AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

LEGISLATIVE PROPOSALS TO UPDATE THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

SEPTEMBER 6, 2006

Serial No. 109–136

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

29–746 PDF WASHINGTON : 2006

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) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*

HENRY J. HYDE, Illinois
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
WILLIAM L. JENKINS, Tennessee
CHRIS CANNON, Utah
SPENCER BACHUS, Alabama
BOB INGLIS, South Carolina
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
RIC KELLER, Florida
DARRELL ISSA, California
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
LINDA T. SÁNCHEZ, California
CHRIS VAN HOLLEN, Maryland
DEBBIE WASSERMAN SCHULTZ, Florida

PHILIP G. KIKO, *General Counsel-Chief of Staff*
PERRY H. APELBAUM, *Minority Chief Counsel*

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

HOWARD COBLE, North Carolina, *Chairman*

DANIEL E. LUNGREN, California
MARK GREEN, Wisconsin
TOM FEENEY, Florida
STEVE CHABOT, Ohio
RIC KELLER, Florida
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
LOUIE GOHMERT, Texas

ROBERT C. SCOTT, Virginia
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ANTHONY D. WEINER, New York

MICHAEL VOLKOV, *Chief Counsel*
DAVID BRINK, *Counsel*
CAROLINE LYNCH, *Counsel*
JASON CERVENAK, *Full Committee Counsel*
BOBBY VASSAR, *Minority Counsel*

CONTENTS

SEPTEMBER 6, 2006

OPENING STATEMENT

Page

The Honorable Howard Coble, a Representative in Congress from the State of North Carolina, and Chairman, Subcommittee on Crime, Terrorism, and Homeland Security 1

The Honorable Robert C. Scott, a Representative in Congress from the State of Virginia, and Ranking Member, Subcommittee on Crime, Terrorism, and Homeland Security 2

The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Ranking Member, Committee on the Judiciary 4

WITNESSES

Mr. Steven G. Bradbury, Acting Assistant Attorney General, Office of Legal Counsel, U.S. Department of Justice

Oral Testimony 8

Prepared Statement 11

Mr. Robert L. Deitz, General Counsel, National Security Agency

Oral Testimony 18

Prepared Statement 20

Mr. Robert D. Alt, Fellow, Legal and International Affairs, The John M. Ashbrook Center for Public Affairs, Ashland University

Oral Testimony 22

Prepared Statement 25

Mr. Jim Dempsey, Policy Director, Center for Democracy and Technology

Oral Testimony 32

Prepared Statement 35

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement of the Honorable Robert C. Scott, a Representative in Congress from the State of Virginia and Ranking Member, Subcommittee on Crime, Terrorism, and Homeland Security 91

Prepared Statement of the Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan and Ranking Member, Committee on the Judiciary 92

Prepared Statement of the Honorable Sheila Jackson Lee, a Representative in Congress from the State of Texas 93

Prepared Statement of the Honorable Jane Harman, a Representative in Congress from the State of California 94

Letter from the Honorable Sheila Jackson Lee to the Honorable F. James Sensenbrenner, Jr., and the Honorable John Conyers, Jr. 95

Letter to the Honorable Peter Hoekstra and the Honorable Jane Harman from Caroline Fredrickson, Director of the Washington Legislative Office, and Lisa Graves, Senior Counsel for Legislative Strategy, American Civil Liberties Union (ACLU) 96

*Newsweek*Article, "Palace Revolt," dated February 6, 2006 102

Page

H.Res. 819, Requesting the President and directing the Attorney General to submit to the House of Representatives all documents in the possesion of the President and the Attorney General relating to requests made by the National Security Agency and other Federal agencies to telephone service providers requesting access to telephone communications records of persons in the United States and communications originating and terminating within the United States without a warrant 108

LEGISLATIVE PROPOSALS TO UPDATE THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

WEDNESDAY, SEPTEMBER 6, 2006

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME, TERRORISM,
AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 1:06 p.m., in Room 2141, Rayburn House Office Building, the Honorable Howard Coble (Chairman of the Subcommittee) presiding.

Mr. COBLE. Good afternoon, ladies and gentlemen. The hearing on updating the Foreign Intelligence Surveillance Act (FISA) will come to order.

Next Monday, as you all know, is September 11, and we will mark the fifth anniversary of the heinous attacks that killed almost 3,000 Americans on U.S. soil. While we remember those lost, we also must not forget those who continue to put their lives on the line here and abroad to prevent subsequent attacks.

The enemy we face, in my opinion, is not our law enforcement nor our intelligence community, who are working to thwart the terrorists set out to destroy our Nation. The enemy we face furthermore is not brave, ethical or humane. The enemy we face, it seems to me, is cowardly, despicable and inhumane. This enemy flies into buildings, straps bombs onto teenagers to kill innocent bystanders, and continues to plan an attempt to kill even more Americans. More recently, you all know about the Great Britain effort to thwart a plan to blow up planes headed for the United States.

We face an enemy who does not want land, does not want rights, does not want to negotiate. This enemy wants death and destruction, our death and destruction. The men and women in law enforcement and the intelligence community need tools that are streamlined and updated to match the technology and efforts of the terrorists.

Knowing that this is a threat we must defeat, Congress continues to update the laws. Today the Subcommittee will examine a number of proposals that affect foreign intelligence gathering and the need to improve such surveillance.

I believe that the vast majority of people agree that we need to conduct and support surveillance against terrorists. We can't have done this while protecting civil liberties. We need to have a constructive debate over how to ensure that our law enforcement and

intelligence community are on equal footing with these killers. As is often said, the terrorists have to be lucky only once to kill and maim Americans. We have to be correct in every instance.

I look forward to the testimony of our witnesses on how to improve FISA; and now I am pleased to recognize the distinguished gentleman from Virginia, the Ranking Member of the Committee, Mr. Scott.

Mr. SCOTT. Thank you, Mr. Chairman. I want to thank you for holding the hearing on the various proposals to address the NSA surveillance issues. However, this is really a broader issue than encompassed by the various proposals and certainly a broader issue than the minority can address with one witness with a 5-minute statement. So I am hopeful this is merely the start of a series of hearings on this subject area.

I look forward to working with you to fully explore the issue on how Government can appropriately and effectively conduct surveillance on those who would harm Americans without the Government harming Americans through the violation of their rights, freedoms, privacies and protections under the law.

When law enforcement and intelligence officials have something or someone on whom they deem it appropriate to conduct surveillance, I find it insulting and disingenuous to our system of laws and procedures for someone to suggest that they cannot conduct that surveillance because of the need to comply with the Constitution, constitutional procedures which have been in effect for over 200 years. Our order suggests that it is inconvenient to comply with them by obtaining a warrant, and therefore they can't do it at all because it is inconvenient.

It is not inadequate or consistent with our system of checks and balances of Government authority and power to suggest that notifying some Members of Congress under circumstances where Members can go to jail for telling the public what they know, that is not a check and balance that we traditionally have. Unfortunately, under the proposals before us that are likely to get consideration, here we go again using terrorism as a basis to greatly expand the Government's authority to conduct surveillance on innocent Americans in the United States without having to demonstrate to a court or any other detached entity that there is a reasonable basis for such surveillance.

First of all, Mr. Chairman, we don't even know what kind of surveillance is currently being done by NSA. The logic used by the Administration, that they have said publicly, to listen in to calls coming into the United States applies equally to those calls that are domestic as well as those that are initiated abroad. Yet without any public or otherwise effective oversight and assessment of what the President through the NSA is doing secretly to conduct surveillance in America and whether or not that is legal would not only designate it as legal but greatly expanding his opportunity to do so.

Now, we have seen numerous instances in this Administration where it sees itself above the traditional boundaries of law. We saw it with the process where they just declare someone an enemy combatant, including American citizens, and holding them indefinitely with no end in sight and depriving them of all rights and remedies to even contest their designation. And when the Administration fi-

nally did have to acknowledge the necessity for charging and trying the accused persons, the decision was made to try them through military tribunals, which don't have the traditional checks and balances that other procedures have.

We also saw the same approach to policies promoted by the torture memorandum leading to the Abu Ghraib torture incidents. In addition, we saw it with the Attorney General's decision to listen in on attorney/client conversations to detain persons. And now with previously secret decisions to listen in on conversations of Americans coming into or going out of the country, and whatever else they are doing, we just don't know because we haven't called on them to account for this to this oversight Committee, and we haven't gotten answers to the questions that we proposed.

All of these activities avoid any approval or scrutiny of the courts. We only find out the true nature of what is happening when it is brought to the courts through challenges to the constitutionality, as we found with the Padilla and the Hamdan cases, and now we see it with the NSA case brought by the ACLU, which is working its way through the courts after the initial finding that the process is unconstitutional.

So instead of moving now to try to cloak the activity in a veil of legitimacy, now, instead of trying to figure out what they are doing, we are simply cloaking the activity through a veil of legitimacy through legislation. Rather than doing that, we should wait at least until the court's final determination or at least have the Administration proceed on its case where it would seek FISA's court review of its activities.

It is simply unacceptable to Americans that a call made or received by citizens in this country can be listened to or otherwise intercepted by the Government without approval or review by a court with authority to authorize or deny such interception based on whether good cause is shown. To do so is tantamount to operating under a police state and in variance to some of the most basic, fundamental principles upon which this Nation was founded. And all of this is done without any presentation or indication of a need for such sweeping additional governmental authority over citizens' private affairs or any credible evidence or finding of any inadequacies in the current law to justify such a drastic change.

One protective thing to note is the Wilson-Sensenbrenner and the Specter bills. One thing they do, by analogy, is to confirm by inference that the current NSA surveillance activity is patently illegal; otherwise, there would be no need for those bills to be introduced. So I hope you will carefully study this issue, Mr. Chairman, and move to require the Administration to be in compliance with existing law.

There is no inconsistency to protecting us from terrorism and remaining a country which operates under the rule of law. We should first assure compliance of existing law, then determine whether any changes are needed to provide for greater effectiveness on the part of law enforcement; not change the law just to conform to what we think the Administration might be doing.

I look forward to the testimony of our witnesses on this important issue, Mr. Chairman; and again, hope that this is one of a series of hearings so that we can fully figure out what is going on.

Mr. COBLE. I thank the gentleman from Virginia.

Prior to recognizing the distinguished gentleman from Michigan, the Ranking Member of the Full Committee, I will say to the Members of the Subcommittee, all Members may without objection may have their statements included into the record.

The gentleman——

Mr. SCOTT. Mr. Chairman, could I recognize—we have one person who is not a Member of the Committee, Ms. Jane Harman, who is the ranking Democrat on the Intelligence Committee.

Mr. COBLE. I was going to recognize her separately. I think not. Good to have you both with us.

And now the distinguished gentleman from—oh, Mr. Delahunt and Mr. Chabot and Mr. Flake from Arizona and Ohio.

Mr. Delahunt from Missouri—strike that. From Massachusetts. I will be okay. It has been a tough work period.

Mr. DELAHUNT. Missouri?

Mr. COBLE. I will talk to you about that later.

The gentleman from Michigan for his opening statement, Mr. Conyers.

Mr. CONYERS. Thank you, Chairman Coble, and to our friends and Members who have joined us.

First of all, I would like to recognize the witnesses, Mr. Dempsey and Mr. Bradbury, Mr. Deitz, Mr. Alt. And also I would like unanimous consent to put in the record the American Civil Liberties Union letter written by ACLU Director Fredrickson.

Mr. COBLE. Without objection, that will be accepted.

[The information referred to follows in the Appendix]

Mr. CONYERS. Thank you very much.

And I am very happy that we have permitted Ranking Member Jane Harman of the Intelligence Committee to join us today. I am sorry that we may not be able to permit her to make any statements. I would be willing to give her some of my time, if not all of it, actually because of the good work she has done on the legislation that we are now also considering before the Committee.

But at any rate, she has a statement that I would like unanimous consent to have put in the record.

Mr. COBLE. Without objection.

[The prepared statement of Ms. Harman follows in the Appendix]

Mr. COBLE. Mr. Conyers, would you yield to me?

Mr. CONYERS. Of course.

Mr. COBLE. Ms. Harman, we are delighted to have you here. In light of consistency, we have never permitted a Member who does not sit on the Full Committee to take part. We will be glad to have your statement in the record.

Thank you, Mr. Conyers.

Mr. CONYERS. Thank you very much.

I start out on the premise, building upon our Ranking Subcommittee Member Scott's excellent set of observations, and I join with him in urging that there be additional hearings on this subject matter. I start out on the point that we strongly support intercepting each and every conversation involving al-Qaeda and its supporters whether in the United States or anywhere else. But the concerns that we meet here today about are whether it is a sensible thing to do to take up legislation that simply codifies an unlawful

surveillance program and which further unjustifiably expands the President's authority.

The current statute on this subject allows for court-approved wiretaps and includes an emergency exception allowing wiretapping without a court order for up to 72 hours. And it seems to me that that is the first hurdle we have got to get over.

If additional resources are needed to comply with the law and the Fourth Amendment, we should authorize them. I think we would be more than happy to do that. But since September 11, we have made more than 25 separate changes in the Foreign Intelligence Surveillance Act at the Administration's request and thousands of wiretaps have been approved by the courts, hundreds of emergency orders have been issued. Very few adviser requests are turned down and the court itself has streamlined its procedures to accommodate the Administration's needs.

We have done everything that's been requested of us. And the Administration has still chosen to act unilaterally and outside the law.

Nine months after we have learned about this warrantless surveillance program, there has been almost—little or no independent inquiry into its legality. Not only have we failed to conduct any sort of investigation, but the Administration summarily rejected all requests for special counsels as well as reviews by the Department of Justice and the Department of Defense Inspectors General.

When the Department of Justice finally opened an investigation, the President himself squashed it by denying the investigators security clearances. The Department of Justice has completely ignored numerous questions posed by this Committee, as well as the Wexler resolution of inquiry that we previously adopted.

We have got some big problems here and I would ask that the remainder of my opening statement be included in the record, and I thank you for the permission to make it at this time.

Mr. COBLE. I thank you, Mr. Conyers.

[The prepared statement of Mr. Conyers follows in the Appendix]

Mr. COBLE. Gentlemen, as part of the Subcommittee, I need to swear in all witnesses appearing before us so if you would please stand and raise your right hand.

[Witnesses sworn.]

Mr. COBLE. Let the record show that each of the witnesses answered in the affirmative.

Mr. DELAHUNT. Mr. Chairman, before we hear from the witnesses, if I could inquire of the Chair, it was my understanding that the Chairman of the Full Committee, Mr. Sensenbrenner, was going to consider the Wexler resolution of inquiry as a subpoena—I don't want to mischaracterize it—and presumably there was going to be, from the passage of the resolution of inquiry coming out of this Committee, some consultation between the Department of Justice, the White House and the Committee.

If you know, Mr. Chairman, has there been any discussion regarding these issues?

Mr. COBLE. I believe, Mr. Delahunt, if you yield——

Mr. DELAHUNT. I yield.

Mr. COBLE.—I think that we are awaiting a response from DOJ.

Mr. DELAHUNT. Well, I think it is important, if you have it readily available, to enter into the record the date of the resolution of inquiry, because I would have expected and anticipated that a 6- or 7-week period would have been sufficient time for the Department of Justice to provide this Committee, the Committee that has jurisdiction over the Department of Justice, the information that was requested.

Mr. COBLE. If the gentleman would yield again, I concur. I do think ample time has expired and a response should be in hand.

Let me talk to the Chairman about that subsequent, Mr. Delahunt, and that is all I can say about that.

Mr. DELAHUNT. Maybe Mr. Bradbury can enlighten us.

Mr. BRADBURY. Unfortunately, I am not in a position to—I am not involved in the discussions, and I don't know the status of that request.

Mr. CONYERS. Mr. Chairman, can I ask unanimous consent that the Wexler resolution be included in the record?

Mr. COBLE. Is there any objection?

Without objection.

[The information referred to follows in the Appendix]

Mr. CONYERS. Thank you.

Mr. COBLE. Mr. Delahunt, are you finished? I cut you off.

Mr. DELAHUNT. You didn't cut me off, and I appreciate you giving me the time.

I just find it disturbing that we don't know. We know nothing about the program. We know nothing about even whether there has been communication between the Department of Justice and this Committee.

I mean, I just have to associate myself with the remarks of Mr. Scott. I mean, I am sure this will be a very nice and cordial conversation among these distinguished gentlemen and we will have a chance to banter back and forth with our friends from Texas.

Mr. GOHMERT. Will the gentleman yield?

Mr. DELAHUNT. Of course.

Mr. GOHMERT. I am curious whether the Jefferson raid on his office may be precedent for the fact that when an entity fails to respond to a request for documents for a certain length of time, if that allows you to get the local law enforcement or the Capitol Police and go raid an office to obtain that information. I am not sure which precedent that set.

Mr. DELAHUNT. Reclaiming my time. That is a very interesting observation. But I just feel, and again with great respect to the Chair, I feel we are being played with.

You know, I don't want to look like we are the Bundestag during the Third Reich and just roll over for an Administration that is going to say to us, we will get around to it when we feel like it.

I hope that is not the case, but it has the appearances, Mr. Chairman, of—well, we are going to have a hearing today, and like I said, I am sure it will be interesting, kind of an academic exercise. But I don't think any Member of this panel—on either side, Republican or Democrat, we don't know anything, and I think that we have a constitutional right and out of just simple comity, respect for this institution, that that response should have been forthcoming. If it's the position of the Department of Justice that

they refuse to respond to this Committee and—by the way, a majority of which is Republican, then I think we ought to know about that.

With that, I yield back.

Mr. COBLE. I thank the gentleman.

We have four distinguished visitors, witnesses, with us today. And, folks, I don't want to sound like we are trying to buggy-whip anybody. I regard myself as a—pardon my immodesty, as a pretty easy dog to hunt with, as is Mr. Scott. But, folks, we received one statement late last night and one statement late this morning. Just take back to your superiors that timely presentation of statements would afford us a little more luxury in preparing for the hearing.

