He heads his own Miami law firm concentrating on the defense of corporate, white collar and complex criminal cases throughout the United States. He has been profiled by the National Law Journal as one of the "Nation's Top White Collar Criminal Defense Lawyers," was selected three times by that publication as one of the "100 Most Influential Lawyers In America," and has been included in all 20 editions of The Best Lawyers in America.

Mr. Sonnett is a former Chair of the ABA Criminal Justice Section, which he now represents in the ABA House of Delegates, and a former President of the National Association of Criminal Defense Lawyers. He is Chair-Elect of the American Judicature Society, Secretary of the ABA Section of Individual Rights and Responsibilities, Chair of the ABA Task Force on Treatment of Enemy Combatants, and serves as the ABA's official Observer for the Guantanamo military commission trials. He is also a member of the ABA Task Force on the Attorney-Client Privilege, the Task Force on Gatekeeper Regulation and the Profession, and he served on the ABA Justice Kennedy Commission. He is a Life Fellow of the American Bar Foundation and serves on the ALI-ABA Advisory Panel on Criminal Law and on the Editorial Advisory Boards of The National Law Journal and Money Laundering Alert.

Mr. Sonnett has received the ADL Jurisprudence Award and the Florida Bar Foundation Medal Of Honor for his "dedicated service in improving the administration of the criminal justice system and in protecting individual rights precious to our American Constitutional form of government." He has received the highest awards of the ABA Criminal Justice Section, the National Association of Criminal Defense Lawyers, the Florida Association of Criminal Defense Lawyers (Miami), and the ACLU of Miami. In June, 2006 he will receive the Selig Goldin Award, the highest award of the Florida Bar Criminal Law Section.

Members

Mark D. Agrast

Mark Agrast is a Senior Fellow at the Center for American Progress in Washington, D.C., where he oversees programs related to the Constitution, the rule of law, and the history of American progressive thought.

Before joining the Center for American Progress, Mr. Agrast was Counsel and Legislative Director to Congressman William D. Delahunt of Massachusetts (1997-2003). He previously served as a top aide to Massachusetts Congressman Gerry E. Studds (1992-97) and practiced international law with the Washington office of Jones, Day, Reavis & Pogue (1985-91). During his years on Capitol Hill, Mr. Agrast played a prominent role in shaping laws on civil and constitutional rights, terrorism and civil liberties, criminal justice,

patent and copyright law, antitrust, and other matters within the jurisdiction of the House Committee on the Judiciary. He was also responsible for legal issues within the jurisdiction of the House International Relations Committee, including the implementation of international agreements on human rights, intercountry adoption, and the protection of intellectual property rights.

Mr. Agrast is a member of the Board of Governors of the American Bar Association and a Fellow of the American Bar Foundation. A past Chair of the ABA Section of Individual Rights and Responsibilities, he currently chairs the ABA's Commission on the Renaissance of Idealism in the Legal Profession.

Deborah Enix-Ross

Prior to joining Debevoise & Plimpton LLP in October 2002, Ms. Enix-Ross served, from January 1998 through September 2002, as a Senior Legal Officer and Head of the External Relations and Information Section of the World Intellectual Property Organization (WIPO) Arbitration and Mediation Center in Geneva, Switzerland.

Before joining WIPO, Ms. Enix-Ross was the Director of International Litigation for the Dispute Analysis and Corporate Recovery Services Group (DA&CR) of Price Waterhouse LLP, and before that, served for seven years as the American representative to the International Chamber of Commerce (ICC) International Court of Arbitration.

Ms. Enix-Ross holds a law degree from the University of Miami School of Law, a Diploma from the Parker School of Foreign and Comparative Law of Columbia University, and a Certificate from the London School of Economics. The U.S. Departments of Commerce and State appointed her as one of the original eight U.S. members of the tri lateral NAFTA Advisory Committee on Private Commercial Disputes. She is Chair-Elect of the American Bar Association (ABA) Section of International Law, a Fellow of the American Bar Foundation and a member of the ABA Center for Rule of Law Initiatives.

Stephen A. Saltzburg

Professor Saltzburg joined the faculty of the George Washington University Law School in 1990. Before that, he had taught at the University of Virginia School of Law since 1972, and was named the first incumbent of the Class of 1962 Endowed Chair there. In 1996, he founded and began directing the master's program in Litigation and Dispute Resolution at GW.

Professor Saltzburg served as Reporter for and then as a member of the Advisory Committee on the Federal Rules of Criminal Procedure and as a member of the Advisory Committee on the Federal Rules of Evidence. He has mediated a wide variety of disputes involving public agencies as well as private litigants; has served as a sole arbitrator, panel Chair, and panel member in domestic arbitrations; and has served as an arbitrator for the International Chamber of Commerce.

Professor Saltzburg's public service includes positions as Associate Independent Counsel in the Iran-Contra investigation, Deputy Assistant Attorney General in the Criminal Division of the U.S. Department of Justice, the Attorney General's ex-officio representative on the U.S. Sentencing Commission, and as director of the Tax Refund Fraud Task Force, appointed by the Secretary of the Treasury. He currently serves on the Council of the

ABA Criminal Justice Section and as its Vice Chair for Planning. He was appointed to the ABA Task Force on Terrorism and the Law and to the Task Force on Gatekeeper Regulation and the Profession in 2001 and to the ABA Task Force on Treatment of Enemy Combatants in 2002.