Let me introduce the distinguished witnesses with us today.

Our first witness is Mr. Steve Bradbury, Acting Assistant Attorney General for the Office of Legal Counsel at the Department of Justice. Prior to working for the Department of Justice, Mr. Bradbury was a partner with the law firm of Kirkland & Ellis, LLP, and prior to that served as a law clerk to Justice Clarence Thomas of the Supreme Court.

Mr. Bradbury obtained his undergraduate degree from Stanford University and his J.D. from the Michigan School of Law, where he was graduating magna cum laude.

Our second witness is Mr. Robert Deitz, General Counsel of the National Security Agency. Mr. Deitz has served as General Counsel of the NSA since 1998, as well as periodically serving as Acting General Counsel for the National Geospatial Intelligence Agency and Acting Deputy Counsel For Intelligence at the Department of Defense. Prior to working for the NSA, Mr. Deitz was a partner in the Washington, DC, office of Perkins Coy.

He received his B.A. with honors from Middlebury College, M.B.A. from the Woodrow Wilson School of Public and International Affairs at Princeton University and his J.D. from the Harvard School of Law where he was graduated magna cum laude.

Our third witness is Mr. Robert Alt. He is a Fellow in Legal and International Affairs at the John M. Ashbrook Center for Public Affairs at Ashland University, where he has taught classes on constitutional law, political parties and interest groups. Most recently, he was made a Fellow at the Institute of Global Security Law & Policy at the Case School of Law, for which we add our congratulations.

Mr. Alt has published articles in numerous media publications including the Wall Street Journal, the Washington Times and the San Diego Union Tribune and has provided commentary on several major news networks. Mr. Alt received his J.D. Degree from the University of Chicago.

Our final witness, Mr. Jim Dempsey, is Policy Director for the Center for Democracy and Technology. Mr. Dempsey has been with the Center since 1997 and previously served as Executive Director. Prior to joining the Center for Democracy and Technology, Mr. Dempsey was the Deputy Director for the Center for National Security Studies, and prior to that he served as Assistant Counsel for the House Judiciary Subcommittee on Civil and Constitutional Rights.

Good to have you back on the Hill, Mr. Dempsey.

Mr. Dempsey also practiced in areas of Government and commercial contracts, energy law and antitrust while an associate with the Washington, D.C., law firm of Arnold & Porter. He maintained that extensive *pro bono* reputation of death row inmates in Federal habeas proceedings.

Now I apologize to all of you for my lengthy, detailed introduction, but I think it is important for all of us, including those in the hearing room, to know the credentials that witnesses do indeed bring to the table at these hearings.

Gentlemen, as you all have been previously advised, we operate under the 5-minute rule. When you see that amber light appear in your face, you will know that your time is running out. You will have a minute at that point. Now, no one is going to be keyholed if you violate the 5-minute rule but when the red light appears, that is your warning that the 5 minutes have elapsed, and we would ask you to conclude at that point.

Mr. Bradbury, we will start with you.

TESTIMONY OF STEVEN G. BRADBURY, ACTING ASSISTANT ATTORNEY GENERAL, OFFICE OF LEGAL COUNSEL, U.S. DEPARTMENT OF JUSTICE

Mr. BRADBURY. Thank you, Mr. Chairman, Ranking Member Scott, distinguished Members of this Committee.

As we approach the 5-year anniversary of 9/11, the single deadliest foreign attack on U.S. soil in our Nation's history, we recognize what our enemies well knew long before 9/11. We are at war. The enemies we face today operate in obscurity through secret cells that operate globally while plotting to carry out attacks from within our own communities. Less than 1 month ago, British security services neutralized a planned attack program only days from execution. These terrorists planned to use sophisticated explosives, capable of evading airport screenings, to blow up perhaps a dozen airliners bound for the United States.

We can all agree that foreign intelligence surveillance is a critical tool in our common effort to prevent another catastrophic terrorist attack on the United States. At the same time, we all recognize the fundamental challenge the war on terror presents for a free society. We must detect and prevent the next 9/11 while steadfastly safeguarding the liberties we cherish. As we seek to reframe FISA, we must ensure that we retain the constitutional balance between security and liberty.

The 28 years since the enactment of FISA have seen one of the greatest transformations in modes of communication of any period in history. In 1978, almost all transoceanic communications into and out of the United States were carried by satellite, and Congress intentionally kept those communications largely outside the scope of FISA's coverage consistent with FISA's primary focus on domestic communications surveillance. At that time, Congress did not anticipate the technology revolution that would bring us global, high-speed fiber-optic networks, the Internet, e-mail and disposable cell phones.

Innovations in communications technology have fundamentally transformed how our enemies communicate, and therefore how they plot and plan their attacks. It is more than a little ironic that

al-Qaeda expertly exploits the communication tools of the Internet Age to advance extremist goals of intolerance and tyranny that are more suited to the 12th century than the 21st. Meanwhile, the United States, the most advanced nation on earth, confronts the threat of al-Qaeda with a legal regime primarily designed for the last century and a Cold War adversary that no longer exists.

The President authorized the terrorist surveillance program in the wake of 9/11 in order to establish an early warning system to detect and prevent further al-Qaeda attacks. As described by the President, that program, which has been the subject of numerous prior congressional hearings and extensive oversight by the Intelligence Committees of both Houses of Congress, involves the NSA's monitoring of international communications into and out of the United States where there are reasonable grounds to believe that at least one party to the communication is a member or agent of al-Qaeda or an affiliated terrorist organization. The terrorist surveillance program places the initial decision to target communications for interception in the hands of highly trained intelligence professionals subject to rigorous oversight. This program preserves the speed and agility necessary for wartime surveillance.

Congress is currently considering several pieces of legislation addressing FISA and the terrorist surveillance program. I want to thank the Members of Congress for their hard work toward crafting a comprehensive approach that will help us protect the Nation from terrorists and other foreign threats, gather critical foreign intelligence more effectively and still protect civil liberties. In particular, I want to thank Representative Wilson, who sits on the Intelligence Committee and has introduced a bill, cosponsored by Sensenbrenner and Hoekstra, which seems to move FISA into the 21st century. I intend to focus my remarks today primarily on Representative Wilson's bill.

Fundamentally, her legislation recognizes that in times of armed conflict involving an exigent terrorist threat, the President may need to act with agility and dispatch to protect the country by putting in place a program of electronic surveillance targeted at the terrorists and designed to detect and prevent the next attack. We see promise in this bill and hope we can work with Congress in producing legislation quickly that addresses the threats that face the Nation.

I would point out that this bill, however, would require the President to wait for the United States actually to be attacked before he could initiate an electronic surveillance program under this Administration. We think the President cannot and should not wait for thousands of Americans to die before initiating vital intelligence collection.

Article II of the Constitution, as we have explained in the paper that we provided to Congress back in January, already gives the President the authority to take such actions to defend the Nation. And to use the words of the FISA Court of Review, nothing in FISA could "encroach on the President's constitutional power." We believe it is important that Congress support and assist the President in performing this most solemn constitutional obligation.

Representative Wilson's bill also includes several important reforms to update FISA for the 21st century. These changes are de-

signed to account for the fundamental changes in technology that have occurred since FISA's enactment in 1978 and to make FISA more effective and more useful in addressing the foreign intelligence needs of the United States.

Changes contained in the bill would correct the most significant anachronisms in FISA. It would also make some significant changes to streamline the FISA application process. These provisions in Representative Wilson's bill offer a good start toward important improvements toward the existing FISA process, but further refinements are appropriate.

The Executive Branch has been working and will work hard to solve the problems represented by updating the FISA statute, and we will work with Representative Wilson and with Members of Congress to put refinements in this legislation and improve it so that it gets the job done in a way that will best protect the country and preserve our liberties.

Again, Mr. Chairman, thank you for the opportunity to appear today on this important issue.

Mr. LUNGREN. [Presiding.] Thank you, Mr. Bradbury.

[The prepared statement of Mr. Bradbury follows:]

PREPARED STATEMENT OF STEVEN G. BRADBURY

Department of Justice

STATEMENT

OF

STEVEN G. BRADBURY
ACTING ASSISTANT ATTORNEY GENERAL
OFFICE OF LEGAL COUNSEL
DEPARTMENT OF JUSTICE

BEFORE THE
SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING
LEGISLATIVE PROPOSALS TO UPDATE
THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

PRESENTED ON
SEPTEMBER 6, 2006

STATEMENT

OF

STEVEN G. BRADBURY
ACTING ASSISTANT ATTORNEY GENERAL
OFFICE OF LEGAL COUNSEL
DEPARTMENT OF JUSTICE

BEFORE THE
SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING
LEGISLATIVE PROPOSALS TO UPDATE THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

PRESENTED ON
SEPTEMBER 6, 2006

Thank you, Chairman Coble, Ranking Member Scott, and Members of the Subcommittee. I appreciate the opportunity to appear here today to discuss proposed revisions to the Foreign Intelligence Surveillance Act of 1978, or "FISA."

As we approach the five-year anniversary of 9/11, the single deadliest foreign attack on U.S. soil in our Nation's history, we recognize what our enemies well knew long before 9/11—we are at war. The enemies we face today operate in obscurity, through secret cells that communicate globally while plotting to carry out surprise attacks from within our own communities. Less than one month ago, British security services neutralized a planned attack—perhaps only days from execution. These terrorists planned to use sophisticated explosives, capable of evading airport screenings, to blow up perhaps a dozen airliners bound for the United States.

We can all agree that foreign intelligence surveillance is a critical tool in our common effort to prevent another catastrophic terrorist attack on the United States. At the same time, we all recognize the fundamental challenge the War on Terror presents for a free society: We must detect and prevent the next 9/11, while steadfastly safeguarding the liberties we cherish. As we seek to reframe FISA, we must ensure that we maintain the constitutional balance between security and liberty.

The 28 years since the enactment of FISA have seen one of the greatest transformations in modes of communication of any period in history. In 1978, almost all transoceanic communications into and out of the United States were carried by satellite, and Congress intentionally kept those communications largely outside the scope of FISA's coverage, consistent with FISA's primary focus on domestic communications surveillance. At that time, Congress did not anticipate the technological revolution that would bring us global high-speed fiber-optic networks, the Internet, e-mail, and disposable cell phones.

Innovations in communications technology have fundamentally transformed how our enemies communicate, and therefore how they plot and plan their attacks. It is more than a little ironic that al Qaeda expertly exploits the communications tools of the Internet age to advance extremist goals of intolerance and tyranny that are more suited to the 12th century than the 21st. Meanwhile, the United States, the most advanced Nation on earth, confronts the threat of al Qaeda with a legal regime primarily designed for the last century and a cold war adversary that no longer exists.

The President authorized the Terrorist Surveillance Program in the wake of 9/11 in order to establish an early warning system to detect and prevent further al Qaeda

attacks. As described by the President, that Program, which has been the subject of numerous prior congressional hearings and extensive oversight by the Intelligence Committees of both Houses of Congress, involves the NSA's monitoring of international communications into and out of the United States where there are reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. The Terrorist Surveillance Program places the initial decision to target communications for interception in the hands of highly trained intelligence professionals, subject to rigorous oversight. This program preserves the speed and agility necessary for wartime surveillance.

Congress is currently considering several pieces of legislation addressing FISA and the Terrorist Surveillance Program. I want to thank the members of Congress for their hard work toward crafting a comprehensive approach that will help us protect the Nation from terrorists and other foreign threats, gather critical foreign intelligence more effectively, and still protect civil liberties. In particular, I want to thank Representative Wilson, who sits on the Intelligence Committee and has introduced a bill, cosponsored by Chairman Sensenbrenner and Chairman Hoekstra of the Intelligence Committee, which seeks to move FISA into the 21st Century.

I intend to focus my remarks today on Rep. Wilson's bill.

Fundamentally, Rep. Wilson's legislation recognizes that in times of armed conflict involving an exigent terrorist threat, the President may need to act with agility and dispatch to protect the country by putting in place a program of electronic surveillance targeted at the terrorists and designed to detect and prevent the next attack. We see promise in this bill, and hope we can work with the Congress in producing

legislation quickly that addresses the threats that face the Nation. This bill, however, would require the President to wait for the United States to be attacked before he could initiate an electronic surveillance program designed to protect against terrorist attack. The President cannot and should not wait for thousands of Americans to die before initiating vital intelligence collection, and we urge that this provision be amended to allow for a program when the best intelligence indicates a severe threat of attack.

Article II of the Constitution already gives the President authority to take such actions to defend the Nation. To use the words of the FISA Court of Review, nothing in FISA (or any other statute) could "encroach on the President's constitutional power." *In re Sealed Case*, 310 F.3d 717, 742 (Foreign Intel. Surv. Ct. of Rev. 2002). It is important that Congress support and assist the President in performing this most solemn constitutional obligation. Legislation that purports to eliminate the President's authority to protect the Nation or to channel that authority through procedures that were never meant to apply during armed conflict and that are inadequate in that context creates an unnecessary conflict between the political Branches and puts the Nation at greater risk.

Rep. Wilson's bill also includes several important reforms to update FISA for the 21st century. These changes are designed to account for the fundamental changes in technology that have occurred since FISA's enactment in 1978, and to make FISA more effective and more useful in addressing the foreign intelligence needs of the United States, especially in protecting the Nation from the unique threats of international terrorism. Importantly, the bill reflects an understanding that the key to reforming FISA—to improving our intelligence capabilities while preserving civil liberties—rests not in multiplying the number of lawyers or in adding layers of review.

Changes contained in the bill would correct the most significant anachronisms in FISA. Most fundamentally, the bill would change the definition of "electronic surveillance" in title I of FISA to restore FISA's original focus on surveillance of the domestic communications of persons in the United States. It would generally exclude surveillance of international communications where the Government is not targeting a particular person in the U.S. This change would update FISA to make it technology-neutral and to reinstate FISA's original carve-out for certain foreign intelligence activities in light of changes in international communications technology that have occurred since 1978.

The bill would also change the statutory definition of "agent of a foreign power"—*i.e.*, who can be subject to FISA surveillance—to include any person other than a U.S. person who possesses or is expected to transmit or receive foreign intelligence information while within the United States. Occasionally, a foreign person will enter the United States in circumstances where the Government knows that he possesses valuable foreign intelligence information, but where that person's relationship with a foreign power or international terrorist organization is unclear. Unfortunately, the Government currently has no means to conduct surveillance of that person under FISA.

Finally, the bill would significantly streamline the FISA application process. Among other things, the bill would limit the amount of detail required for applications and would amend the "emergency authorization" provision to permit emergency surveillance for a longer period, as opposed to the current three days—the period within which an application would have to be submitted and approved by the FISA Court or the emergency surveillance cease. (Currently, Rep. Wilson's bill would make it five days;

we suggest that it be seven.) These provisions offer a good start toward important improvements to the existing FISA process, but further refinements are appropriate. The Executive Branch has worked hard to solve the problems presented by updating a statute as important and complicated as FISA. We believe that we can offer many technical improvements to this part of Rep. Wilson's bill, and we look forward to working with her and Congress to make these critical changes.

We believe that any legislative package must also deal with the litigation arising from the Terrorist Surveillance Program and other alleged classified communications intelligence activities. Such litigation undeniably risks national security by increasing the risk of additional disclosures and by subjecting vital intelligence activities to the unpredictability of varying (sometimes conflicting) court decisions.

We urge Congress to act to protect sensitive national security programs from the risk of disclosure and disparate treatment in the various district courts where litigation may be brought.

* * *

Again, Mr. Chairman, thank you for the opportunity to appear today to discuss this important issue. We look forward to working with Congress on this critical matter.

# # #

Mr. LUNGREN. Mr. Deitz.

TESTIMONY OF ROBERT L. DEITZ, GENERAL COUNSEL, NATIONAL SECURITY AGENCY

Mr. DEITZ. Good afternoon, Mr. Chairman, Ranking Member Scott and Members of the Committee.

I am pleased to be here today to provide testimony in support of legislative efforts to amend the Foreign Intelligence Surveillance Act of 1978. Changes are needed, I believe, in order to recapture the original constitutional intent of the statute regulating the electronic surveillance of persons within the United States as the Government engages in electronic surveillance. At the same time, surveillance directed at individuals who are not due protection under the Fourth Amendment should be removed from the statute's coverage.

Some of the specifics that support my testimony cannot be addressed in open session, and while I would be happy to elaborate on the technological changes that have taken place since 1978 in an appropriate setting, the essential point can be made very clearly and publicly.

Communications technology has evolved in the 28 years between 1978 and today in ways that have had unforeseen consequences under FISA. Technological changes in the communications environment have brought within FISA's scope communications that we believe the 1978 Congress did not intend to be covered and that were excluded from the act's scope.

Despite this change, NSA's mission remains the same. NSA intercepts communications to protect the lives, liberties

and well-being of the citizens of the United States from those who would do us harm. Today, NSA is often required by the terms of FISA to make a showing of probable cause, a notion derived from the Fourth Amendment in order to target for surveillance the communications of a foreign person overseas. Frequently, though by no means always, that person's communications, in turn, are with another foreign person overseas. In such cases, the current statutory requirement to obtain a court order based on a showing of probable cause slows and in some cases prevents altogether the Government's efforts to conduct surveillance of communications it believes are significant to the national security.

The FISA seeks, in our view, to permit the surveillance of foreign intelligence targets while providing appropriate detection through court supervision to U.S. citizens and to other persons inside the United States. As the legislative history of the 1978 statute states, "The history and law relating to electronic surveillance for 'national security' purposes have revolved around the competing demands of the President's constitutional powers to gather intelligence deemed necessary for security of the nation and the requirements of the Fourth Amendment."