Hon. William S. Sessions

William S. Sessions has had a distinguished career in public service, as Chief of the Government Operations Section of the Department of Justice, United States Attorney for the Western District of Texas, United States District Judge for the Western District of Texas, Chief Judge of that court, and as the Director of the Federal Bureau of Investigation. He received the 2002 Price Daniel Distinguished Public Service Award and has been honored by Baylor University Law School as the 1988 Lawyer of the Year.

Judge Sessions joined Holland & Knight LLP in 2000 and is a partner engaged primarily in Alternative Dispute Resolution procedures. He holds the highest rating assigned by Martindale-Hubbell and is listed in The Best Lawyers In America for 2005 & 2006 for Alternative Dispute Resolution. He serves as an arbitrator and mediator for the American Arbitration Association, the International Center for Dispute Resolution and for the CPR Institute of Dispute Resolution.

Since June 2002, Judge Sessions has served on The Governor's Anti-Crime Commission and as the Vice Chair of the Governor's Task Force on Homeland Security for the State of Texas. He is a past President of the Waco-McLennan County Bar Association, the Federal Bar Association of San Antonio, the District Judges Association of the Fifth Circuit, and he was a member of the Board of Directors of the Federal Judicial Center. He served as the initial Chair of the ABA Committee on Independence of the Judiciary, honorary co-Chair of the ABA Commission on the 21st Century Judiciary, and as a member of the ABA Commission on Civic Education and the Separation of Powers. He was a member of the Martin Luther King, Jr. Federal Holiday Commission and he serves on the George W. Bush Presidential Library Steering Committee for Baylor University.

James R. Silkenat

Jim Silkenat is a partner in the New York office of Arent Fox and coordinates the firm's International Business Practice Group. His primary focus is on international joint ventures, mergers and acquisitions, privatizations, project finance transactions (in developed and developing countries) and private equity investment funds. He is a former Legal Counsel of the World Bank's International Finance Corporation.

An active member of the American Bar Association, Mr. Silkenat has served as Chair of both the Section of International Law and the Section Officers Conference. In 1990 he was elected to the ABA House of Delegates and has served as Chair of the New York Delegation in the House of Delegates since 2000. He served on the ABA Board of Governors from 1994-1997 and has chaired the ABA's Latin American Legal Initiatives Council.

Mr. Silkenat is also a former Chair of the Fellows of the American Bar Foundation, of the A.B.A.'s Museum of Law and of the A.B.A.'s China Law Committee. He is also a member of the House of Delegates of the New York State Bar Association and Chair of the Council on International Affairs of the Association of the Bar of the City of New York. Jim is a former Adjunct Professor of Law at Georgetown University Law Center and

Chair of the Lawyers Committee for International Human Rights (now, Human Rights First).

Suzanne Spaulding

Suzanne Spaulding is a Managing Director at The Harbour Group, LLC. Ms. Spaulding is an expert on national security related issues, including terrorism, homeland security, critical infrastructure protection, cyber security, intelligence, law enforcement, crisis management, and issues related to the threat from chemical, biological, nuclear, or radiological weapons. She works with clients to develop and implement legislative strategies around these and other issues.

Prior to joining The Harbour Group, Ms. Spaulding was Minority Staff Director for the U.S. House of Representatives Permanent Select Committee on Intelligence. Her previous legislative experience includes serving as Deputy Staff Director and General Counsel for the Senate Select Committee on Intelligence and as Legislative Director and Senior Counsel for Senator Arlen Specter (R-PA). She has also worked for Representative Jane Harman (D-CA) and served as Assistant General Counsel for the CIA..

Ms. Spaulding received her undergraduate and law degrees from the University of Virginia. She is the immediate past Chair and current Advisory Board member of the American Bar Association's Standing Committee on Law and National Security. In addition, Ms. Spaulding is a member of the ABA President's Task Force on Enemy Combatants and of the Gavel Award Screening Committee.

Special Advisers

Harold Hongju Koh

Harold Hongju Koh, Dean and Gerard C. and Bernice Latrobe Smith Professor of International Law, is one of the country's leading experts on international law, international human rights, national security law and international economic law. He has received more than twenty awards for his human rights work.

A former Assistant Secretary of State, Dean Koh advised former Secretary Albright on U.S. policy on democracy, human rights, labor, the rule of law, and religious freedom. Harold clerked for both Judge Malcolm Richard Wilkey of the U.S. Court of Appeals for the D.C. Circuit and Justice Harry A. Blackmun of the United States Supreme Court. He worked in private practice in Washington, D.C. and as an attorney at the Office of Legal Counsel at the U.S. Department of Justice.

Dean Koh earned a B.A. from Harvard University in 1975, an Honours B.A. from Magdalen College, Oxford University in 1977, and a J.D. from Harvard Law School in 1980. He has been a Visiting Fellow and Lecturer at Magdalen and All Souls Colleges, Oxford University, and has taught at The Hague Academy of International Law, the University of Toronto, and the George Washington University National Law Center.

Elizabeth Rindskopf Parker

Dean Rindskopf Parker joined Pacific McGeorge as its eighth dean in 2003 from her position as General Counsel for the 26-campus University of Wisconsin System. Her fields of expertise, in addition to the law of national security and terrorism, include international relations, public policy and trade, technology development

and transfer, commerce, and litigation in the areas of civil rights and liberties.

Dean Rindskopf Parker's expertise in national security and terrorism comes from 11 years of federal service, first as General Counsel of the National Security Agency (1984-1989), then as Principal Deputy Legal Adviser at the U.S. Department of State (1989-1990), and as General Counsel for the Central Intelligence Agency (1990-1995). From 1979 to 1981, Dean Rindskopf Parker served as Acting Assistant Director for Mergers and Acquisitions at the Federal Trade Commission.