While debates concerning the extent of the President's constitutional powers were heated in the mid-1970's, as they indeed are today, we believe that the judgment of Congress at that time was that it was only when significant Fourth Amendment interests were implicated that court supervision was important. Yet the Fourth Amendment is clearly not always at issue when NSA or an-

other intelligence agency acts, and the FISA on its face never sought to encompass all activities of the NSA within its coverage. Rather, the definitions of the term "electronic surveillance" contained in the statute have always affected just a portion, just a portion of NSA's signals intelligence mission. Indeed, by far the bulk of NSA's surveillance activities take place overseas, and these activities are directed entirely at foreign countries and foreign persons within those countries.

All concerned agree, and to my knowledge have always agreed, that the FISA does not and should not apply to such activities. When NSA undertakes surveillance, that does not mean—I am sorry, when NSA undertakes surveillance that does not meet any of the definitions of electronic surveillance contained in the FISA, it does so lawfully under Executive Order 12333 without any resort to the FISA court.

In addition, even as it engages in its overseas mission, in the course of targeting the communications of persons overseas, NSA will sometimes encounter communications to, from or about U.S. persons. Yet this fact does not in itself cause the FISA to apply to NSA's overseas surveillance activities, and to my knowledge, no serious argument exists that it should. Instead, at all times, NSA applies procedures approved by the U.S. Attorney General to all aspects of its activities, seeking through these procedures to minimize—it is a term of art—the acquisition, retention and dissemination of information concerning U.S. persons. These procedures have worked well for decades to ensure the constitutional reasonableness of NSA's surveillance activities, and eliminate from intelligence reports, incidentally, information concerning U.S. persons that does not constitute foreign intelligence. Accomplishing this has never required a court order.

Because of the way the definition of electronic surveillance contained in the current statute is constructed, NSA must answer four questions in order to determine whether a FISA order is required for it to engage in electronic surveillance. These questions concern the nationality of the target, the location of the target, the means by which the target is communicating and the location from which the communications will be carried out. We believe that the truly significant question on the list is the one that gets to the heart of the applicability of the Constitution, that is, the location of the target of surveillance. The other questions reflect a common-sense approach to 1978 technology that worked well then, but that today has unintended consequences. They are ancillary, if not irrelevant, to the more fundamental issue.

Thus, in some cases, the location from which NSA seeks to acquire communication becomes a question clothed in undue significance. So, too, the technology employed by the provider of the communication service can in some cases be dispositive of whether the Government must obtain a FISA order or not. We think this is far from what was intended by the statute supporters in 1978 and requires change.

Mr. Chairman, I know my time has elapsed. May I have another minute or two, please?

Mr. COBLE. Well, go ahead, but wrap it up.

Mr. DEITZ. Thank you. I will be very quick.

Mr. COBLE. And in a sense of fairness and equity, I will also be equally liberal to the two remaining witnesses. But move it along.

Mr. DEITZ. In our view, the FISA should be returned to what we believe was its original purpose of regulating foreign surveillance targeting persons in the United States, not the surveillance of non-U.S. persons overseas who are not entitled to constitutional rights.

And if I may conclude, we think that these principles that I have articulated, clearly and artfully captured in parts of the original FISA legislation and in its legislative history, should extend to all surveillance under the FISA. The need for a court order should not depend on whether NSA's employees conducting the surveillance are inside the United States or outside the United States, nor should it depend on whether the communications meet the technical definition of "wire communications" or not.

Thank you, Mr. Chairman, and if I could, I request the remainder of my statement be placed in the record.

Mr. COBLE. Without objection.

[The prepared statement of Mr. Deitz follows:]

PREPARED STATEMENT OF ROBERT L. DEITZ

Good morning Mr. Chairman, Ranking Member Scott, and Members of the Committee.

I am pleased to be here today to provide testimony in support of legislative efforts to amend the Foreign Intelligence Surveillance Act of 1978. Changes are needed, I believe, in order to recapture the original Congressional intent of the statute—regulating the electronic surveillance of persons within the United States—as the Government engages in electronic surveillance. At the same time, surveillance directed at individuals who are not due protection under the Fourth Amendment should be removed from the statute's coverage.

Some of the specifics that support my testimony cannot be discussed in open session, and while I would be happy to elaborate on the technological changes that have taken place since 1978 in an appropriate setting, the essential point can be made very clearly and publicly: communications technology has evolved in the 28 years between 1978 and today in ways that have had unforeseen consequences under FISA. These stunning technological changes in the communications environment have brought within FISA's scope communications that we believe the 1978 Congress did not intend to be covered and that were excluded from the Act's scope.

Despite this change, NSA's mission remains the same. NSA intercepts communications to protect the lives, the liberties, and the well-being of the citizens of the United States from those who would do us harm. Today, NSA is often required by the terms of FISA to make a showing of probable cause, a notion derived from the Fourth Amendment, in order to target for surveillance the communications of a foreign person overseas. Frequently, though by no means always, that person's communications are with another foreign person overseas. In such cases, the current statutory requirement to obtain a court order, based on a showing of probable cause, slows, and in some cases prevents altogether, the Government's efforts to conduct surveillance of communications it believes are significant to the national security.

The FISA seeks—we believe—to permit the surveillance of foreign intelligence targets, while providing appropriate protection through court supervision to U.S. citizens and to other persons in the United States. As the legislative history of the 1978 statute states: "[t]he history and law relating to electronic surveillance for 'national security' purposes have revolved around the competing demands of the President's constitutional powers to gather intelligence deemed necessary for the security of the nation and the requirements of the Fourth Amendment." [1] While debates concerning the extent of the President's constitutional powers were heated in the mid-1970s, as indeed they are today, we believe that the judgment of Congress at that time was that it was only when significant Fourth Amendment interests were implicated that court supervision was important .

Yet the Fourth Amendment is clearly not always at issue when NSA or another intelligence agency acts, and the FISA on its face never sought to encompass all ac-

[1] H.Rpt. 95–1283 at p. 15, 95th Congress, 2d Session, June 8, 1978.

tivities of the NSA within its coverage. Rather, the definitions of the term "electronic surveillance" contained in the statute have always affected just a portion of NSA's signals intelligence mission. Indeed, by far the bulk of NSA's surveillance activities take place overseas, and these activities are directed entirely at foreign countries and foreign persons within those countries. All concerned agree, and to my knowledge have always agreed, that the FISA does not and should not apply to such activities. When NSA undertakes surveillance that does not meet any of the definitions of electronic surveillance contained in the FISA, it does so lawfully under Executive Order 12333 without any resort to the FISA court.

In addition, even as it engages in its overseas mission, in the course of targeting the communications of foreign persons overseas, NSA will sometimes encounter information to, from or about U.S. persons. Yet this fact does not, in itself, cause the FISA to apply to NSA's overseas surveillance activities, and to my knowledge no serious argument exists that it should. Instead, at all times, NSA applies procedures approved by the U.S. Attorney General to all aspects of its activities, seeking through these procedures to minimize the acquisition, retention, and dissemination of information concerning U.S. persons. These procedures have worked well for decades to ensure the constitutional reasonableness of NSA's surveillance activities, and eliminate from intelligence reports incidentally acquired information concerning U.S. persons that does not constitute foreign intelligence. Accomplishing this has not required a court order.

Because of the way the definition of "electronic surveillance" contained in the current statute is constructed, NSA must answer four questions in order to determine whether a FISA order is required for it to engage in electronic surveillance. These questions concern the nationality of the target, the location of the target, the means by which the target is communicating, and the location from which the surveillance will be carried out. We believe that the truly significant question on this list is the one that gets to the heart of the applicability of the Constitution—the location of the target of surveillance. The other questions reflect a common sense approach to 1978 technology that worked well then, but that today has unintended effects. They are ancillary, if not irrelevant, to the more fundamental issue.

Thus, in some cases, the location from which NSA seeks to acquire a communication becomes a question clothed in undue significance. So, too, the technology employed by the provider of the communications service can in some cases be dispositive of whether the Government must obtain a FISA order or not. We think this is far from what was intended by the statute's supporters in 1978, and requires change.

Principally, the issue on which the need for a court order should turn—but does not turn under the current FISA—is whether or not the person whose communications are targeted is generally protected by the guarantees of the Constitution. That question, in turn, is largely determined by the location of the target. People inside the United States who are the targets of electronic surveillance, regardless of where the surveillance is conducted or what means are used to transmit a communication, should be the only ones who receive the protection afforded by court approval. At the same time, people outside the United States who are not U.S. persons, again regardless of where the surveillance is effected or the technology employed, should not receive such protection. The FISA should be returned to what we believe was its original purpose of regulating foreign surveillance targeting persons in the United States, not the surveillance of non-U.S. persons overseas who are not entitled to constitutional rights.

Moreover, the current FISA—at least in some places—already recognizes this principle. As I have noted already, we think the most significant factor in determining whether or not a court order is required ought to be the location of the target of the surveillance, and that other factors such as where the surveillance takes place and the mode of communication surveilled should not play a role in this determination. Significantly, this was recognized in the legislative history of the current statute with respect to the first of the definitions of electronic surveillance—the intentional targeting of the communications of a U.S. person in the United States. We believe the legislative history makes clear with respect to that definition that when the communications of U.S. persons located in the United States are targeted, the surveillance is within the scope of FISA regardless of whether the communications are domestic or international and regardless of where the surveillance is being carried out.[2] The same legislative history regarding that first definition of electronic surveillance makes equally clear, however, that the statute does not regulate the

[2] Id. at 50.

acquisition of communications of U.S. persons in the United States when those persons are not the actual targets of the surveillance.[3]

We think these principles, clearly and artfully captured in parts of the legislation and in the legislative history, should extend to all surveillance under the FISA. The need for a court order should not depend on whether NSA's employees conducting the surveillance are inside the United States or outside the United States, nor should it depend on whether the communications meet the technical definition of "wire communications" or not. These factors were never directly relevant in principle, but in the context of yesterday's telecommunications infrastructure were used as a proxy for relevant considerations. Today they are utterly irrelevant to the central question at issue: who are the people deserving protection. Whether surveillance should require court supervision ought to depend on whether the target of such surveillance is located within the United States.

In addition to changing the definition of electronic surveillance, other changes are needed as well. For example, it is vitally important that the Government retain a means to compel communications providers to provide information to the Government, even in the absence of a court order. It is also critical that companies assisting the Intelligence Community in preventing future attacks on the United States be insulated from liability for doing so.

Let me reiterate in closing that we believe the statute should be updated to account for changes that have taken place in technology since its initial passage. Furthermore, we think the appropriate way to change the statute is to focus on constitutionally significant factors that will ensure that the rights of U.S. citizens are protected, while setting aside ancillary issues such as the technical means employed or the location from which the surveillance was conducted.

Mr. COBLE. Mr. Bradbury, you were an unfortunate beneficiary of having gone first, but the gentleman from California said you have an extra minute as well.

So you and Mr. Dempsey will be treated accordingly.

Mr. Alt.

TESTIMONY OF ROBERT D. ALT, FELLOW, LEGAL AND INTERNATIONAL AFFAIRS, THE JOHN M. ASHBROOK CENTER FOR PUBLIC AFFAIRS, ASHLAND UNIVERSITY

Mr. ALT. Thank you, Mr. Chairman and Members of the Subcommittee.

As you begin to take up the potential legislation that's been authored, there may be a temptation to wait for a judicial determination of the NSA wiretap program. Let me implore you, don't indulge that temptation. While the District Court recently offered its opinion that the program is unconstitutional, the court clearly erred with respect to the question of standing and failed to properly apply Supreme Court precedent which was directly on point.

It is extraordinarily likely that the District Court's opinion will be reversed on appeal without the reviewing court having to address any of the merits in the case. Given the difficulty in establishing standing in this case in general and against—in these sorts of challenges against FISA in particular, the legal status of the NSA wiretap program is not easily amenable or reducible to judicial determination. Accordingly, it is necessary for the political branches to regulate themselves, and therefore it is imperative for Congress to take a fresh look at the FISA program.

Having determined that a legislative solution is necessary, some of the proposed legislation this Committee is reviewing today seeks to introduce FISA's requirements as the sole method of conducting the NSA's surveillance program thereby effectively terminating the program. While some seek to provide the President with clear stat-

[3] Id.

utory authorization under FISA to conduct the program itself, in deciding which course to take, this Committee should be cognizant of two things: First, the NSA wiretap program is needed, as a practical matter, to address the emerging national security threats in a timely fashion, and second, the program is consistent with the constitutional requirements for the acquisition of foreign intelligence surveillance.

Given the classified nature of the NSA program, the witnesses testifying today from the DOJ and NSA will presumably be better equipped to discuss the necessity for the Executive Branch to maintain continued flexibility in how it performs foreign intelligence surveillance. However, the need to streamline and modernize the procedures required by FISA to allow the Executive Branch to effectively combat the current terrorist threat is readily apparent even without specific knowledge of the program. Inevitably, while some changes were made to the requirements for obtaining a FISA warrant after the terrorist attack on 9/11, the process remains cumbersome and subject to bureaucratic delay, a fact that the 9/11 Commission noted in its fact-finding in which it specifically noted that requests for such approvals are overwhelming the ability of the system to process them and to conduct the surveillance.

Accordingly, the well-worn argument that FISA's procedural barriers are light is belied by actual practice, and the related claim that the Executive Branch need only submit all requests for foreign surveillance to the FISA court turns out to be unduly burdensome.

This leads naturally to the second point, a discussion of constitutional considerations, because—notwithstanding the desire of the Government to eliminate roadblocks of information gathering—our constitutional system imposes burdens on such practices in order to maintain a proper separation of the powers and to safeguard civil liberties.

For example, in the context of criminal law enforcement, the Fourth Amendment's general search requirement—subject, of course, to exceptions—prior to the execution of a search is one such barrier that will be placed on the Government. However, the courts have consistently acknowledged that the standard which the Government must meet in order to conduct foreign intelligence surveillance and the President's authority to conduct such surveillance are constitutionally distinct from general criminal law enforcement.

A recent decision by the FISA Court of Appeals held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information and suggested, further, that we take for granted that the President does not—or has the authority and, assuming that is so, FISA could not encroach on the President's constitutional power.

This case is instructive concerning the scope of Presidential power in the field of foreign intelligence surveillance, and indeed the last sentence of this quote is telling because it suggests that the Presidential authority is sufficient in the context of foreign intelligence surveillance even when the President's power is languishing at what Justice Jackson famously referred to as "its lowest ebb," that is, when the President "takes matters incompatible with the expressed or implied will of Congress."

Because reforming FISA is necessary to address emerging threats to national security, and because instituting procedures like those used in the NSA's wiretap program are consistent with the constitutional requirements for foreign intelligence surveillance, Congress should seek reforms to FISA which provide the Executive Branch with the kind of flexibility available to the Executive in the NSA program, while maintaining adequate oversight to assure that the program is administered within the limitations of foreign intelligence surveillance.

In so doing, any legislation addressing FISA should seek to meet the following objectives:

First, it should update the language of FISA to address the changes in technology and modes of communication which the former witnesses have already discussed.

Second, it should provide the President with the ability to conduct foreign intelligence surveillance with fixed, renewable periods of time without obtaining a FISA warrant.

And third, it should require renewals of the warrantless surveillance program to be submitted directly to Congress, preferably to the Intelligence Committees, in order to assure that the warrantless surveillance is limited to foreign intelligence surveillance while limiting the dissemination of classified information about the program and reducing the possibility of leaks.

The attacks carried out against the United States on 9/11 and our response to the new terrorists threats in the wake of that tragic day have demonstrated weaknesses in our intelligence gathering capabilities. Notable among these weaknesses is the cumbersome process to obtain the FISA warrants requisite to address intelligence opportunities presented by an all too nimble enemy. By reforming FISA to permit the necessary and constitutional use of warrantless foreign intelligence surveillance renewable for fixed periods of time, Congress can assure that the Executive Branch has the tools it needs to address the 21st century threats while providing the oversight necessary to assure that the program is not abused.

Thank you, Mr. Chairman.

Mr. COBLE. Thank you, Mr. Alt.

[The prepared statement of Mr. Alt follows:]

PREPARED STATEMENT OF ROBERT D. ALT

JOHN M. ASHBROOK
CENTER FOR PUBLIC AFFAIRS
Ashland University

Revising FISA to Address 21st Century Threats to National Security

Testimony Before
The House Judiciary Committee
Subcommittee on Crime, Terrorism, and Homeland Security

By
Robert D. Alt

September 6, 2006

Good afternoon Chairman Coble and Members of the Subcommittee. Thank you for the opportunity to testify. For the record, I am a Fellow in Legal and International Affairs at The John M. Ashbrook Center for Public Affairs at Ashland University, an independent educational organization. I am also a Fellow in Terrorism and Homeland Security at The Institute for Global Security Law and Policy at The Case School of Law, where I teach classes including criminal law and legislation. I am a graduate of the University of Chicago Law School and a former law clerk to Judge Alice M. Batchelder on the U.S. Sixth Circuit Court of Appeals.

The topic of today's hearing, "FISA in the 21st Century," addresses one of the most pressing legal issues arising from the ongoing war on terror. Since the *New York Times* revealed in December, 2005, that the President directed the National Security Agency ("NSA") to monitor communications of individuals who had contacts with suspected terrorists overseas without first obtaining warrants, speculation has swirled concerning the legality of the program. Among the most contentious legal issues raised to date concerning the program is the statutory question of whether the Foreign Intelligence Surveillance Act ("FISA"), Pub. L. 95-511, Title I, 92 Stat. 1796 (Oct. 25, 1978), codified as amended at 50 U.S.C. §§ 1801 *et seq.*, requires the executive to procure a FISA warrant before engaging in the wiretaps utilized by the NSA, or whether Congress alternatively authorized the President to conduct the warrantless surveillance by passage of the Authorization for Use of Military Force ("AUMF"), Pub. L. 107-40, 115 Stat. 224 (2001).

A strong argument can be made that the AUMF provides the authority necessary to carry out the NSA's surveillance program. In the AUMF, Congress authorized the President:

> to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.

AUMF, § 2. The question then is whether intelligence gathering of the kind conducted by the NSA constitutes "force." The Supreme Court provided some guidance on this question in *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004), in which it examined, *inter alia*, whether the AUMF, which does not specifically mention enemy combatants, nonetheless provides a statutory basis for the President to detain enemy combatants even in the face of the restrictions of the Anti-Detention Act. The plurality opinion of the Court held that "the detention of individuals falling into the limited category we are considering . . . is so fundamental and accepted an incident of war as to be an exercise of the 'necessary and appropriate force' Congress has authorized the President to use." *Id.* at 518 (O'Connor, plurality opinion). In support of the conclusion that detention is so fundamental and accepted an incident of war as to constitute "force," the Court cited to prior judicial opinions, a law review quoting a Nuremberg Military Tribunal opinion, and a Civil War Army field code, speaking respectively about the accepted wartime practice of detaining enemy combatants. *Id.* at 518-19.

In support of the NSA wiretap program, the administration has marshaled ample citations to the kind of authority relied upon by the Court in *Hamdi*. The Department of Justice ("DOJ") cites to numerous cases acknowledging both the practice and authority of the President to conduct electronic surveillance to protect national security, particularly during time of war or armed conflict. *See, e.g.*, U.S. Dept. of Justice, "Legal Authorities Supporting the Activities of the National Security Agency Described by the President," (Jan. 19, 2006) at 7-8. Furthermore, and directly relevant to *Hamdi's* analysis of whether the contested category is a fundamental and *accepted* incident of war, the DOJ Memo recounts the widespread acceptance and use of the practice of electronic surveillance at wartime dating back to the Civil War. *Id.* at 7-8 (quoting *United States v. United States District Court*, 444 F.2d 651, 669-70 (6th Cir. 1971) (reproducing as an appendix memoranda from Presidents Roosevelt, Truman, and Johnson); *id.* at 14-17 (quoting, *inter alia*, G.J.A. O'Toole, *The Encyclopedia of American Intelligence and Espionage* 498 (1988) (noting that as early as the Civil War, "telegraph wiretapping was common, and an important intelligence source for both sides"). The weight of the evidence in favor of considering signals intelligence as a fundamental and accepted incidence of war so as to constitute "force" is at least as strong as was the evidence in favor of considering detention "force" in *Hamdi*, and as such *Hamdi* provides strong support for the administrations position that the AUMF constitutes an adequate statutory fount of authority.

Some commenters have countered that FISA provides the exclusive means for conducting the kind of electronic surveillance at issue. *See, e.g.,* Letter from Curtis Bradley, Richard and Marcy Horvitz Professor of Law, *Duke University et al.*, to the Hon. Bill Frist, Majority Leader, *U.S. Senate* (Jan. 9, 2006). While federal law does state that the "procedures" outlined in FISA "shall be the exclusive means by which electronic surveillance . . . and the interception of domestic wire, oral, and electronic communications may be conducted," 18 U.S.C. § 2511(2)(f), FISA itself contains an exception for those who "engage[] in electronic surveillance under color of law . . . *as authorized by statute*." 50 U.S.C. § 1809(a)(1) (emphasis added). Again, it is instructive to look to *Hamdi*, in which the petitioner claimed that his detention was unlawful under the Anti-Detention Act, which states in relevant part that "[n]o citizen shall be imprisoned or otherwise detained by the United States except pursuant to an Act of Congress." 18 U.S.C. § 4001(a). The plurality opinion found that "the AUMF satisfied § 4001(a)'s requirement that a detention be 'pursuant to an Act of Congress' . . ." based upon its previous determination that enemy detention constituted such a fundamental and accepted incidence of war as to constitute force for the purposes of the AUMF. *Hamdi*, 542 U.S. at 517 (O'Connor, plurality opinion). Here, likewise, the AUMF constitutes authorization by statute permitting the President to engage in signals intelligence that is a fundamental and accepted incidence of war and thereby constitutes force for the purposes of the AUMF.

Another common argument is that reading the AUMF to authorize the wiretaps would repeal the exclusivity requirements of 18 U.S.C. § 2511(2)(f) by implication. However, by the very terms of the FISA and § 2511, no repeal by implication occurs. Section 2511 states in fuller measure that the:

> procedures in this chapter or chapter 121 or 206 of this title and the Foreign Intelligence Surveillance Act of 1978 [codified at 50 U.S.C. §§ 1801 et seq.] shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act [codified at 50 U.S.C. § 1801], and the interception of domestic wire, oral, and electronic communications may be conducted.

18 U.S.C. § 2511(2)(f). Accordingly, the procedures outlined in FISA (including as it must, according to § 2511's plain terms, FISA's express exemption from the regulatory scheme of electronic surveillance conducted according to statute) are the exclusive means by which electronic surveillance and the interception of domestic electronic communications may be conducted. There can be no repeal by implication where the allegedly "repealing" statute is contemplated, and indeed provided for, by the statute it is alleged to repeal. By incorporating the procedures of FISA, the exception found at 50 U.S.C. § 1809(a)(1) is as much a part of 18 U.S.C. § 2511(2)(f) as it would be if § 2511 included the phrase, "except as authorized by statute." Simply put, "the predicate for finding an implied repeal is not present in this case, because the . . . provisions of the two statutes are not inconsistent [.]" *Hagen v. Utah*, 510 U.S. 399, 416 (1994). This

reasoning applies equally to arguments suggesting that FISA must control under the rule that the specific controls the general—another rule for which conflict between the statutes is a predicate.

While the arguments in favor of the President's authority to conduct the NSA wiretap program pursuant to the AUMF in conjunction with FISA are strong, there is considerable debate on the matter. To clarify the effect of FISA on the NSA program, several bills have been offered, which are the focus of the hearing today. Some of the legislation seeks to implement FISA's warrant requirements as the sole method of conducting the NSA surveillance program (thereby effectively terminating the program), while some seek to provide the President with clearer statutory authorization under FISA itself to conduct the program. In deciding which course to take, this committee should be cognizant of two important points: first, the NSA wiretap program is needed as a practical matter to address emerging national security threats in a timely fashion; and second, the program is consistent with constitutional requirements for foreign intelligence surveillance.

Given the classified nature of the NSA program, the witnesses testifying today from the DOJ and NSA will presumably be better equipped to discuss the necessity for the executive branch to maintain continued flexibility in how it performs foreign intelligence surveillance. However, the need to streamline and modernize the procedures required by FISA to allow the executive branch to effectively combat the current terrorist threat is readily apparent even without such specific knowledge of the program. Notably, while some changes were made to the requirements for obtaining a FISA warrant after the terrorist attacks on 9/11, the process remains cumbersome and subject to bureaucratic delay, a fact that the 9/11 Commission noted its fact finding:

> Many agents in the field told us that although there is now less hesitancy in seeking approval for electronic surveillance under the Foreign Intelligence Surveillance Act, or FISA, the application process nonetheless continues to be long and slow. Requests for such approvals are overwhelming the ability of the system to process them and to conduct the surveillance.

National Commission on Terrorist Attacks Upon the United States, "Reforming Law Enforcement, Counterterrorism and Intelligence Collection in the United States," Tenth Public Hearing (Apr. 10, 2004). Accordingly, the well-worn argument that FISA's procedural burdens are light is belied by actual practice, and the related claim that the executive branch need only submit all requests for foreign intelligence surveillance to the FISA court turns out to be unduly burdensome.

This leads naturally to the second point, a discussion of constitutional considerations, because—notwithstanding the desire of the government to eliminate roadblocks to information gathering—our constitutional system imposes burdens on such practices in order to maintain a proper separation of powers, and to safeguard civil

liberties. For example, in the context of criminal law enforcement, the Fourth Amendment's general warrant requirement (subject to exceptions) prior to the execution of a search is one such burden that we place on the government. However, the courts have consistently acknowledged that the standards which the government must meet in order to conduct foreign intelligence surveillance, and the President's authority to conduct such surveillance, are constitutionally distinct from general criminal law enforcement.

In addressing the warrant requirement for domestic security matters, the Supreme Court in *United States v. U.S. Dist. Court for Eastern Dist. Of Mich.*, 407 U.S. 297 (1972) ("Keith") expressly avoided addressing national security surveillance with respect to the activities of *foreign* powers, and strongly suggested that warrantless surveillance, "though impermissible in domestic security cases, may be constitutional where foreign powers are involved[.]" *Id.* at 322 n.20. The courts which have addressed this issue appear to have agreed with this distinction. A recent decision by the FISA Court of Appeals noted that every court to have addressed the issue found that the President possesses the inherent constitutional authority to conduct warrantless searches for the purposes of obtaining foreign intelligence information:

> 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.

In re Sealed Case, 310 F.3d 717, 742 (Foreign. Intel. Surv. Ct. of Rev. 2002) (citing generally to *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir.1980)) (emphasis added); *accord United States v. Butenko*, 494 F.2d 593 (3d Cir . 1974) (en banc); and *United States v.* Brown, 484 F.2d 418 (5th Cir. 1973). *But see Zweibon v.* Mitchell, 516 F.2d 594 (D.C. Cir. 1975 (en banc) (suggesting in dictum without deciding that a warrant would be required in foreign intelligence investigations). These decisions are important for two reasons: first, they conform to the principle that the touchstone of Fourth Amendment jurisprudence is reasonableness rather than the formalism of warrants. *See, e.g., Vernonia Sch. Dist. v. Acton*, 515 U.S. 646, 653 (1995). Second, the cases are instructive concerning the scope of presidential power in foreign intelligence surveillance. Indeed, the last sentence of the FISA Court block quote above is telling, for it suggests that presidential authority is sufficient in the context of foreign intelligence surveillance even when the President's power is languishing at what Justice Jackson famously referred to as "its lowest ebb"—that is, when the President "takes measures incompatible with the expressed or implied will of Congress" and thereby "can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matters." *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 638 (1952) (Jackson, concurring).

Because reforming FISA is necessary to address emerging threats to national security, and because instituting procedures like those used in the NSA's wiretap program are consistent with the constitutional requirements for foreign intelligence surveillance, Congress should seek reforms to FISA which provide the executive with the kind of flexibility available to the executive in the NSA program, while maintaining adequate oversight to assure that the program is administered within the limitations of foreign intelligence surveillance.

In so doing, any legislation addressing FISA should seek to meet the following objectives:

1) Update the language of FISA to address changes in technology and in modes of communication.

2) Provide the President with the ability to conduct foreign intelligence surveillance for fixed, renewable periods of time without obtaining a FISA warrant.

3) Require renewals of the warrantless surveillance program to be submitted directly to Congress, preferably to the Intelligence Committees, in order to assure that the warrantless surveillance is limited to foreign intelligence surveillance, while limiting the dissemination of classified information about the program.

In formulating these reforms, there may be some temptation to wait for judicial determination of the NSA wiretap program. While a district court recently offered its opinion that the program is unconstitutional, Congress should not be dissuaded from acting on the FISA legislation while that case is pending. *See American Civil Liberties Union v. National Sec. Agency*, 2006 WL 2371463 (E.D. Mich. Aug. 17, 2006) (judgment stayed pending appeal). Without discussing the serious questions concerning the merits of this case, the district court clearly erred with respect to the question of standing, and failed to properly apply Supreme Court precedent which was directly on point. *See Laird v. Tatum*, 408 U.S. 1 (1972). It is extraordinarily likely that the district court's opinion will be reversed on appeal without the reviewing court reaching the merits. Given the difficulty in establishing standing, the legal status of the NSA wiretap program is not an issue which is easily reducible to judicial determination. Accordingly, it is necessary for the political branches to regulate themselves, and therefore it is imperative for Congress to take a fresh look at the FISA program.

Similarly, I am not convinced of the prudence of delegating determinations concerning permissibility of the NSA wiretap program to a commission, as some legislation proposes. First, the focus of the proposed commission's mandate appears to be largely retrospective, rather than prospective. The goal of Congress in reviewing FISA should be to establish clear guidelines going forward to assure that national security

interests are served and civil liberties are protected. Second, given the disagreement as to the proper reading of FISA and the AUMF, it is not clear that the commission would provide much new insight, rather than re-airing old arguments. This, combined with the statutorily-mandated parity of membership between the congressional majority and minority parties on the commission lends itself to the old Washington criticism that if you don't want something done, then create a blue-ribbon panel of experts. Third (and perhaps most important), given the national security issues at stake in the wiretap program, efforts should be made to keep tight controls over the dissemination of information in the course of oversight. The creation of the commission necessarily adds another bureaucratic layer to the oversight regime, and thereby increases the possibility of leaks. It would be better for those who are empowered to make changes to the program—i.e., members of Congress via the Intelligence Committees—to directly monitor the program, rather than to indirectly be apprised of its retroactive effects.

Conclusion

The attacks carried out against the United States on September 11, 2001, and our response to the new terrorists threats in the wake of that tragic day have demonstrated weaknesses in our intelligence gathering capabilities. Notable among these weaknesses is the cumbersome process to obtain the FISA warrants requisite to address intelligence opportunities presented by an all too nimble enemy. By reforming FISA to permit the necessary and constitutional use of warrantless foreign intelligence surveillance renewable for fixed periods of time, Congress can assure that the executive branch has the tools it needs to address 21st century threats, while providing the oversight necessary to assure that the program is not abused.

Mr. COBLE. Mr. Dempsey.

TESTIMONY OF JIM DEMPSEY, POLICY DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. DEMPSEY. Mr. Chairman, Mr. Scott, Mrs. Harman, Members of the Committee, good afternoon. Thank you for this opportunity to testify at today's hearing.

I will focus most of my attention on the Wilson-Sensenbrenner bill, because it is clearly the majority's preferred bill in this Chamber and because I think it has been the subject of inaccurate reporting, including in today's *Washington Post.*

Simply put, the Wilson bill would permit the NSA's vacuum cleaners to be turned on international and purely domestic calls and e-mails of U.S. citizens. That is not modernization; that is a major step backwards. If we are ever going to win this war on terrorism, we need to focus our intelligence agencies, not cut them loose from checks and balances.

The Wilson-Sensenbrenner bill would vastly expand the scope of warrantless surveillance inside the United States, and we would create a vast database of information on U.S. citizens, which the Administration could datamine at will outside any judicial or congressional oversight in a fashion reminiscent of the Total Information Awareness program.

The Wilson-Sensenbrenner bill, in our view, is every bit as dangerous as the Specter-Cheney bill. Both would authorize broad, warrantless surveillance of U.S. citizens inside the United States. Both would not only ratify the President's program, but would authorize warrantless surveillance far beyond what the President is doing. Both would make warrantless surveillance the rule not the exception.

While the Wilson bill would nominally preserve FISA as the exclusive means for conducting surveillance inside the United States, it would exempt so much domestic gain from the act as to effectively repeal FISA.

Now, in order to understand the impact of the Wilson bill, it is necessary to appreciate that much of the weight of FISA is carried by the definitions section, and for our purposes today the most important definition is the definition of "electronic surveillance." Under FISA, if the collection of information fits within the definition of "electronic surveillance," it requires a court order or must fall under one of FISA's exceptions.

If the collection of information is excluded from the definition of "electronic surveillance," then it is not covered by the Act. It can be carried on without a warrant, without reporting to Congress, without compliance with the minimization requirement of the statute. And that is what the Wilson bill does.

The Wilson bill takes the definition of "electronic surveillance," carves out large categories that the average person would call wiretapping and places them outside judicial and congressional oversight of the Act, outside the minimization requirements, and outside other provisions of the Act.

First, the bill would make the President's warrantless surveillance program legal and exempt it from judicial scrutiny by defining what the President is ordering as not to be "electronic surveil-

lance." Here I am referring to the publicly admitted program of intercepting calls with one leg in the United States and one leg overseas where the Government is targeting suspected terrorists.

The bill says that targeting calls into and out of the United States is not terrorism if you are targeting someone overseas. The problem with that is—and the constitutional flaw that I saw in that is—there are two parties to the call, and one of them is in the United States and might be a citizen. That person might be a journalist, it might be a relative, it might be an aid worker, it might be some dupe, it might be any number of kinds of innocent people, American citizens whose conversations would be wiretapped without court order under this bill.

Secondly, the bill would authorize a program of warrantless surveillance far broader than what the President has been conducting. The President has assured the American public that his program is targeted against specific members of al-Qaeda overseas calling into the United States.

The bill before you, the Wilson bill, would authorize warrantless surveillance of all international calls, calls into and out of the United States, by saying that if you are not targeting someone, but if you are sweeping up everything, then it is not electronic surveillance; therefore, it is outside the coverage of the act.

So this means that under this bill, for the first time ever, NSA would be able to train its vacuum cleaner on the contents of all international calls, all e-mails that have a recipient overseas, recording every single one so long as it was not targeting a specific person in the United States. Then they could go back to that database and target later and extract whatever they wanted. That would not be considered electronic surveillance under this bill.

Third, the bill would allow the vacuum cleaner of the NSA to be turned on information concerning the purely domestic calls of U.S. citizens. The bill would allow the NSA to scoop up and would require the telephone and Internet companies to turn over to the Government all records of all calls and e-mail in the United States, purely domestic-to-domestic—not the content of the calls—but to collect the information about who's calling whom and to keep that information forever and to analyze it and datamine it without any judicial approval.

Fourth, in its amendment to section 1802 of FISA, the bill would go farther than the President has gone by allowing warrantless surveillance of the content of domestic telephone calls so long as it is, quote, "solely directed at the acquisition of the content of a foreign power or a person suspected—a non-U.S. person suspected of being an agent of the foreign power."