A member of the American Bar Foundation and the Council on Foreign Relations, and former Chair of the ABA Standing Committee on Law and National Security, Dean Parker is a frequent speaker and lecturer and has taught national security law at Case Western Reserve Law School, Cleveland State School of Law and Pacific McGeorge. Currently, she serves on several committees of the National Academy of Sciences, including the Roundtable on Scientific Communication and National Security, and the Commission on Scientific Communication and National Security, examining responses to terrorism.

Liaison to the Task Force

Alan Rothstein

Alan Rothstein serves as General Counsel to the Association of the Bar of the City of New York, where he coordinate the extensive law reform and public policy work of this 22,000-member Association. Founded in 1870, the Association has been influential on a local, state, national and international level.

Prior to his 20 years with the Association, Rothstein was the Associate Director of Citizens Union, a long-standing civic association in New York City. Rothstein started his legal career with the firm of Weil, Gotshal & Manges. He earned his B.A. degree from City College of New York and an M.A. in Economics from Brown University before earning his J.D. from NYU in 1978. Prior to his legal career, Rothstein worked as an economist in the environmental consulting field and for the New York City Economic Development Administration.

Mr. Rothstein serves on the boards of directors of Volunteers of Legal Service and Citizens Union, where he chairs its Committee on State Affairs. He also serves on the New York State Bar Association House of Delegates.

LETTER FROM JOHN W. WHITEHEAD, FOUNDER AND PRESIDENT, THE RUTHERFORD INSTITUTE, DATED SEPTEMBER 7, 2007, TO CHAIRMAN JOHN CONYERS, JR.

THE RUTHERFORD INSTITUTE

JOHN W. WHITEHEAD
Founder and President

INTERNATIONAL HEADQUARTERS
Post Office Box 7482
Charlottesville, VA 22906-7482
U.S.A.
Telephone 434 • 978 • 3888
Facsimile 434 • 978 • 1789
E-Mail • staff@rutherford.org
Internet • www.rutherford.org

INTERNATIONAL OFFICE
CENTRAL AND EASTERN EUROPE
Budapest, Hungary

September 7, 2007

The Honorable John Conyers, Jr.
Chairman
Committee on the Judiciary
United States House of Representatives
2138 Rayburn House Office Building
Washington, D.C. 20515

Dear Mr. Chairman:

I am writing in my capacity as president of The Rutherford Institute to explain our concerns about the Protect America Act, which was recently enacted by Congress. The Rutherford Institute is a civil liberties and human rights organization dedicated to preserving the integrity of the United States Constitution and the freedoms guaranteed in the Bill of Rights.

Since the 9/11 terrorist attacks on the nation, Americans have been repeatedly subjected to their liberties being sacrificed on the supposed altar of national security. Indeed, in recent years, there has been a steady erosion of the protections afforded American citizens, especially in regard to their privacy rights.

Recently, President Bush insisted that the Foreign Intelligence Surveillance Act of 1978 (FISA), which limits the government's domestic surveillance capabilities, is out of sync with modern telecommunications technology and does not grant intelligence officials enough flexibility to prevent another attack on our country. Therefore, he asserted, it is necessary "to close intelligence gaps."[1] However, the president's proposed solution—the "Protect America Act of 2007" (PAA), which was passed by Congress in August 2007—represents a blatant broadside attack against one of the most cherished liberties guaranteed in the Bill of Rights: the right to be free from unnecessary government intrusions.

[1] http://www.whitehouse.gov/news/releases/2007/08/20070803-9.html

Under PAA, the government is no longer compelled to seek warrants prior to eavesdropping on American citizens' telephone calls and e-mails. Indeed, PAA authorizes the government to wiretap or intercept *any* international communication without a warrant, even if one of the parties is an American citizen on American soil. The only essential requirements under the law are that the intercept be undertaken for acquisition of "foreign intelligence information" and be "directed at a person reasonably believed to be located outside of the United States."

PAA undermines the protections guaranteed by the Fourth Amendment, which states: "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."

PAA Does Away with Warrants Based on Probable Cause

As University of Chicago law professor Geoffrey R. Stone has observed, under PAA "[t]here is no requirement that the government must have probable cause to believe that the person 'reasonably believed to be outside of the United States' is a terrorist or even an associate of terrorists."[2]

By merely requiring the intercept be "directed at a person reasonably believed to be located outside of the United States," Congress has given the Bush Administration a dragnet in which to eavesdrop on a myriad of phone calls and e-mails by potentially innocent Americans with no connection to terrorism. Clearly, this drastically undermines the Fourth Amendment's requirement that individual warrants be issued, based on probable cause and detailing the particulars of the place to be searched and places and persons to be seized.

PAA Is an Open-Ended Invitation to Eavesdrop

PAA represents a remarkable departure from the requirements set forth in FISA. Its broad language, which impacts even those "reasonably believed" to be outside the country, provides the Bush Administration with significant latitude.

As Aziz Huq[3] explains, "Under this language, the NSA could decide to 'direct' its surveillance at Peshawar, Pakistan—and seize all U.S. calls to and from there. It could focus on Amman, or Cairo, or London, or Paris, or Toronto.... Simply put, the law is an

[2] Geoffrey R. Stone, *The Huffington Post*, "The New FISA," August 7, 2007. Access at http://www.huffingtonpost.com/geoffrey-r-stone/the-new-fisa_b_59383.html
[3] Deputy Director of the Brennan Center for Justice at NYU School of Law.

open-ended invitation to collect Americans' international calls and emails."[4] Under this standard, even a private phone call between spouses while one of them is on vacation in Cancun, Mexico, could get swept up in the government's eavesdropping program.

PAA Provides Meaningless Judicial Review and Congressional Oversight

PAA requires the Director of National Intelligence and the Attorney General to *certify year-long programs* for collecting international calls to the secret FISA court in lieu of issuing individualized warrants. Worse, the secret court can only invalidate the government's surveillance procedures that are "clearly erroneous." As professor Huq has noted, "The government thus has to meet an extraordinarily low standard, in a one-sided judicial procedure in which the court has no access to details of the program's actual operation."[5]

However, this administration's lack of candor and transparency, coupled with reports that the president violated FISA from 2001 to 2006, do not engender confidence that the Bush Administration would operate its surveillance programs within constitutional parameters.[6]

Furthermore, the program established under PAA provides little, if any, congressional oversight. Under the statute, the Attorney General is not compelled to report to Congress on the program's details. Instead, it merely requires the Attorney General to report "incidents of noncompliance." In other words, it places the preservation of Americans' Fourth Amendment rights comprehensively in the hands and trust of an executive branch that has been less than truthful with the American people and Congress.

PAA Is a Frontal Assault on the First Amendment

At the height of the Army surveillance investigations of the 1970s, Senator Sam Ervin (D-N.C.) observed, "When people fear surveillance, whether it exists or not, when they grow afraid to speak their minds and hearts freely to their government or to anyone else, then we shall cease to be a free society."[7] Indeed, this principle is the bedrock of all free societies.

---

[4] Aziz Huq, *The Nation*, "Data-Mining Our Liberties," August 7, 2007. Access at http://www.thenation.com/doc/20070813/huq2
[5] *Id.*
[6] Rehnquist, U.S. Congress, Senate, Committee on the Judiciary, Hearings Before the Subcommittee on Constitutional Rights, 92nd Cong., 1st Sess., 1971.
[7] Ervin, U.S. Congress, Senate, Committee on the Judiciary, Hearings Before the Subcommittee on Constitutional Rights, 92nd Cong., 1st Sess., 1971.

As the 1967 President's Commission on Law Enforcement and Administration of Justice declared, "In a democratic society privacy of communication is essential if citizens are to think and act creatively and constructively. Fear or suspicion that one's speech is being monitored by a stranger, even without the reality of such activity, can have a seriously inhibiting effect upon the willingness to voice critical and constructive ideas."[8]

Such concerns are especially relevant today, given the suspect manner in which government officials censor unpopular or nonconforming speech. For instance, an August 16, 2007 report by the *Associated Press* detailed how official government manuals direct the removal of persons expressing anti-Bush messages on their clothing at political rallies attended by the president. The report states, "The ACLU said in a statement that a presidential advance manual makes it clear that the government tries to exclude dissenters from the president's appearances. 'As a last resort,' the manual says, 'security should remove the demonstrators from the event.'"[9]

This is merely a single instance among many. Simply put, the widespread government surveillance authorized under PAA will "chill" the very speech that is protected by the First Amendment—peaceful political speech directed at or about the government.

A Slippery Slope

Attempts by the Executive Branch to do an end run around the Fourth Amendment by utilizing emerging technologies in order to spy on American citizens have increased dramatically over the past half century. During this time, the United States government has engaged in vast, widespread wiretaps and other surveillance measures without a hint of oversight demanded by the Fourth Amendment. The pattern has been remarkably disturbing.

In January 1970, for example, Christopher H. Pyle reported in *Washington Monthly* that "For the past four years, the U.S. Army has been closely watching civilian political activity within the United States."[10] "Today," Pyle detailed, "the Army maintains files on the membership, ideology, programs, and practices of virtually every activist political group in the country." Subsequent Congressional hearings revealed that

---

[8] President's Commission on Law Enforcement and Administration of Justice, The Challenge of Crime in a Free Society 202 (1967).
[9] "Feds pay $80,000 over anti-Bush T-shirts," *Associated Press*, August 16, 2007. Access at http://news.yahoo.com/s/ap/20070817/ap_on_re_us/bush_protesters_lawsuit_2&printer=1.
[10] Christopher H. Pyle, "CONUS Intelligence: The Army Watches Civilian Politics," *Washington Monthly*, January 1970.

the Army surveillance program generally targeted political activists and elected officials who had opposed the Vietnam War.

In 1975, the Church Committee Congressional hearings, headed by Senator Frank Church (D-Idaho), exposed a broader government spy operation aimed at American citizens. It was revealed that the National Security Agency (NSA) had been engaged in a secret operation in which the agency tapped into the international and domestic communication traffic of some of the country's largest communication companies of the day. Indeed, it is estimated that approximately 150,000 private conversations by Americans *per month* were analyzed by the NSA and then sent off to the FBI and CIA.[11]

The Foreign Intelligence Surveillance Act of 1978 was designed to protect the privacy rights of American citizens as guaranteed under the Fourth Amendment, while also providing the president with the ability to covertly collect information on foreign enemies. FISA established a special "secret" court responsible for reviewing the legality of these covert government spy programs and to issue secret warrants. The government was required to obtain a warrant based upon probable cause that the target of its surveillance operation is a foreign power, an agent of a foreign power or, as later amended, a "lone-wolf" terrorist. However, instead of being forced to provide specific facts to a magistrate who was a known member of the public-at-large, FISA merely required government agents to apply for a warrant to a secret judge in a secret court.