Again, the problem is, many of those calls, domestic calls, will have a U.S. citizen on one end of them. And so again we will be intruding upon the privacy of U.S. citizens in the U.S. making or receiving a domestic call, without court order.

And fifth, the Wilson bill would authorize surveillance of purely domestic calls for a period of 45 days, renewed indefinitely after a terrorist attack.

Mr. COBLE. Are you about at the end of your line of your extended time? If you could wrap up.

Mr. DEMPSEY. Yes. Mr. Chairman, I think we have before us a complicated bill. It is hard to parse, and I heard Mr. Bradbury say in his remarks that the Administration was planning yet further suggestions on further changes to the bill, which says to me this cannot possibly be marked up and dealt with in this Congress. If—I think it's hard to understand this bill as it is. The changes are sweeping, radical; and to have yet further things in the works that will come in in conference or something like that, or wrapped into some kind of omnibus, I think is very dangerous in a time of war, when we have before us a constitutional framework, and to start changing that so radically I think is dangerous not only from a civil liberty standpoint, but also from a national security standpoint.

[The prepared statement of Mr. Dempsey follows:]

PREPARED STATEMENT OF JAMES X. DEMPSEY

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

before the

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

"Updating FISA"

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

September 6, 2006

Chairman Coble, Ranking Member Scott, Members of the Subcommittee, thank you for the opportunity to testify today.

Is "Modernization" Another Way of Saying Warrantless Searches and a Blank Check for the President?

Undoubtedly, it is appropriate to consider from time to time whether the Foreign Intelligence Surveillance Act should be amended to respond to the changing threats facing our nation or advances in technology. However, FISA has been updated already several times since 9/11, most notably in the recently reauthorized PATRIOT Act.

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

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

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

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

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

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

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

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

Congress can best update FISA – if it needs updating -- only after further hearings, focusing on the problems publicly identified by the Administration. Updating FISA in a way that is Constitutional and responsive to the Administration's needs will require an iterative process of in-depth analysis (some of it necessarily classified) and public dialogue.

The threat of terrorism demands such a careful response. Of course, the government must have strong powers, including the authority to carry out various forms of electronic surveillance. However, not only to protect constitutional rights but also to ensure effective application of those powers, government surveillance must be focused. That focus can best be achieved through a system of checks and balances, implemented through executive, legislative and judicial review.

In addition, any modernization of FISA should be open not only to ways in which the Act may unduly burden intelligence gathering but also to ways in which its controls need to be tightened in light of modern realities. The standards of the surveillance laws, weak in some key respects before 9/11, have been eroded by the PATRIOT Act, by Executive Branch actions, and most dramatically by the evolution of technology, which has made more and more personal information readily accessible to the government. A number of steps – none of them in current proposals -- could be taken to improve FISA compliance, accountability, oversight and transparency.

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

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

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

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

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

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

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

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

How The Revised Definitions Expand Warrantless Surveillance

Probably 30% of the meaning of FISA is buried in its definitions, especially its definition of "electronic surveillance" and "minimization procedures." The changes made by Wilson-Sensenbrenner-Hoekstra to these two definitions, and the changes to Section 102 of FISA, would authorize large-scale warrantless surveillance of American citizens and the indefinite retention of citizens' communications for future datamining.

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

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

"(f) 'Electronic surveillance' means—

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

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

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

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

~~(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of title 18;~~

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

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

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

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

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

---

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

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

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

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

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

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

How the Amendments to FISA Section 102 Expand Warrantless Surveillance

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

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

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

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

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

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

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

Reducing Judicial Oversight By Reducing The Detail In FISA Applications

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

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

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

Reducing Political Accountability

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

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

Expanding Emergency Taps

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

Expanding Non-Emergency Taps

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

Authorizing Warrantless Surveillance After an Armed Attack and After Terrorist Attacks

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

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

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

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

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

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

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

Other Provisions

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

Chairman Specter's Legislation Would Turn Back the Clock to an Era of Warrantless Domestic Surveillance

Since last December, the President, the Attorney General, and other senior Administration officials have stated that the President's program of warrantless wiretapping is narrowly focused on international calls of suspected terrorists, that the program is used in circumstances where immediate monitoring is necessary for some short period of time, that domestic calls are not covered, and that in every case there is reasonable ground (or "probable cause") to believe that the target is associated with al Qaeda. The Administration has repeatedly assured lawmakers and the public that it is not engaged in a program of "domestic surveillance."

Chairman Specter has negotiated with the Administration a bill that would

turn back the clock, not only by repealing FISA's exclusivity provision but also by authorizing a domestic program far broader – and far more intrusive on the privacy of American citizens -- than the one the President and Attorney General have described.

Section 4, the Supposed Core of the Specter Bill, Is Unnecessary

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

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

Second, the Chairman's bill does not bind this President to submit for judicial review future programs nor does it require future Presidents to submit their programs for court review – programs that may be substantially different from this President's program.

Third, the definitions used in Chairman Specter's bill might fail to give the FISA court jurisdiction to review the President's program:

- The President has said that his program only allows short term monitoring, but Chairman Specter's bill applies *only* to programs of long term monitoring.
- The Attorney General has said that in every case, the President's program targets a specific suspected member or affiliate of al Qaeda, but Chairman Specter's bill applies *only* when it is not possible to specify who is being targeted.

Finally, even assuming that Chairman Specter's bill would allow the FISA court to review the President's program, the bill imposes no consequences on the Administration should the Court refuse to approve the President's program. Unlike FISA, which states that surveillance begun without court approval must cease if the surveillance is later found to be unjustified, the Chairman's bill does not say that the government must cease programmatic activity that the court refuses to approve.

What did it take to get the President to agree to submit his program to judicial review? It took a radical rewrite of FISA: the authorization of a broad new category of domestic surveillance, under "programmatic" or "general search" warrants; the repeal of FISA's exclusivity provision, making the entire statute, including Chairman Specter's amendments, merely optional; the repeal of FISA's wartime exception, granting the President a blank check in domestic surveillance; and, in Section 9, major new exceptions to the warrant requirement for communications to which Americans are a party.

Sections 5-6 –General Warrants

Sections 5 and 6 of Chairman Specter's bill would authorize (but not require) the Administration to apply for, and the FISA court to grant, "general warrants," which are prohibited by two key provisions of the Fourth Amendment: particularity and probable cause.

With a general warrant, Chairman Specter's bill would authorize a program of domestic surveillance far broader than President Bush's program. The Attorney General has said that the President's program targets only communications with particular suspected members or affiliates of al Qaeda, only on the basis of probable cause, and only if one leg of the call is with a party overseas. The latest version of Chairman Specter's bill would authorize seizing the contents of purely domestic calls of American citizens without probable cause, without specific suspicion, and where the call has nothing to do with al Qaeda and not even anything to do with terrorism.

The substitute is especially broad because it allows interception intended to collect the communications not only of suspected terrorists but also a person who "is reasonably believed to have communication with or be associated with" a terror group or suspected terrorist. This means that a journalist who interviews a suspected terrorist, and doesn't even know that the person is considered a terrorist, could be subject to surveillance under this bill. Also, there is no limit on "associated with." Is one "associated with" a suspected terrorist because one goes to the same mosque? Is one "associated with" a suspected terrorist because one has roots in the same village or neighborhood? These connections may be worth checking out, but they are not adequate basis for content interception, which has always been considered one of the most intrusive forms of government invasion of privacy.

Also, Chairman Specter's bill does not use the Constitutional concept of probable cause. It actually does not specify the standard the court must use in determining whether the government has made the requisite showings. Instead, the substitute states that the court must find that the program is "reasonably designed" to intercept the communications of suspected terrorists or persons "reasonably believed [by whom it doesn't say] to have communication with or be associated with" suspected terrorists.

Invoking the FISA court's approval is purely optional under the substitute. Unlike the original version of Chairman Specter's bill, the substitute does not require the Administration to submit the President's warrantless surveillance program or any future program for judicial review.

Chairman Specter's bill, unlike FISA, requires either that a "significant purpose" of the program be the collection of foreign intelligence or that its purpose be to "protect against international terrorism," which means that the program can be used when its sole purpose is the collection of criminal evidence

While initial court approval of a program would be for up to 90 days, the court could renew the program for any length of time it deems reasonable.

Section 8 The Repeal of FISA's Exclusivity Provision ***Is*** *Significant*

Section 8 of Chairman Specter's bill would repeal the exclusivity provisions of FISA and allow the President to choose, at his discretion, between using FISA and pursuing some other undefined and constitutionally questionable method to carry out secret surveillance of Americans. This provision would turn back the clock 30 years ago, inviting a return to the era of COINTELPRO and the intelligence-related abuses that created confusion and drove down morale inside the intelligence agencies.

Repeal of exclusivity is not meaningless, for the whole purpose of the exclusivity clause is to constrain any "inherent power" the President has to carry out electronic surveillance in the absence of Congressional action. Indeed, in 1978, this very Committee stated in its Report on FISA that, "even if the President has 'inherent' constitutional power to authorize warrantless surveillance for foreign intelligence purposes, Congress has the power to regulate the exercise of this authority by legislating a reasonable warrant procedure governing foreign intelligence surveillance."[6]

In its recent opinion in *Hamdan v. Rumsfeld*, the Supreme Court majority noted, "Whether or not the President has independent power, absent congressional authorization, to convene military commissions, he may not disregard limitations that Congress has, in proper exercise of its own war powers, placed on his powers." Justice Kennedy, in his concurrence, explained why it is both constitutional and desirable for the Congress and the President to work together to devise a consensus set of rules for the exercise of national security powers and why the President is bound by those rules enacted by Congress:

> This is not a case, then, where the Executive can assert some unilateral authority to fill a void left by congressional inaction. It is a case where Congress, in the proper exercise of its powers as an independent branch of government, and as part of a long tradition of legislative involvement in matters of military justice, has considered the subject of military tribunals and set limits on the President's authority. Where a statute provides the conditions for the exercise of governmental power, its requirements are the result of a deliberative and reflective process engaging both of the political branches. Respect for laws derived from the customary operation of the Executive and Legislative Branches gives some assurance of stability in time of crisis. The Constitution is best preserved by reliance on

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

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

There is no doubt about it: repeal of exclusivity would restore to their full, albeit undefined scope, the President's inherent powers to conduct surveillance, turning back the clock to the era of uncertainty and abuse.

The Specter- Feinstein Bill Takes a More Targeted Approach

It is important to note that Senator Feinstein is one of the members of the special Senate Intelligence Subcommittee that received classified briefings about the President's program(s). After receiving the briefings, she concluded that the appropriate legislative response would be a bill narrowly focused on the issues the Administration said caused it to circumvent FISA-namely, the need for more resources, greater speed in approving FISA applications and more flexibility to begin wiretapping in an emergency. Significantly, Senator Feinstein remained convinced after receiving classified briefings that the program(s) can and should be conducted under FISA.

The Specter-Feinstein bill responds to the Administration's public testimony to date. As we understand the Attorney General's testimony, the sole reason the administration could not use FISA was that the emergency procedure was not flexible enough. This bill addresses that issue by providing more resources to the FISC, DOJ, FBI, and NSA and allowing the Attorney General to delegate the power to approve applications and to authorize surveillance in emergencies.

The most important aspect of this bill is its reaffirmation that FISA and Title 18 are the exclusive means by which the government can conduct electronic surveillance. The bill reinforces this by prohibiting the appropriation of funds for electronic surveillance outside of FISA or Title 18 and by stating that if Congress intends to repeal or modify FISA in future legislation, it must expressly state in the legislation its intention to do so.

Specter-Feinstein would:

- reaffirm the exclusivity provisions of FISA and Title 18;
- prohibit the appropriation of funds for any electronic surveillance conducted outside of FISA or Title 18;
- enhance congressional oversight;
- extend the FISA emergency period from 72 hours to 7 days;
- allow the Attorney General to delegate authority to approve FISA applications and to authorize emergency surveillance;
- give the FISC, DOJ, FBI and NSA the ability to hire more staff as necessary to meet the demands of the application process;

---

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

- give the Chief Justice of the United States the power to appoint additional judges to the FISC, as needed;
- mandate the development of a document management system to expedite and facilitate the FISA application process; and
- make "authorization for the use of military force" and the declaration of a "national emergency" events that trigger the FISA wartime exception.

The Administration's Testimony To Date Has Merely Reaffirmed the Enduring Value of FISA's Core Principles

FISA contains five basic principles, each of which is independent from the others, and prior to today the Administration has not made a case for altering any of them:

- Except in emergency situations, the government must obtain **prior judicial approval** to intercept communications inside the US.
- **Congress carefully oversees** surveillance activity within the US, which presumes that Congress is fully informed of all surveillance activity.
- The interception of the content of communications is **focused on particular individuals** suspected of being terrorists or particular physical or virtual addresses used by terrorists.
- The threshold for initiating a content interception is **probable cause** to believe that the target is a terrorist and that the interception will yield intelligence.
- The rules laid down publicly in statute are the **exclusive means** for carrying out electronic surveillance within the US.

So far, on the first question, the Administration has offered on the public record no reason for dispensing with prior judicial approval, except in emergency cases for short-term surveillance.

Other than its philosophical antipathy to Congressional oversight, the Administration has offered no substantive reason for not seeking the support and oversight of Congress.

In terms of particularized suspicion, on the record so far the Administration has consistently emphasized that all interceptions of content under the President's Terrorist Surveillance Program are based on particularized suspicion.

In terms of probable cause, the Attorney General emphasized in Congressional testimony that the Administration is adhering in the Terrorist Surveillance Program to the probable cause standard.

On the question of exclusivity, twice the Supreme Court has rejected the Administration's extreme views of executive power, and, in any case, for a variety of reasons, intelligence activities are most effectively sustained when they are carried out on the basis of a public consensus between Congress and the Executive Branch.

FISA Has Well-Served Both Civil Liberties and the National Security

FISA has well-served the nation for nearly 30 years, placing electronic surveillance inside the United States for foreign intelligence and counter-intelligence purposes on a sound legal footing. Tens of thousands of surveillance orders have been issued under FISA, and the results have been used in hundreds of criminal cases, and never once has a constitutional challenge been sustained.[8]

Changing FISA in the radical ways now being proposed would jeopardize this certainty and could harm the national security. It would cast a cloud of constitutional doubt over intelligence gathering. Those in the government and the private sector who carry out electronic surveillance would no longer be assured their actions were lawful. Hesitation and second-guessing could inhibit risk-taking. In the absence of mandatory court review, internal doubts might arise more frequently about the legality of a program, but those with concerned might see no other option except to publicly leak the existence of the program in order to force its reconsideration. If the Administration did find a terrorist through surveillance under a radically different FISA, that person might escape conviction and imprisonment if the evidence against him were rejected on constitutional grounds.

FISA Has Already Been Updated

In the PATRIOT Act and in other legislation since 9/11, Congress has already "modernized" FISA. In signing the PATRIOT Act in 2001, President Bush specifically concluded that it would modernize FISA:

> We're dealing with terrorists who operate by **highly sophisticated methods and technologies**, some of which were not even available when our existing laws were written. The **bill before me takes account of the new realities** and dangers posed by **modern terrorists**. ... This new law that I sign today **will allow surveillance of all communications** used by terrorists, including e-mails, the Internet, and cell phones. As of today, we'll be able to **better meet the technological challenges** posed by this proliferation of communications technology.[9]

Four and half years later, when the PATRIOT Act's sunsetting provisions were reauthorized, the Justice Department concluded on the basis of its record that the PATRIOT Act had done its job in modernizing FISA and other laws:

---

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

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

> The USA PATRIOT Act, enacted on October 26, 2001, has been critical in preventing another terrorist attack on the United States. It brought the federal government's ability to investigate threats to the national security into the modern era—by modifying our investigative tools to reflect modern technologies … .[10]

In contrast, recent proposals seem intended not to "modernize" FISA, but to cast aside fundamental Fourth Amendment protections simply because the government has too much communications information available to it for easy interception.

Public Congressional Hearings Led To Enactment of FISA, and Should be the Prerequisite for Any Major Changes

Congress can examine FISA publicly without compromising national security. Of course, some elements of the inquiry will have to be conducted in secret, with in-depth staff involvement, but once Congress has the full picture it can and should conduct public hearings with Administration witnesses taking the lead. Indeed, Congress did this successfully thirty years ago: FISA was the product of exhaustive public hearings. The debate on FISA was full and robust. There were years of fact-based hearings and extensive staff investigations into the complete facts about spying on Americans in the name of national security. Multiple committees in both Houses considered the legislation in both public and closed hearings. There was extended floor debate as well. The secrecy of electronic surveillance methods was preserved throughout.

Congress cannot determine whether or how to change FISA without a thorough understanding of what the Administration is doing domestically and why it believes the current law is inadequate. The Administration must explain to Congress why it is necessary to change the law, and Congress must satisfy itself that any recommended changes would be constitutionally permissible. As Chairman Hoekstra recently said in his letter to the President, "Congress simply should not have to play Twenty Questions to get the information that it deserves under our Constitution."

Technological Changes Improve the Government's Surveillance Capabilities and May Justify Tighter Controls

The digital revolution has been a boon to government surveillance. The proliferation of communications technologies and the increased processing power of computers have made vastly greater amounts of information available to the government. In some respects, digital communications are easier to collect, store, process and analyze than analog communications.

---

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

If FISA is ill-suited to the new technology, it is because its standards are too weak and the vacuum cleaner technology of the NSA is too powerful when aimed domestically, given the reliance of so many ordinary Americans on the Internet, its global nature, and the huge growth in the volume of international communications traffic on the part of ordinary Americans. Given the post-9/11 loosening of regulations governing intelligence sharing, the risk of intercepting the communications of ordinary Americans and of those communications being misinterpreted by a variety of agencies as the basis for adverse action is vastly increased. This context requires more precise—*not looser*—standards, closer oversight, new mechanisms for minimization, and limits on retention of inadvertently intercepted communications.

Improving FISA Compliance, Transparency, Accountability and Oversight

There are a number of steps Congress could take improve to FISA compliance, accountability, oversight and transparency, including facilitating district court review of FISA surveillance when the government uses FISA evidence in criminal cases, providing notice to individuals who have been FISA targets and who turn out to be innocent, and developing procedures for handling judicial challenges to surveillance short of invoking the state secrets doctrine.

Conclusion

Mr. Chairman, Members of the Subcommittee, we urge you to look on this as a process that will take some time. Any changes to FISA should be narrowly crafted to meet specific problems identified by the Administration. Equal attention should be given to ways in which civil liberties safeguards should be strengthened as well as to ways in which procedures can be streamlined.

Mr. COBLE. We have been joined by the distinguished gentlelady from California, Ms. Waters, and the distinguished gentlelady from Texas, Ms. Sheila Jackson Lee. I did not officially recognize the distinguished gentleman from California, Mr. Lungren.

Gentlemen, we impose the 5-minute rule against us as well. So if you could keep your questions short, we would appreciate that.

Start my time, if you will, Beth.

The Foreign Intelligence Surveillance Court of Review in 2002 pointed out that, quote, "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," and further quoting, "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," close quote.

Was the Foreign Intelligence Surveillance Court of Review correct when it said that FISA cannot encroach on the President's constitutional authority?

Mr. Deitz, let me put that to you.

Mr. DEITZ. I would defer to Mr. Bradbury, but I would concur with that statement.

Mr. COBLE. Mr. Bradbury, do you want to take the baton?

Mr. BRADBURY. Yes, we do agree with that statement. Statutes do not take away constitutional authority.

Mr. COBLE. Both the Wilson bill and the Specter bill attempt to streamline FISA.

Do you believe that is necessary that we further streamline FISA, Mr. Alt; and why, if you do agree?

Mr. ALT. Once again, in some ways, I would defer on some of the technological points to the DOJ and NSA representatives here today, but I did note in the Wilson bill they did actually clean up some of the language on some of the technological components, and that, I would presume, is a step forward.

But streamlining the overall procedures in terms of getting a warrant and permitting the President the flexibility to obtain foreign intelligence surveillance without needing to go through the onerous process of getting a warrant, particularly after a time of war or attack on the U.S., I think is very necessary.

I would also agree with the DOJ representative. My one recommendation would be, I don't think that necessarily that trigger should be based upon an attack on the United States. I think that the President needs greater flexibility to be able to anticipate attacks, anticipate potential attacks, and not simply respond to those attacks once they have happened.

Mr. COBLE. Mr. Bradbury, do you want the baton again to extend on that?

Mr. BRADBURY. Yes.

As stated in my testimony, Mr. Chairman, we certainly agree that it is important to streamline the application process. We don't need more lawyers in the process or more bureaucracy. We need to streamline the process, make it more flexible, make it more usable in the war on terror. And I think that is a very important part of the legislation that Representative Wilson has introduced and also that Senator Specter has introduced, and it really is something

that I know that the National Security Agency has long been interested in.

Mr. COBLE. Mr. Deitz, let me extend that a little bit. Again, alluding to the Wilson and the Specter bills, both bills change the definition of electronic surveillance. Do you agree with that proposal and why?

Mr. DEITZ. Yes, Mr. Chairman, we do. And, again, the reason is that the 1978 FISA Act involved a certain set of technologies, and those technologies have changed, and one of the things that we would like, that NSA and analysts need, is a technology neutral bill in which the FISA Act—amended FISA Act gets to the point of Fourth Amendment protections, isn't tied to a particular kind of technology. Yes, sir.

Mr. COBLE. Now, Mr. Dempsey contends that the Wilson bill and the Specter bill call for warrantless surveillance over domestic—over both domestic and international calls. Do you agree with that, Mr. Deitz?

Mr. DEITZ. No. And I don't really understand—I don't understand where that—how he is interpreting them that way.

What we have tried to do in working with Mr. Bradbury and his folks and the CIA and so forth is to try to focus the bill on—in the interest you are trying to protect. The only way you can get a U.S. person in an unwarranted fashion is by an intention to tap a foreigner, and if that foreigner happens to be speaking to an American, then you do pick up that conversation. However, that happens today and the procedures are designed to what is called minimize those intercepts. So there is nothing new about them. Minimization would continue to apply under this legislation, under the Wilson and Specter legislation.

Mr. COBLE. Well, my red light is about to appear. Mr. Dempsey, I will give you a chance subsequently if no one else gives you a chance to elaborate on that.

The distinguished gentleman from Michigan, Mr. Conyers, is recognized for 5 minutes.

Mr. CONYERS. Thank you, Mr. Chairman; and I thank all the witnesses for being as helpful as they can. But let's just go back to Mr. Deitz, who said he doesn't understand why Mr. Dempsey would suggest that both under the Specter and Wilson bills that warrantless wiretapping would be permitted in the United States. Could you clear that up so that we can make sure this record has got it straight?

Mr. DEMPSEY. Mr. Chairman, I was—the new definition of electronic surveillance would say that for calls where one leg is in the United States and one leg is overseas, that is calls very likely involving a United States citizen, that a warrant is not required, that it is not electronic surveillance if you are targeting a person overseas. That is, you want to get—initially, you are focusing on the target overseas, but you are picking up the calls to the United States in the United States, and you are, therefore, picking up, intercepting the calls of U.S. citizens. Under the bill, that is defined as not being electronic surveillance and does not require a court order. I think that that should, because the rights of the American citizen on the other end of that call are clearly at issue.

Mr. CONYERS. I think that that to me is the very uncontroversial understanding and implications of that procedure.

But let me ask Mr. Bradbury this. Why can't we get FISA orders under the current law? I mean, what is wrong with the situation right now?

Mr. BRADBURY. Congressman, are you referring to the terrorist surveillance program——

Mr. CONYERS. Yes.

Mr. BRADBURY.—the President has authorized? In a word—two words—speed and agility, the need for speed and agility. The purpose of the program is to create an early warning detection system when anyone associated with al-Qaeda—we have reason to believe is a member or agent of al-Qaeda.

Mr. CONYERS. What about 72 hours? That is not speedy enough?

Mr. BRADBURY. The 72 hours emergency authorization provision still requires the Attorney General, before surveillance can begin, to make a determination that all of the requirements of FISA are met. So it requires a mini-FISA approval process that goes up through layers of lawyers.

Mr. CONYERS. But that isn't in the law. This self-imposed bureaucracy of which you complain has not been put into the law. And so what we have here is, after 25 changes in the FISA law and many of them recommended by the Administration, you still come to us saying that it is too long. Now, what about extending the 72-hour emergency period to 5 days or to 7 days? What do you think of that?

Mr. BRADBURY. We think extending it to 7 days is a good idea.

Mr. CONYERS. Well, thank you very much. Because the Harman bill, with Conyers attached on—as well, House Resolution 5371—does just three things that I hope doesn't raise any quarrels with you.

It reiterates that foreign intelligence surveillance must be conducted within FISA as written, including obtaining a warrant whenever there is a possibility that a United States person will be tapped; two, it allows the Administration to make any internal procedural changes necessary to make applying for a FISA order quicker and easy—easier; and, three, it appropriates whatever funds are necessary to make sure the Justice Department can seek as many court wiretapping orders as they see fit.

Do you have any objections to any of those provisions?

Mr. BRADBURY. Congressman, that legislation will not enable the program to continue as it is currently operated if the program were required to be maintained only under the provisions of FISA as currently written, and we think simply adding more lawyers and more bureaucracy is not—and more money is not the answer for the need for speed and agility in this program.

Mr. CONYERS. So giving you more resources won't make it speedier or work more effectively.

Let me turn to Mr. Dempsey to see if we can find out what else the Harman-Conyers LISTEN Act might do to help facilitate this. After all, we are going the extra mile. The only thing we ask is that it is done within the FISA law; and you keep saying that if we gave you all the lawyers we wanted, if we expedited the procedure end-

lessly, it still wouldn't be so hot. We have got to be able to go around the FISA law. What makes that so important?

Mr. COBLE. Well, Mr. Dempsey, if you could wrap up—the gentleman's time is expired—you could wrap up, we have a lot of questions remaining.

Mr. DEMPSEY. I would say at this time, Mr. Conyers, I have always thought that the Attorney General authority for emergency wiretaps could be downward delegated. It, in my view, doesn't have to be personally exercised by the Attorney General.

On my latest reading of the Wilson bill, I actually didn't see that in the Wilson bill. Maybe I missed it. To me, that was one of the changes that directly responded to what the President has said was his problem, that it has to go all the way up to the Attorney General personally and he personally has to make the determination. I think that can be downward delegated with some limitations.

The President has said it is still probable cause. The President has said we are targeting individuals. At that point there, you are meeting—you are targeting members of al-Qaeda. At that point there, you meet the standards of FISA. You can go to the court after the 72 hours or 5 days.

Mr. CONYERS. Thank you so much. Thank you, Mr. Chairman.

Mr. DEITZ. Mr. Chairman, could I just add a quick response to Mr. Conyers' question?

Mr. COBLE. Let me move along. I will get to you, Mr. Deitz, before we go on.

In order of appearance, I recognize the distinguished gentleman from Ohio, Mr. Chabot, for 5 minutes.

Mr. CHABOT. Thank you, Mr. Chairman.

Mr. Deitz, if you want to briefly respond, you can do it on my time.

Mr. DEITZ. Thank you very much. I appreciate that.

The problem with the 72-hour rule, as Mr. Bradbury said, A, it is not a freebie. It is not you get to do whatever you want for 72 hours. From the moment you want to put on an emergency FISA, you need to have the wherewithal to create probable cause.

My concern is not lawyer time, although that is precious enough. My concern is analyst time, and the issue that most concerns us is your counterterrorism experts and analysts do not grow on trees. Every time I have got 5 or 10 or 15 or 20 counterterrorism experts working FISA factual issues, that is time when they are not trying to stop the enemies of the United States.

The second thing, if I may say so—and I appreciate your indulgence—there is a notion that every time an American is being intercepted, that is under FISA. That is simply not true, and it is important that we not pretend it is true. Every day we pick up lawfully conversations to, from or about U.S. persons that are not under FISA warrant, and that nobody has ever thought they ought to be under FISA. This is simply the way the system was set up.

We are obligated to do what is a term of ours, is minimization. That is, we take that information and put—take it out of the intercept and put, bracket, U.S. person number one, closed bracket, or U.S. person number two, and only in unusual circumstances are those identities made known. So I am just trying to eliminate this

notion once a U.S. person is involved all of a sudden there is a FISA warrant obligation. There simply isn't.

Thank you, sir.

Mr. CHABOT. Thank you.

Mr. Bradbury, let me turn to you, if I can. You had mentioned in your opening statement the plot to blow 10 to 12 British airliners out of the air which was uncovered quite recently. I think the whole world was focused on this and rightly so, because an awful lot of lives, perhaps more than were lost on September 11, were at risk, and this was, my understanding, a very serious plot.

To the extent that we are able to discuss it in this forum—and we obviously can't reveal secrets which might let the terrorists understand how we acquire this type of information—but could you just give us your opinion or perhaps let us know—what we are talking about here today can sometime become a good, esoteric—and may not be real relevant. But could you tell us how what we are talking about here today actually can affect something like that and how it may prevent something like that from actually happening somewhere down the road.

Mr. BRADBURY. Well, Congressman, I can't talk about that particular case, but I can say that, obviously, U.S. intelligence experts, U.S. intelligence services cooperate with the intelligence services of our allies around the world, including the British, a key ally to the United States; and this program is one program that enables our intelligence experts to get some of the most valuable and current intelligence information in real time. So to the extent it contributes to our knowledge and to the extent our knowledge can lend assistance to the intelligence efforts of our allies, it is a critical part. It is a link in that chain.

Mr. CHABOT. Okay, thank you.

Mr. Deitz, let me ask you, the idea that Mr. Dempsey was talking about before, that, you know, sometime—he was saying that sometimes both ends of this are domestic, when in fact it is my understanding that we are talking about somebody here in the United States and a terrorist-connected person in Pakistan or Saudi Arabia or Afghanistan or somewhere else. And sometimes you hear people that say, well, they are just using that excuse that they are al-Qaeda connected. We really don't know that. Could you touch on that and how in real life how that actually is determined?

Mr. DEITZ. I'd be glad to.

The first thing I'd say, Mr. Congressman, is we don't have a vacuum cleaner at NSA and we haven't for years and years and years. There is simply too many conversations, too many minutes to vacuum. I think General Hayden testified at one point that there are 2 billion minutes of long distance phone calls a year. We simply don't have the resources to grab all that. So the vacuum cleaner metaphor is simply not useful.

What we do—and this is all based on probable cause—I assume we are speaking of the President's program, sir—always based on probable cause. Do our analysts have probable cause to believe that one end of a conversation is a member of al-Qaeda or affiliate?

And those terms are robustly defined. That simply isn't a decision of one person. There is a chain of command there. There is a set of protocols that must be satisfied in order for a shift supervisor

to agree, yes, you have satisfied the conditions to intercept this person. Once that intercept takes place, the conversations—as I referred to earlier with the time you gave me, those conversations are minimized so the U.S. person part is removed if it does not have foreign intelligence value.

Once all that happens, you know—and I don't want to bore you—but there is oversight and compliance by the mission people. There is oversight and compliance by the Office of General Counsel, my office, and there is oversight and compliance conducted by the Inspector General. So this is not—this isn't simply Liberty Hall, sir.

Mr. CHABOT. Thank you very much.

Mr. COBLE. I thank the gentleman.

In order of appearance, the distinguished gentleman from Massachusetts. I stand corrected. The Ranking Member from Virginia—I overlooked him—Mr. Scott.

I will get to you soon, Mr. Delahunt.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. Deitz, it has been mentioned several times that we really don't know what you are doing at NSA. Can we get a clear description of what is going on now before you would expect us to consider any new law?

Mr. DEITZ. Are you speaking about the President's surveillance program?

Mr. SCOTT. All we know is what has been leaked to the press. So we want to know before we change the law what is going on under the present law.

Mr. DEITZ. I am not in control of that decision. Certainly we couldn't do this in public in public testimony.

Mr. COBLE. Would the gentleman yield just a moment?

Thank you, Mr. Scott.

Mr. Deitz, I am just winging this now. I can appreciate the sensitivity of some of this information—and I am thinking aloud now. Mr. Scott, we may want to schedule a secret meeting at some time. We can't do it today, but just chew on that for the moment.

Now I recognize the gentleman from Virginia.

Mr. SCOTT. Reclaiming my time, there is no point in having a secret meeting if they are not going to tell us any more than they've told us already.

I yield.

Mr. COBLE. Well, I will assume that more would be forthcoming at a secret meeting, Mr. Deitz, am I correct?

Mr. DEITZ. Mr. Chairman, what I can tell you is in a closed session I could describe the shortcomings of FISA by chapter and verse. What I cannot tell you—I cannot trump the President's decision about who will or who will not be briefed on the TSP.

Mr. SCOTT. I think that answers my question.

Mr. Dempsey.

Mr. DEMPSEY. I think we know enough on the public record. The President has said, the Attorney General has testified, General Hayden, who was one of the architects of the program, testified in July before the Senate Judiciary Committee that the President has authorized warrantless surveillance inside the United States of calls that have one leg here and one leg overseas where there is probable cause to believe that the person overseas is a member or

associate of al-Qaeda. That is on the record. Now, normally, that would require a court order. That is on the record.

Mr. SCOTT. Let me ask you while you are speaking, you answered Mr. Conyers' question about the one leg overseas, one leg over here. You also mention domestic and domestic would be covered, too.

Mr. DEMPSEY. That is why I wish Mr. Chabot were here. Because we are talking about two different things. We are talking about the President's program, one leg here, one leg overseas; and we are talking about the Wilson bill. The Wilson bill authorizes the President's program and then goes farther, much, much farther. One of the things it does, it says in its amendment to section 1802 of FISA, for purely domestic calls a warrant is not required if the Attorney General says we are directing our activities solely at the communications of a foreign power inside the United States, an embassy or a non-U.S. person agent of a foreign power engaged in terrorist activities inside the United States.

Again, the problem with that is these are purely domestic calls where there is a high likelihood that the other person to the call is a U.S. citizen. And certainly this has nothing to do with—I mean, Mr. Deitz talks about what was the original intent of Congress in 1978. There is enough water under the bridge in both directions that there is limited value to looking back to that. But this is one where Congress never dreamed it was authorizing communications interception in the United States without a court order where both parties were in the United States and one of them is likely to be a citizen.

Mr. SCOTT. My time is almost up, and I wanted to ask Mr. Deitz whether or not—when you make a decision to do a wiretap, whether or not there is an individual assessment for each call where you do categories—you said you are not doing a vacuum cleaner?

Mr. DEITZ. We are not doing a vacuum cleaner, correct.

Mr. SCOTT. Do you do an individual assessment before you wiretap a conversation to ascertain whether or not the standard has been met?

Mr. DEITZ. We are speaking about the TSP.

Mr. SCOTT. I don't know what—we are playing 20 questions now. I am not sure I am asking the question to get the right answer. So just do the best you can.

Mr. DEITZ. I will. The President's program, the program that has been leaked to the press and then acknowledged by the President, requires a probable cause determination that an individual is a member of al-Qaeda or an affiliate. And, again, those are precisely determined. So it is not a vacuum cleaner pulling up everybody, for example, who lives in a certain city or who professes a certain faith. It is not that. It is aimed at an al-Qaeda affiliate or al-Qaeda——

Mr. SCOTT. That is the President's plan. Do we assume he is not doing it, any wiretaps, without a warrant, without an individual assessment?

Mr. DEITZ. That is the program I am describing, yes, sir.