The USA Patriot Act, passed in 2001, granted the government even more expansive powers than FISA to investigate and prosecute persons believed to be involved in terrorist activities. For example, the Patriot Act extinguished the FISA standard requiring the government to demonstrate that the collection of foreign intelligence information was the "primary purpose" of its surveillance. Moreover, the Patriot Act permitted the government to engage in so-called "roving wiretaps," which afforded the government virtually unfettered access to potentially millions of private telephone calls and e-mails of American citizens.

Now, with its recent passage of the "Protect America Act of 2007," Congress has moved us further down the slippery slope toward a complete erosion of our rights by authorizing the government to claim unprecedented powers to conduct warrantless surveillance of Americans.

Thus, if we are to have any hope of preserving our right to be free from unreasonable searches and seizures, Congress must allow this legislation to sunset.

---

[11] http://www.pbs.org/wgbh/pages/frontline/homefront/preemption/churchfisa.html

If we can be of further assistance, feel free to contact us.

With best regards, I remain,

Sincerely yours,

John W. Whitehead

JWW:vc

PREPARED STATEMENT OF CAROLINE FREDERICKSON, DIRECTOR, WASHINGTON LEGISLATIVE OFFICE, AMERICAN CIVIL LIBERTIES UNION (ACLU)

WASHINGTON
LEGISLATIVE OFFICE

Testimony of Caroline Fredrickson
Director, Washington Legislative Office

American Civil Liberties Union

AMERICAN CIVIL
LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

Caroline Fredrickson
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

OFFICERS AND DIRECTORS
NADINE STROSSEN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

RICHARD ZACKS
TREASURER

Protect Privacy by Overhauling the Protect America Act

U.S. House of Representatives Committee on the Judiciary

Hearing Regarding Warrantless Surveillance and the Foreign Intelligence Surveillance Act (FISA): The Role of Checks and Balances in Protecting Americans' Privacy Rights

September 5, 2007
2141 Rayburn House Office Building

Chairman Conyers, Ranking Member Smith, and Committee Members, on behalf of the American Civil Liberties Union ("ACLU"), America's oldest and largest civil liberties organization, its 53 affiliates and hundreds of thousands of Members, we write to share our views with the Committee regarding the recently enacted Protect America Act, Pub. L. 110-55, and legislation to replace that Act. Because § 6 of the Protect America Act causes the Act to sunset if not reauthorized or replaced within six months, the ACLU recommends that this Committee allow the Act to expire. Alternatively, should Congress feel compelled to legislate, Congress should replace the Act with a full scale revision that respects the letter and spirit of the Fourth Amendment with regards to intercepting U.S. persons' communications.

Congress must also vigorously resist legislative attempts to grant retroactive immunity to government employees and telecommunications companies and their employees for facilitating criminal and unconstitutional wiretapping. Absolving these individuals and companies of their violations of the Foreign Intelligence Surveillance Act's ("FISA") will encourage future lawlessness and interception of communications outside of FISA. Ultimately, extinguishing liability – especially while litigation is proceeding – will prevent U.S. citizens from vindicating their constitutional, legal and contractual rights as customers of the telecommunications companies.

Neither the Protect America Act, nor S. 2011, authored by Sen. Carl Levin (D-MI) and Intelligence Committee Chair, Sen. John D. Rockefeller, sufficiently protect the privacy of communications of innocent U.S. persons. Any legislation replacing the Protect America Act must reintroduce privacy protections into FISA's treatment of communications intercepted between U.S. persons and persons reasonably believed to be outside of the United States.

In passing the Protect America Act, Congress legislated in the dark and should not do so again. Despite repeated requests for documents, testimony and briefings regarding the illegal, warrantless wiretapping conducted at the President's bequest, Congress has to date been utterly stymied in conducting meaningful oversight over those illegal acts. The White House has flouted Congressional subpoenas and deadlines for the provision of documents related to that warrantless wiretapping. The end result is that Congress has effectively been prevented from conducting oversight regarding surveillance conducted on U.S. soil since September 12, 2001. In essence, Congress has been all but eliminated as an independent check on abuses by the President and the National Security Agency ("NSA"). No amendments to FISA should be made permanent until Congress and the public receive answers about what surveillance activities have been conducted over the last six years and the legal basis for those programs. This Committee should hold extensive public hearings regarding the NSA's warrantless wiretapping and the telecommunications companies' facilitation of that illegal wiretapping. Information regarding this illegal activity to determine how the Administration ignored the clear mandates of FISA should be forthcoming <u>prior</u> to the enactment of any new legislation. After all, any Congressional effort to carefully draw the statutory lines between permissible surveillance to prevent acts of terrorism is meaningless should this, or a future, Administration choose to ignore or circumvent FISA's mandates and limitations.

Further, information regarding how the authorities provided for in the Protect America Act are being interpreted and operationalized by the NSA should be shared with Congress. To facilitate Congress' legislative efforts, the NSA should be required to articulate with specificity the problematic aspects of the prior statutory scheme and whether the Protect America Act responds to those intelligence concerns.