Mr. SCOTT. Is there another program? I mean, you are using 20 questions. We are trying to get around to, if I can ask the right question, to target the right answer. Are you wiretapping people

without an individual assessment of probable cause that they are a member of al-Qaeda or without a warrant?

Mr. DEITZ. I can't answer that.

Mr. SCOTT. Well, if you can't answer that, then just say you can't answer it.

Mr. BRADBURY. Well, if I might just jump in, Congressman. I think the President has made it clear that there is no other program that involves domestic electronic surveillance of domestic communications, and so the program that the President has described is the only program along those lines.

And I need to point out one thing if I might, Mr. Chairman, just very quickly just for the record. We have not publicly acknowledged that the surveillance in this program would constitute electronic surveillance under FISA as it exists today. So we have been very careful not to do that. Our legal analysis that we provided in the paper in January assumes that that is the case for purposes of going through the legal analysis, but we have not publicly acknowledged the method.

Mr. DEMPSEY. Correction. Everybody knows that it would be electronic surveillance. But, anyhow, I accept the correction.

Mr. COBLE. I thank the gentleman from Virginia, Mr. Deitz, and then I will recognize the distinguished gentleman from Arizona.

If I understood you correctly, in responding to Mr. Scott's testimony you indicate even if we went into Secret session with the Judiciary Subcommittee you still would be somewhat limited. I assume that that limitation would not apply if you appeared before the House and Senate Intelligence Committees and the Democrat and Republican leadership.

Mr. DEITZ. That is correct, Mr. Chairman.

Mr. COBLE. So there would be no limitation there.

Mr. DEITZ. Correct, your honor—or Mr. Chairman.

Mr. COBLE. The gentleman from Arizona, Mr. Flake, recognized for 5 minutes.

Mr. FLAKE. Thank you, Mr. Chairman.

And given just the short time, if you could keep your answers—I have a number to get through.

Mr. Bradbury, if we were to pass the Wilson bill, would the President stop the current program or do it all within the Wilson language? What is your understanding?

Mr. BRADBURY. Well, Congressman, I can't speak for the President on a determination like that, so I can't say what the President would do.

I would note—and I will try to be very brief. I would note that there are difficulties with the current version of the language. It talks about a 45-day period following an attack on the country. It is not clear whether that would apply today, 5 years after 9/11. Whether that is the intent, that needs to be clarified. And again we would say we shouldn't wait until the Nation has been attacked to acknowledge whether the President can do this kind of program.

Mr. COBLE. I guess what I am asking is, what would prevent the President from circumventing the Wilson language, given his inherent powers that he claimed under Article II?

Mr. BRADBURY. Well, the President is not interested in circumventing statutes; and, as you know from our legal analysis, we are

not saying that the President has circumvented any statute. We are saying the President has operated within the authority provided in the authorization through the use of military force which acknowledged and supplemented his constitutional authority in this particular conflict, our armed conflict with al-Qaeda. And, just focusing on that, the President has acted to undertake surveillance of international communications; and we view that as a supplemental authority to the authority provided in FISA.

Mr. FLAKE. Mr. Deitz, you talked about minimization and the importance of—for example, current law requires after 72 hours, I believe, that any information retained on individuals who are not the target is dumped. Is that what you understand?

Mr. DEITZ. Minimization applies to everything the same, not just discovery on the order—I mean, taps on the orders. Everything NSA does involves minimization.

Mr. FLAKE. And you are talking about that being important about what you do.

Mr. DEITZ. Yes, it is important.

Mr. FLAKE. Are you aware that the Wilson language actually strikes those provisions which require that information retained after 72 hours be disposed of?

Mr. DEITZ. I am not aware of that.

Mr. FLAKE. Mr. Bradbury, do you have an answer to that?

Mr. BRADBURY. I know that Representative Wilson's legislation would extend the period to 5 days. We actually think it should be 7. But I thought that it should retain provisions that restricted the content of the information that had been obtained if you don't subsequently obtain that order. We actually think that is an area where further refinement is important; and I would be happy to talk to you, Congressman, separately about any particular aspect of the legislation.

Mr. FLAKE. Mr. Deitz, you talked about the problem with a 72-hour period is that it is tough to establish a probable cause before a FISA court. Yet you said that every example of NSA's surveillance under the current program involved an analyst establishing probable cause. If you can establish it within your agency, why can't you establish it before a judge?

Mr. DEITZ. That is a very, very different proposition. Analysts talk to each other. They do memoranda. They pass the memoranda onto shift supervisors and so forth, but it is a discrete number of people, all of whom, by the way, are speaking the same language.

In order for us to go for an emergency FISA, the analysts have to do their part. Then it has to go to our lawyers. Then it has to go to a group of lawyers at the Department of Justice; and then, ultimately, it has to go to the Attorney General. In other words, we have to be prepared at the beginning of that 72-hour period to present all this information or ultimately to go to court with it, and that is very different from doing this intramurally.

Mr. FLAKE. The frustration that we have had is we have had these kind of hearings for, you know, ever since 9/11, and we have not heard from the Justice Department or from NSA or others what specifically—we always hear streamlining, streamlining. Yet we never seem to hear what streamlining means, and yet then we hear that the President can simply go around it. So that is the dif-

ficulty that we are in here as a Committee with oversight and with—I am troubled with the Wilson bill, that it basically takes this Committee out of the loop completely.

Mr. DEITZ. Sir, FISA applications now are approximately ¾ of an inch thick. That is paper producing. And if you are doing it—as I have suggested in my testimony, if you are doing it to prevent foreigner A or tried to protect the same sort of rights of foreigner A communicating with foreigner B, I suggest that that is simply a waste of that paper and effort and analysts' time.

Mr. DEMPSEY. If I could just say, I have looked at far fewer FISA applications than Mr. Deitz, but the ones that I have looked at, most of everything after the first page or so is boilerplate, and you read the first page and you know whether it is probable cause or not. I don't know that they need the boilerplate. I don't know in this day and age of computers why production of boilerplate is such a difficulty anyhow.

But I would say that, on your question of minimization, FISA clearly says, information acquired from an electronic surveillance must be handled pursuant to the minimization requirements. And if you take the President's program and define it as not being electronic surveillance, then it is not subject to the minimization requirements under the act; and if you take other things and define them as not being electronic surveillance, then the minimization requirements by law don't apply.

Mr. DEITZ. That is simply not correct. We are obligated under Executive Order 12333 before we do any—exercise any NSA authority. Minimization procedures in place which we then use.

Mr. COBLE. Gentleman's time has expired.

If you all will note that the Chair has been liberal today, but I think this is an important issue, and we are not going to run through it, but I hope the Members will keep in mind the sensitivity of time.

Mr. SCOTT. Mr. Chairman.

Mr. COBLE. Gentleman from Virginia.

Mr. SCOTT. I just wanted to make sure I heard what the gentleman said. He is only limited by Executive Order, not by statute, not by case law?

Mr. DEITZ. What I am saying, sir, is we have an Executive Order that obligates us to minimize.

Mr. SCOTT. That answered the question.

Mr. COBLE. Finally, the distinguished gentleman from Massachusetts, Mr. Delahunt.

Mr. DELAHUNT. Yeah. I was glad to hear that the Chairman's become so liberal.

You know, I hear what you are saying, Mr. Deitz, and I think you have to understand that there is a history in this country—and I am sure you do, given your impeccable academic credentials—we don't trust you. We trust you as an individual.

But I think what you are hearing here today is, you know, an echo of American history regarding the relationship between the branches. There is no oversight going on. You can establish a protocol that has a variety of mechanisms to ensure that statutes and Executive Orders are not being violated, but it is intramural, as you say. This is not—you know, in democracy, it is varsity ball. It

is not intramural. And we are an independent branch of Government. So I think that is the core issue. Because what you are saying here is Democrats and Republicans, conservatives and liberals, saying that is not sufficient, that is not sufficient.

Now, in a previous career, I used to do a lot of court-authorized wiretaps; and I read your testimony, and I hear what you are saying and the precious time and the paper. With all due respect, you know, there is close to 1,800 applications, none of which have been denied, I think, in a single year. You know, my colleague and friend from Arizona I think makes a very good point.

By the way, the President—you are talking about the whole issue of probable cause and refining that and it not being necessarily an ingredient in this. I mean, the President in the public statement, and I think you just said it, he has no issue with probable cause when it comes to al-Qaeda. So I think we can take that off the table.

But in terms of speed and agility, I have to tell you I just can't buy and accept, based on my own experience, that particular argument. I mean, I am sure that you've knocked some agent or somebody from the Department of Justice has knocked on the door of some FISA judge at 3 a.m. and, after a 15-minute conversation, it is approved. I mean, that is the real world. That is the real world. And if we need more analysts, then we should have more analysts. That I suggest is a real problem.

Mr. DEITZ. May I respond?

Mr. DELAHUNT. Of course. But I have a question for Mr. Bradbury, so try to be concise.

Mr. DEITZ. I will be very quick. There is clearly a difference between criminal law and foreign intelligence collection——

Mr. DELAHUNT. I understand that.

Mr. DEITZ.—and in terms of where it rests within the constitutional framework.

Mr. DELAHUNT. I understand that.

Mr. DEITZ. And, by the way, if we are 2 days late serving a search warrant on a criminal, we may have blown a case. If we are 2 days late to getting a wiretap on a foreign intelligence context, we may have a disaster.

Mr. DELAHUNT. I understand that. But that goes to the question that was posed by Mr. Conyers. What do you need? There is nobody here on this panel that won't give you the tools that you need. Whether it is 7 days, 14 days, let's discuss them. We are not going to hold hostage the American people. That is for sure. Everybody here wants to destroy al-Qaeda and affiliates. That is a given. Okay? But how do we do it without betraying the Constitution? Because if we go down that road—we hear a lot about Hitler and fascism these days. That is the beginning——

Mr. Bradbury, you indicated that you were—you'd consider amendments and suggestions and you want to work with Congress. Is that a fair statement?

Mr. BRADBURY. Absolutely, Congressman.

Mr. DELAHUNT. Can I ask you something? Have you drafted legislation?

Mr. BRADBURY. We have provided a lot of suggestions.

Mr. DELAHUNT. But that is not my question. Has the Administration drafted legislation for consideration based upon your understanding of what your needs are? Can you just give me——

Mr. BRADBURY. We have not drafted and submitted legislation.

Mr. DELAHUNT. Then I think—you know, I have to tell you, it is—when I hear that, I feel like I am being played with. You have many, you know, I think legitimate concerns that can be addressed; and I would challenge the Administration and the White House and the President to come forward with a piece of legislation that this Committee, sitting as the Committee of jurisdiction, can review.

It is far too late. It is my understanding back on June 21 the Wexler resolution of inquiry was passed. We haven't heard anything. And, you know, you talk—you are talking a good game, but you are not delivering. That is the problem that I have.

Now, we can play this out. We all know it is 9 weeks to an election, okay? And I am not so naive to think that politics isn't, you know, involved here. I am not suggesting you or any of the panelists—but if you want to do something real, then come forward with a document that we can debate and argue.

You are here. Everybody is eloquent in terms of their testimony. There are legitimate concerns. I think we can get it done. It is incumbent on the Administration to see that we have something before us that we can debate. It is the President that isn't playing fair and square with this Congress.

I yield back.

Mr. BRADBURY. Mr. Chairman, may I——

Mr. COBLE. Very briefly.

Mr. BRADBURY. The President does want to work together with Congress on this issue. The President has indicated that we do support Chairman Specter's legislation, wants to see it move forward. He has also said that we see positive things in Senator DeWine's legislation and also in Representative Wilson's legislation.

We do want those to move forward. We don't want them to be stymied. We would like to see something that resolves this issue in a legislative way where the branches are working together.

In that spirit, I would say that, as you know, I think both Intelligence Committees of the House and the Senate are fully briefed into the program and have been conducting very intensive, very intensive oversight of the NSA program; and I would dare say I think it is the most scrutinized, legislatively scrutinized program perhaps in the history of the NSA. So there is very extensive work being done, good work being done by the Intelligence Committees of Congress.

Mr. DELAHUNT. Mr. Bradbury, I am not denying that. But what I am saying, let's bring this forward in something that the American people can review.

This Committee will be the primary Committee of jurisdiction, or at least concurrently. I see Ms. Harman has left. But, in any event, have the Administration come forward, if you have concerns, and then we can take them up. We have been delaying this for a period of time, the concerns that are expressed by all of those that are

what I would call parties of interest. I think it is up to the Administration.

Mr. COBLE. Gentleman's time has expired.

The distinguished gentleman from California, Mr. Lungren.

Mr. LUNGREN. Thank you, Mr. Chairman.

I would just ask unanimous consent to have half the time Mr. Delahunt had today.

Mr. DELAHUNT. Objection.

Mr. LUNGREN. Boy, that is a boatload from my friend from Massachusetts. We have worked together on legislation because of our concerns about the two branches of Government, but, boy, bringing in Hitler and the bundestag and fascism and reference to the Administration I think is a bit much here today.

I wish we had an easy answer to this. I hearken back to the language of Justice White in his concurring opinion in the Katz decision, which was one of the seminal opinions dealing with privacy in the context of search and seizure; and, as he said, wiretapping to protect the security of the Nation has been authorized by successive Presidents. The present Administration he is talking about at that time would apparently save national security cases from restrictions against wiretapping. We should not require, he said, the warrant procedure and the magistrate's judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable.

And it just strikes me that in this program that we are discussing the President has followed the suggestion of Justice White and specifically had his hands-on review of this program and the Attorney General—and maybe it is not so easy to say it could be delegated downward, if you believe in what Justice White has said.

Here's the conundrum I have. I happen to think the Constitution under Article II does give the President certain authority; and it has been historical, I would say to my friend from Massachusetts, that successive Supreme Courts have recognized that the President of the United States has unique capability and authority in the area of gathering information, dealing with the enemy. In fact, it has been extended beyond wartime situations in terms of foreign intelligence of all types.

Now, given that fact, I look at what can we do legislatively. I think it is so easy for us to talk to the American people and talk to the cameras and say, well, the President's violating the law because he is not following FISA. I wish it were that simple.

It was the Attorney General for the Carter Administration, Griffin Bell, who, in testifying on behalf of the Carter Administration in support of the FISA Act, specifically stated that it was the position of the Carter Administration that the FISA Act did not in any way nor could it encroach on the President's constitutional authority under Article II.

Now we can say we don't like to follow the Constitution. Maybe we think the Supreme Court doesn't follow the Constitution at times, but I hope we would be consistent with our oath to the Constitution.

So does that mean we can't do anything? No. I look and see that the powers we have—I mean, the most extreme power is the power

of impeachment, but short of that is the power of the purse. And that is where we can, in fact, stop the President from doing some things; and it seems to me that is what Congress can do in a situation like this. So the question is if we construct legislation that gives Congress the information such that it could make the judgment if it wanted to exercise the power of the purse.

So that goes to the question of how do we want to be informed? And we have set up in the Congress, in the House, a program where issues of this nature, whether we like it or not, being on the Judiciary Committee, are the prime responsibility of the Intelligence Committee; and that is sort of where we find ourselves here.

So, try as we might, it seems to me in some situations we can construct legislation for the preferred process that the President should follow, but I think we are straining in the face of the Constitution to say we can do it such that we will limit the President's otherwise existing constitutional power here.

That is the difficulty that I am under. There are certain things I'd like to do to restrict the Administration. If I look at the Constitution I don't think I can do that, so my point is how do we construct a methodology whereby the Administration—not only this Administration but future Administrations are most likely to follow that procedure, number one.

Number two, how do we avoid confusing, as Mr. Deitz has said, the expectation of privacy concept that we find in the Constitution? Do we extend it to everybody around the world? Do we extend it to anybody and everybody because somehow we believe that our sense of justice is an appropriate one for American citizens and therefore should we extend that to those who would do us harm in the war on terror?

I know my time is almost up. Let me ask Mr. Dempsey this.

Mr. Dempsey, first of all, do you believe that we are, in fact, in a war? And, number two, if we are, does the President have certain inherent powers under Article II in the gathering of information? And, number three, if the program is as it exists, that is the one we are talking about, that everybody's talking about, the specific program to listen in on al-Qaeda, if it is as it has been suggested even though it does include, as Mr. Deitz said, conversation by someone here in the United States because the other part of the conversation—is that unconstitutional in your view?

Mr. DEMPSEY. Congressman, to some extent we are in a war. I don't think that the war reference or the war concept covers everything that is going on. There is, obviously, law enforcement aspects as well.

I think the President does have powers to collect intelligence in times of war against foreign adversaries, even not in times of war. However, I do think those powers are shared powers, like all of the President's war powers are shared powers, and that constitutionally Congress has the authority to pass laws regulating the exercise of the President's powers.

In terms of constitutionality, I think that we have come far enough in our understanding of the Fourth Amendment to say that the best way to guarantee constitutionality of a search inside the

United States is to have a judicial warrant; and I think it is unwise, I will simply say, to push that farther.

Now the bottom line, Congressman, I think you raise a good point, and where it leads me to is, for now, you should do nothing. That is, the current system—in my view, the current situation of warrantless wiretaps, close congressional oversight, warrantless wiretaps are narrowly focused, as the President has said, where there is probable cause to believe that a member of al-Qaeda or an associate is on the phone: That is far better than the Wilson Bill.

The Wilson Bill goes far beyond that and would cut congressional oversight, not increase it. Because the way the oversight process works, oversight is required only for things that are electronic surveillance. If it is not electronic surveillance, then you are back to sort of the power of the purse and the push and tug, which is where we are now.

So I would say, let the situation go on. It is not a pretty picture, but it is certainly better than the Wilson bill.

Mr. COBLE. The gentleman's time has expired; and, for the record, I will say to the gentleman for California, you received as much time as Mr. Delahunt did. So you all are even.

Mr. LUNGREN. I only got it once, though.

Mr. COBLE. The distinguished gentlelady from California, Ms. Waters.