The ACLU also recommends that Congress codify a FISA regime that increases the privacy protections for U.S. persons' communications as the level of intrusiveness of intercepts of those communications increases. If content is acquired and/or reviewed, particularly where probable cause has not been developed to investigate a U.S. persons' communications, the government's burden of protecting that communication should be increased, and commensurate limitations should be placed on the use or dissemination of that communication to ensure compliance with the Fourth Amendment. Additionally, meaningful judicial review of the NSA must be built into any legislation so that the court may act to ensure the privacy of U.S. persons' communications. Only the Foreign Intelligence Surveillance Court ("FISC") can insist that surveillance is targeted to individualized intercepts. Court review is also essential so as to force the NSA and Department of Justice to comply with the letter and spirit of any new law enacted.

II. Analysis of the Protect America Act and S. 2011

President Bush enacted sweeping revisions to FISA on August 5, 2007 by signing into law the Protect America Act. The Act was signed just two days after final passage by the U.S. Senate and one day after final passage by the U.S. House of Representatives. Director of National Intelligence McConnell allegedly lobbied heavily and personally for the Act's passage, briefing more than 200 Members of Congress on the NSA's purported need to close an intelligence gap. This rush to legislate led to a substantially overbroad law that does not appear to provide the type of narrowly-targeted expansion of surveillance authority McConnell claims to have sought. Rather, the Act appears to have eroded Americans' privacy protections for their e-mails and phone calls to and from foreign-based persons – including U.S. citizens living, working or traveling abroad – in a tidal wave of over-reaching legislative language. The ACLU calls upon Congress to reverse this sea change in the laws governing surveillance by the U.S. government of U.S. citizens and lawful permanent residents.

The Protect America Act turns the Fourth Amendment to the U.S. Constitution on its head.[1] It eviscerates privacy protections for U.S. persons' communications and does great damage to the Fourth Amendment's protections by:

(i) expressly permitting non-targeted, warrantless mass acquisition of U.S. persons' communications with foreign-based communicants by defining such communications as outside of the definition of FISA-protected "electronic surveillance";

(ii) failing to require the NSA to demonstrate that they have probable cause to believe one party to the communication is a terrorist or foreign power before intercepting U.S. persons' communications;

(iii) eliminating requirements that factual predicates for surveillance be listed with specificity such as the "facilities, places, premises, or property at which the acquisition of foreign intelligence information will be directed;" and

(iv) implicitly permitting the limitless warehousing and subsequent data mining of both the metadata regarding those communications and the content of the communications themselves.

First, the Act states that all intercepts of communications – both e-mail and phone calls – between any person the government "reasonably believe[s]" is located outside the U.S. and anyone within the U.S. are exempt from the definition of Fourth Amendment-protected electronic surveillance. Protect America Act, Pub. L. 110-55 at § 105B(a). Thus, for the first time, FISA: (i) permits the mass acquisition of U.S. persons' communications, (ii) eliminates any requirement that the government target its acquisition to acquire only certain persons' conversations; and (iii) eliminates the requirement that a judge approve those interceptions. Now, if the government is directing its surveillance at foreign-based communicants it may sweep up the conversations of U.S.-based persons. FISA previously required the government to establish reasonable suspicion or probable cause to obtain, keep and utilize the communications of U.S. persons that were inadvertently acquired. Second, the Protect America Act eliminates any requirement that the NSA, in obtaining a general warrant, provide facts to target the interceptions to specific facilities, places, premises or property. Id. at § 105B(b). In short, the FISC no longer plays a meaningful role – one that it had played effectively since 1978 – and it can no longer provide judicial oversight given the powers granted to the NSA in the Protect America Act. This amendment to FISA essentially establishes a system of surveillance solely dictated and controlled by Executive Branch fiat without the independent review by the judicial branch. Further, the Act essentially eliminates judicial review of DOJ and NSA activities by the FISC. The end result is a cosmetic patina of judicial review without providing the FISC with substantive authority to halt or modify improper intercepts. Finally, the Protect America Act permits continued warrantless surveillance of a person, account or facility – even when it becomes clear that the subject of surveillance will have repeated contact with a U.S. person.

All of these constitutional and policy failings are only exacerbated by the fact that the Protect America Act allows the government to retain, use and disseminate the content of or the data about these communications however it sees fit. While supporters of the Protect America Act point to so-called "minimization procedures," those procedures have never been used on mass, otherwise legalized collection, nor have those procedures ever had a public airing. In effect, the Protect America Act resorts back to "trust us," and leaves the Administration to its own devices to operate in secret and without any

limitation on how to treat U.S. information. Thus, the NSA is now permitted to intercept and utilize communications without minimizing the U.S. persons' identity and personally identifiable information. Prior to the Protect American Act, personally identifiable information and "header" information identifying a particular U.S. person would have been minimized.

The Act, therefore, erects a geometric increase in the kind and quantum of U.S. persons' communications that may be intercepted. It is no exaggeration to state that all communications – both e-mails and phone calls – originating from a non-U.S.-based person could be intercepted. Similarly, the communications to people abroad originating from the U.S. also are likely to be intercepted as part of the communications chain. In short, it is likely that all, or substantially all, communications entering or exiting the U.S. will be intercepted. The implications of such a change are profound, likely leading to the acquisition of all communications in the following illustrative scenarios:

(i) communications to U.S.-based businesses from their foreign-based subsidiaries or business partners/clients;

(ii) calls and e-mails to U.S.-based parents of high-school, college, and university students participating in "study abroad" programs;

(iii) calls and e-mails between missionaries and their religious sponsor churches, mosques and synagogues in the U.S.;

(iv) e-mails and calls from any U.S. citizen travelling outside of the U.S. on vacation; and

(v) purely domestic calls and e-mails between U.S. persons that are routed through foreign countries, such as Canada, simply for ease, cost-savings, or network efficiency.

Now, the mass interception of foreign-to-U.S. communications is permissible due to the evisceration of Fourth Amendment-based statutory requirements that mandated the targeting of, interception and judicial approval of individualized surveillance.

The Protect America Act also implicitly authorizes mass warehousing and limitless data mining of the communications of U.S. persons intercepted. The Act states that the government may engage in "acquisition [of] foreign intelligence information" from a "custodian" either as the communications are "transmitted or while they are stored . . . ." Id. at § 105B(a)(3). In essence, the Act facilitates the application by the NSA for a general warrant for a group of individuals and their communications, no matter whether a U.S. person's communications are swept up. Because Congress failed to limit the types of data mining that may occur, or prevent data mining of the metadata concerning the communications, we can expect the application of link analysis data mining to attempt to establish the relationship between a foreign-based communicant and the U.S. person with whom they communicate, even if the contact is casual, incidental or accidental. Thus, an

innocent U.S. person whose communications are intercepted because they received a phone call or e-mail from a person reasonably believed to be located overseas could come under government suspicion simply because they were sent an e-mail or received a phone call.

The failure of Congress to limit the data mining of either the metadata concerning the communications or the content of those communications is likely to have profound legal and practical consequences for innocent U.S. persons. The Act does not limit the NSA's ability to interpret the communications intercepted, thus innocent U.S. persons' communications could be misinterpreted because the data mining of the content of those communications detects the presence of some code word. The implications for innocent U.S. persons wrongly drawn into this web of government suspicion are heretofore unknown. Certain questions naturally arise from this lack of legal limitation:

(i) will innocent U.S. persons' exercise of legally or constitutionally guaranteed rights and privileges be limited?;

(ii) what redress, if any, will innocent U.S. persons have when their communications are misinterpreted?;

(iii) how will an innocent person who is wrongly suspected recover his or her good name and reputation?; and

(iv) will the friends, families and associates of the wrongly suspected U.S. persons also come under suspicion? If so, are there any limits to the concentric rings of communicants (i.e., how many degrees of separation removed from the foreign-based communicant) the government will draw into this burgeoning web of suspicion?

The Protect America Act's revisions of FISA also render the longstanding law unrecognizable by virtually eliminating the role of telecommunications providers as independent guarantors of their customers' privacy under this new mass communications acquisition scheme. The Act substantially eliminates the ability of the telecoms to resist facilitating the interception of U.S. persons' communications. As originally drafted, FISA placed the telecoms in the shoes of their customers and permitted the telecoms to go to court to resist an allegedly improper FISA intercept application on a customer's behalf. The Protect America Act eviscerates this third-party guarantor role. It permits the NSA to demand that telecoms facilitate interception. Id. at § 105B(e). Should a telecom resist such a directive, the NSA may obtain a court order compelling facilitation. Id. at § 105B(g). Failure to comply with that court order is punishable with a finding of contempt of court. Id. Although the Act sets forth procedures for a telecom to challenge a directive, the streamlining of the FISA application – such as the elimination of the requirement that the NSA provide specific targeting facts – prevents attorneys for any telecom from having certain pre-existing avenues to challenge the legal sufficiency of a mass acquisition directive. Further, the FISC must review any ex parte, sealed

submissions regarding the interception, which lessens the likelihood that a telecom could successfully resist such an interception directive. Id. at § 105B(k).

In addition, to reduce the telecom industry's resistance to facilitating mass communications interception, the Protect America Act provides significant financial inducement to the telecoms. Pursuant to the Act, the telecoms are compensated "at the prevailing rate" for "providing information, facilities, or assistance" to aid the government's wiretapping. Id. at § 105B(f). Thus, the Act guarantees that wiretapping facilitation remains profitable for the telecoms. More importantly, to further erode telecom resistance to this massive wiretapping expansion, the Act grants the telecoms seeming absolute prospective immunity for wiretapping of e-mails and phone calls pursuant to the Act. Id. at § 105B(l).

The reporting requirements of the Act do not guarantee that Congress, much less the media or the public, will have sufficient information about wiretapping permitted under the Act to judge its efficacy or the NSA's compliance with the Act. The Attorney General of the U.S. is only required to brief the four lead Congressional Committees – the House and Senate Intelligence and Judiciary Committees – semiannually. That report need only provide a "description . . . of incidents of non-compliance by an element of the Intelligence Community with guidelines or procedures established for determining that the acquisition of foreign intelligence [pursuant to the Act] concerns persons reasonably believed to be outside the United States." Further, the report only must list the number of certifications issued by the Attorney General and the number of directives to telecoms to facilitate interceptions during the relevant period. In short, Congress' failure to require additional information or reporting specificity prevents the provision of information to judge:

(i) whether the Act's expansion was justified or useful from an intelligence resource perspective;

(ii) whether violations of U.S. persons' constitutional or legal rights occurred;

(iii) whether the interceptions ordered are targeted in any way to comport with the Fourth Amendment's requirements; and

(iv) whether and/or what disciplinary action was taken for any violations of any procedural, regulatory, legal or constitutional violations by any NSA or Department of Justice employee.

The Protect America Act also includes a six month-long "sunset" provision, which causes the Act to expire if it is not replaced within six months after the date of enactment (i.e., after February 5, 2007).

The Democrats' alternative legislative proposal, S. 2011 (the short title of S. 2011 was also the Protect America Act, therefore, hereinafter "Democrats' alternative" or "S. 2011"), introduced by senior Intelligence Committee Member Senator Carl Levin (D-MI)

and Committee Chair John D. Rockefeller (D-WV), failed ACLU standards in several important respects. First, the Democrats' alternative eliminated targeting requirements in language identical to the Protect America Act. S. 2011 at § 105(B)(b)(2). This allows for the mass acquisition of communications involving at least one U.S. person. Further, the legislation authorized year-long interceptions. Id. at § 105B(a). Additionally, the Democrats' alternative would have created a "listen-first-apply-for-a-warrant-later" procedure authorizing immediate interception of U.S. persons' communications with persons reasonably believed to be outside the U.S. Id. at § 105C. Finally, the alternative left the Executive Branch to minimize U.S. persons' communications through secret Attorney General-issued procedures, and did not require that improperly intercepted U.S. persons' communications be destroyed. This amendment would have permitted surveillance without any indicia of Fourth Amendment protection in that U.S. persons' communications could be intercepted and reviewed in the absence of any targeting of the foreign-based communicant and without probable cause or reasonable suspicion to have been developed with respect to the U.S. person.

The Democrats' alternative was superior to the Protect America Act in two respects, neither of which outweighed the alternative's implications for vastly expanded acquisition of U.S. persons' communications with foreign-based persons. First, S. 2011 would have required court review of the Attorney General's certification and application for surveillance. Id. at § 105B. In contrast, the Protect America Act requires only certification by the Attorney General. Second, S. 2011 would have required the NSA to obtain a warrant from the FISC to continue interception at the point at which the U.S. person became the subject of surveillance. Id. at § 105B(d). The ACLU supports both of these improvements.

III. Recommended Principles for Reforming the Protect America Act

The ACLU notes again that Congress is not compelled to pass additional legislation. The effect of not doing so would be to return FISA to the statutory limitations in place prior to enactment of the Protect America Act. The ACLU believes that no legislation would be better than the permanent authorization of the Protect America Act or any legislation that substantially mirrors that Act. Further, any grant of retroactive telecom immunity will reward law-breaking and fundamentally undermine the FISA structure by eliminating any arm's length distance between the telecoms and the government. In short, should the telecoms be given amnesty for violating the law, AT&T, Verizon and other companies will essentially be functioning as quasi-governmental appendages of the NSA.

In the alternative, should Congress feel compelled to legislate, the ACLU recommends that this Committee adhere to the following principles in drafting legislation to replace the Protect America Act:

1. **Any further legislation must reiterate that FISA is the exclusive means of intelligence gathering on U.S. soil, and the legislation must include automatically**

triggered consequences for violating this exclusivity. As initially enacted by Congress, the exclusivity of FISA was unambiguous. This new exercise in defining the lawful extent of surveillance authorities will be useless if the resulting legislation can be ignored. We further recommend that any new legislation state explicitly that the Authorization for the Use of Military Force in Afghanistan and Iraq do not authorize any surveillance outside FISA. Additionally, we recommend that the NSA be required to report to Congress repeatedly on its implementation of any new surveillance activities conducted pursuant to FISA.

2. **Interceptions of U.S. persons' communications within the U.S. should continue to be included within, and, therefore, protected by the definition of "electronic surveillance."** The Protect America Act's seeming elimination of this protection should be repealed.

3. **Collection and isolation of the particular communications sought by the government should be conducted by the telecommunications industry itself – the government should not be given direct and unfettered access to telecommunications infrastructure.** We are concerned that the Protect America Act appears to allow the government to "sit on the line" and scoop up all communications and sort through them later. Instead, the government should receive only the information it is authorized to intercept by law.

4. **The FISC must play a meaningful role in ensuring compliance with the law. First and foremost, electronic surveillance should be authorized by the FISC through the issuance of an individualized warrant based on probable cause.** This oversight should include, where possible, prior and, always, regular judicial approval and review of surveillance based on full disclosure about what information is to be sought, whose communications will be collected, how it will be gathered and how content and other data in communications to and from the United States will be handled. The Court must also have regular access to information about how many U.S. communications are being collected and the authority to require court orders when it becomes clear that a certain program or surveillance of a target is scooping up communications of U.S. persons.

5. **Under any new amendment to FISA established in your legislation, when the government intercepts a communication to which a person in the U.S. is a party, there should be a presumption requiring the NSA to immediately destroy that communication unless the NSA documents that it has reason to believe that the communication reflects an immediate threat to life or limb.** All public FISA legislation has been deficient in that it has lacked a presumption of destruction of the improperly intercepted communications of U.S. persons. Without such a presumption, the Administration's secret "minimization" procedures will be all that govern U.S. communications. Congress has the authority – and the responsibility – to explicitly define how these communications are treated, and should no longer defer to the Executive branch's unknown policies. If the programs are truly directed at people overseas, this should be noncontroversial.

6. **Once the government has reason to believe that there is a substantial likelihood that a specific account, person or facility will have contact with someone in the United States, the government should be required to return to the FISC to obtain a court order for continued surveillance of that account, person or facility.** Reliance on the FISC will help ensure the privacy of U.S. persons' communications.

For further information, please contact:
Timothy D. Sparapani
Senior Legislative Counsel
(202) 715-0839

Michelle Richardson
Legislative Consultant
(202)715-0825

---

[i] The Fourth Amendment to the Constitution provides in pertinent part that "no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be search, and the persons or things to be seized."

○