Ms. WATERS. Thank you very much.

Mr. Chairman and Members, I think the concerns that I have basically been raised over and over again. One is this: I do not understand how we could even consider any of the bills that are being proposed to make changes as it relates to foreign intelligence surveillance given what little information we have from the Administration about the problems, what are the problems with the way the law is constructed now. A lot of work, a lot of time, a lot of attention have gone into constructing a law that balances the need for information and protection of the Fourth Amendment in the Constitution.

Let me ask Mr. Bradbury, were you involved in advising the President in any way when he decided to undermine the Constitution of the United States of America? Were you a part of the team of people that talked with him about what he was doing? Did he seek your advice?

Mr. BRADBURY. Well, Congresswoman, I was not in the Department of Justice when the program was initiated in 2001.

Ms. WATERS. Who was? Who did you hear was there to advise him? What do you know about this?

Mr. BRADBURY. Well, I think the Department of Justice under the Attorney General is—the Attorney General is the officer under our laws that provides legal advice to the President, to the Executive Branch.

Ms. WATERS. You think the Attorney General—he sought the advice of his Attorney General and he advised him that he could, in fact, proceed with warrantless surveillance, is that right?

Mr. BRADBURY. Yes, Congresswoman. As the President has described it, he sought legal advice, including from the Department of Justice, at the time this program was initiated and was advised that the program was lawful and consistent with the Constitution.

Ms. WATERS. And again you may have done this already, but could you quickly describe to me how it is consistent with the Constitution of the United States?

Mr. BRADBURY. Absolutely. I will try to be very, very brief.

Ms. WATERS. Yes.

Mr. BRADBURY. We have set it forth at length in a paper that we have provided to Congress, made public. The President has long been recognized to have authority under Article II of the Constitution to take actions to protect the country, including in the area of electronic surveillance. That is an authority presidents have exercised in wars from the beginning of the Republic, including, for example, in World War II and World War I when Presidents Franklin Roosevelt and President Wilson——

Ms. WATERS. Does not the Foreign Intelligence Surveillance Act of 1978 describe how he is to do that?

Mr. BRADBURY. Well, we would actually—I actually believe the Foreign Intelligence Surveillance Act does not fully address the question of what happens in time of war. It has a provision in there about declarations of war, which to me makes it clear that Congress intended——

Ms. WATERS. When did the Justice Department discover that the Foreign Intelligence Surveillance Act of 1978 was inadequate?

Mr. BRADBURY. Well, I think what we are talking about is a different paradigm from FISA surveillance. We are talking about a wartime program to detect enemy communications. So we are really talking about a different paradigm, and we think authorization for the use of military force that Congress passed in the days after 9/11——

Ms. WATERS. All encompassing and it takes care of anything the President would like to do?

Mr. BRADBURY. No, Congresswoman. Absolutely not. But it does focus with the particular conflict we are engaged in with al-Qaeda and makes it clear that the President does have all those traditional authorities necessary and appropriate——

Ms. WATERS. I am sorry I had to interrupt you. We only have so much time. Attempt to describe why the President of the United States believes he can ignore the Constitution of the United States and the Fourth Amendment.

But I am going to use my last few seconds to simply say that this is another bungled action by the Administration in the so-called war on terror. Unfortunately, Mr. Chairman and Members, the President has failed to provide quality leadership as he has executed the so-called war on terror, mistake after mistake after mistake, and has got us to the point where we are now—where our soldiers are caught in a civil war that this Administration will not admit, caught between the Sunnis, the Shiites and the Kurds, with people dying every day, civilians and soldiers.

In addition to that, we are losing in Afghanistan. We are threatening to go to war, I guess, with Iran and Syria.

I mean, we cannot take you seriously; and if, in fact, his Attorney General and this Department of Justice is advising him, then you and Rumsfeld and all the rest of you guys really should have to go.

There is a lot of talk about calling for Mr. Rumsfeld's resignation again and again and again, but the fact of the matter is you should

all hang your heads in shame for the way that you have mismanaged this so-called war on terror. The people of this country do not deserve to have the Constitution undermined in the way that the President is doing it. And to then have the audacity to tell us that the President has the right to do it, despite what we are guaranteed by the Constitution and the Fourth Amendment, somehow make this fallacious argument——

Mr. COBLE. The gentlelady's time has expired.

Ms. WATERS. I have more to say, but I respect that my time has come.

Mr. COBLE. Mr. Delahunt, I have known for some time you are a formidable legislator, but you have more muscle in your arm than I realized. Because you expressed earlier concern about the Department of Justice's response to our inquiry some weeks ago. It was delivered today to Chairman Sensenbrenner and to Congressman Conyers. So I commend you, sir.

Mr. DELAHUNT. I appreciate that commendation, Mr. Chairman; and it does, I guess, demonstrate that there is muscle over here.

Mr. COBLE. Distinguished gentleman from Texas, Mr. Gohmert.

Mr. GOHMERT. Thank you, Mr. Chairman; and I am hoping my 5 minutes will be stretched into 10 as some of our colleagues across the aisle will be allowed.

Mr. COBLE. I will continue to be liberal.

Mr. GOHMERT. But, in any event, I'd have to address some of the comments that were just made. Anybody who wants to blame this President and Don Rumsfeld and his Attorney General for the acts of terrorism that are occurring against our Nation has to also blame Bill Clinton for 9/11. You've got no choice. Because 9/11 we know unequivocally was planned and almost completed, all preparation, during his presidency. So if you are going to blame George Bush and Don Rumsfeld, it is time to hang 9/11 on Bill Clinton.

The fact is Bill Clinton did nothing to deserve 9/11 being plotted as it was during his presidency. If you look at his commitment of troops, they were most often to protect Muslims. If you look, he was the most friendly toward Palestinians of any of the Presidents we have had. He did not deserve to have 9/11 plotted and planned during his presidency as it was, but it was because since 1979 war has been going on. We just didn't know we were at war. They knew that we were at war. They were at war against us, as the attack in 1979, 1984, 1993, on through the 1990's showed. So we are at war. It is just that, after 9/11, we only now realize that we are.

The question is, what do we do from here? You can play the blame game and say, well, this was Bush's fault or Rumsfeld's fault and 9/11 obviously was Bill Clinton's fault. I don't think any of those acts of blame apply.

So I had to get that out. But let me get to the panel and thank you for your patience with our little bickering up here, because we do have some very similar concerns in some areas.

Something I want to hit on is something that we have discussed in areas of the PATRIOT Act, FISA, some of these surveillance programs, data mining. I will go back to a concern that was raised years ago when I read Chuck Colson's novel. It was regarding an idiot that blew up an abortion clinic. Somebody was killed, so the Attorney General basically declared war on churches where pro-life

was being preached. That gave the Government a basis to go in, do surveillance, whatever they wanted. Everything was okay because this was considered a terrorist activity because churches were preaching pro-life and somebody blew up an abortion clinic.

So I keep coming back to that scenario, and I told Attorney General Gonzalez when he was testifying there at the table where y'all are that, you know—of course, this was before the breach of 219 years of precedent and respect for article 1, sections 5 and 6, but I told him that I was not concerned about him or this Administration, but I wasn't sure about future Administrations. So we had to be concerned about the existence of authority to do things that we did not anticipate.

I had concerns in the PATRIOT Act because it referenced that certain things could be done by our intelligence people if it was believed there was a foreign intelligence component or—and it was a big or—clandestine intelligence activities.

Mr. GOHMERT. And I thought I was throwing the Attorney General a softball to ask has there been any surveillance of any kind based solely on it being a clandestine intelligence activity without any foreign component, because most of us don't have any problem—we don't believe it violates the Constitution to surveil foreign to foreign, foreign with any type of terrorist links to domestic. We don't have problems with that. But when you bring in an all-domestic component, I start having concerns. And I thought I was throwing up a softball, and then the Attorney General danced all around without giving a straight answer.

So I want to come back and try to get a clear answer as to whether anyone here knows of any warrantless surveillance that is authorized in domestic-to-domestic calls through—whether it is the NSA, the FBI, anything of that nature—through either the PATRIOT Act, FISA, or the President's own acts and determinations. Does anybody know of anything that authorized domestic purely on the basis of being a clandestine intelligence activity?

Mr. BRADBURY. Congressman, I am not aware of any. And I believe that the President did make it clear, as I indicated earlier to Congressman Scott, that there isn't any domestic-to-domestic communications being listened to without court order, pursuant to the President's authority. And I would just point out that the Keith case, the *United States v. United States District Court*, the Supreme Court in the *Keith* case addressed questions of domestic security surveillance as opposed to foreign intelligence surveillance, whereas you point out there is no foreign power component at all, and concluded in that case the warrant was required. So I am not aware of anything such as you described.

Mr. DEITZ. I hope I can equally give an unambiguous no.

Mr. GOHMERT. That is what I was looking for. I thought I would get that from the Attorney General. But then shortly after that, we found out there was data mining going on domestic-to-domestic, and then that raised concerns that perhaps if there is data mining going on, perhaps there is a little further intrusion into actual communications. But you are both saying that answer is no, correct?

Mr. DEITZ. Correct.

Mr. GOHMERT. And, Mr. Alt, earlier you looked like when my colleague was asking questions that you were ready to give an an-

swer, and I want to make sure you have a chance if there was something you wanted to interject earlier that you didn't get a chance to.

Mr. ALT. I appreciate that. I have sort of a couple of comments based on Congressman Lungren and what Congresswoman Waters had to say.

I think that we need to be careful about sort of framing this issue as if foreign intelligence surveillance magically appeared 28 years ago, and as if FISA somehow is coterminous with the requirements of the Constitution.

Mr. GOHMERT. Don't use too big of words.

Mr. ALT. So in other words, FISA doesn't necessarily cover the same things the Constitution does and to, you know, sort of suggest that it does is to, you know, betray sort of a lack of knowledge of the case law in this area. Quite frankly, you know, without sort of sounding like I am talking to my students, oftentimes when someone doesn't like something, they scream it is unconstitutional. But in fact, quite frankly, foreign intelligence surveillance has always been treated differently by the courts than has title 3-style criminal warrant procedures. Not only that, you know, while we may talk about the fact that warrants are the general rule, they are not the general rule without exceptions, special needs doctrine cases.

And in particular, it is worth noting that there is a special exception for Customs checkpoint which covers the mail. When you receive something in the mail quite frankly in the electronic age, international transactions which previously had to be done through the mail or through Customs checkpoint now take place by computers and via telephone transmissions and so forth.

The rule about protecting the territorial integrity of the United States, which was seen as being inherent in the Fourth Amendment, sits beyond the special needs doctrine under the Ramsey case, would seem to clearly apply in cases of foreign intelligence surveillance. And so simply screaming that something is unconstitutional without providing a single citation adds nothing to the debate, and I would recommend that as we are looking at this, we look at what the Constitution actually requires.

Mr. GOHMERT. If I could ask one quick question. In Congresswoman Wilson's bill it mentions that after there is a terrorist attack against the United States that there will be certain powers, not to exceed 45 days, following a terrorist attack. I am concerned that if we have another 9/11, that 45 days, just to have blanket ability to absorb whatever we can, may not be enough. And I was curious about DOJ's and NSA's position on 45 days. Are you familiar with the provision I am talking about?

Mr. BRADBURY. Yes, Congressman.

Mr. GOHMERT. So without me reading the whole thing, if you would comment, what do you think about 45 days? Is that enough time after another 9/11?

Mr. BRADBURY. I would say that in Representative Wilson's bill it is a renewable period. So it would—could be reauthorized. I think that is very important. We certainly don't think it should be limited to after an attack has already been successfully received by the United States. It should be to protect us from an imminent or

severe threat of attack. But as to the sufficiency of 45 days, I would probably defer to the intelligence experts.

Mr. DEITZ. I agree with every comment he just made. The renewability helps a great deal but our goal at NSA, their goal is to protect this country from ever being attacked again.

Mr. GOHMERT. And thank you.

Mr. BRADBURY. Thanks.

Mr. DEMPSEY. May I comment? You know, "to protect against"—I have no doubt that there are people today planning an attack on the United States. So under what Mr. Bradbury is proposing, we would have perpetual prospective authorization to the President to carry out wiretaps without a warrant.

Mr. GOHMERT. Thank you.

Mr. COBLE. The gentleman's time has expired. Ladies and gentlemen, the 5-minute rule has been profoundly violated today, and the Chair assumes all guilt. But as I said before, it is an important issue and I think that justifies the violation. I appreciate you all bearing with us.

Before I recognize the gentlelady from Texas, I want to say in response to what my friend from Texas said, let the record show that I have been vocally critical of my Bush Administration. I have been vocally critical of the previous Clinton Administration. So I just want to reiterate what you said, Mr. Gohmert: There is plenty of blame to be placed inside that target. Both parties.

The distinguished gentlelady from Texas, Ms. Sheila Jackson Lee.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman. I was hoping you would not qualify your liberality preceding the opportunity to inquire and thank you very much, as well the Ranking Member, for recognizing the importance of these—of this hearing. I would like to offer into the record a letter that I wrote on May 12, 2006, asking for such hearing by the Full Committee, and I thank this Subcommittee for holding them, and I think it would be important for the hearing by the Full Committee as well.

Mr. COBLE. Without objection it will be received.

[The information referred to follows in the Appendix]

Ms. JACKSON LEE. I would offer to say that I believe that we are in fact the defenders and protectors of the Constitution. I would also suggest, Professor Alt, that you are speaking to lawyers who have taken Constitution 101, but frankly I practiced law and I would beg to differ. I think there are nuances. There are exceptions. But we are representing the people of the United States, and with that in mind, we have a responsibility to interpret the Constitution as the Founding Fathers obviously laid out the framework, which is a Nation adhering to the Bill of Rights, but also we have the responsibility of responding to the political will of the people. And I would venture to say to you that even your students would be outraged or have been outraged by some of the violations of the basic tenets of the Fourth Amendment.

Let me read into the record I think the beginnings of a very thoughtful opinion by Judge Anna Diggs Taylor. I know there is a rush to judgment to the Court of Appeals to malign her, but frankly her portfolio is one to be compared to any of you gentlemen who are sitting there.

And the opening remarks as she began to assess the NSA spying, if you will: This is a challenge to the legality of a secret program hereinafter called TSP, undisputedly inaugurated by the NSA agency, at least by 2002, and continues today, which intercepts without benefit of a warrant or other judicial approval prior or subsequent, the international telephone and Internet communications of numerous persons and organizations within this country.

So there is a domestic element to this. The TSP has been acknowledged by this Administration to have been authorized by the President's secret order during 2002 and reauthorized at least 30 times since.

I disagree with the idea that, Mr. Chairman, if we had an opportunity for a secret meeting, I disagree that we should be limited because we are either not leadership or the Intelligence Committee. I truly believe that this Committee deserves to understand what you are doing. We deserve so because we represent the people of the United States. And I am offended by the fact that there is a limitation of who can understand, if it is a classified presentation, what the President is doing.

And let me try to set the facts why I think there is such a great deal of consternation. One, there is no divide in any Committee on the war on terror. But let us be very clear: There is no war that this country is now engaged in under the Constitution of article 3, section 8. That is what many of us quarrel with. There has been no declaration of war. We accept the metaphoric terminology that we are in a war on terror but there is no declaration under the Constitution. Until I am told otherwise, the Constitution is still the governing document interpreted by Federal courts and others, but it is still the governing document.

So let me be very clear that we do have a right of oversight, and here are my concerns. I think it is important because I think we have been motivated to have this hearing in light of the recent, if you will, successful discovery of the plot that would have generated the loss of thousands of lives. We celebrate that. But let us be very clear that in the course of that investigation, that discovery, that find, that criminal investigation, there is no evidence that the NSA work, the NSA approach, the NSA spying, the NSA data collecting had anything to do with—and let me read the words of Secretary Chertoff: Currently we do not have evidence that there was as part of this plot any plan to initiate activity inside the United States or that the plotting was done in the United States. So, first of all, the NSA domestic wiretapping certainly cannot have played a significant role in unraveling the plot.

And then at the same time, let it be known that the U.K, as I understand it, still has warrants that they utilize, that they did not waive in their investigation for national intelligence, and it is done by the Secretary of State for the United Kingdom. And therefore they too followed a certain procedure in discovering the plot.

The 9/11 Commission made it clear that we could have discovered the tragedy that occurred, the horrific tragedy, hindsight, if we had simply connected the dots, and that was made very clear. We had all of the intelligence. In fact, my understanding is there was a memorandum submitted to this Administration that was on their desk prior to 9/11. So you can investigate that. There was a

memo discussing some of these very issues. So it is all about the intelligence and the dot collecting.

Mr. Dempsey, let me raise these questions with you, then.

You had indicated a sentence, that I think needs to be edified in your opening paragraph, that the Administration, caught in secret violation of FISA, is now seeking radical changes in the law. And when we make those kinds of comments, clearly we need to have an explanation. And I would like to raise these questions so the panelists can answer.

The Wilson bill says that you can allow wiretapping without a warrant. First of all, we are doing it now with no limitation. The Wilson bill says 90 days after an attack on the U.S., and of course I am concerned about what is an attack on the U.S. It is very vague at this point. But the 90 days without a warrant is really an affirmation of what is going on now. It only has a limit, and then why would the people of the United States want to take the Representatives of the United States out of the oversight as you mentioned?

So would you answer the radical aspect of your—what is it that you perceive to be radical? I think it is important if you can speak to the concerns of the American people. Mr. Deitz, since you are the general counsel and because you offered the words that we typically say as lawyers, "Your Honor," I know you are obviously a very competent counsel, you are always in court. But tell me why this Committee could not be briefed to understand what the President is doing in a classified briefing and why you could not function, as Judge Diggs Taylor has said, with at least approval by the courts, even after the fact, when we know that 99 percent of the FISA requests have been approved.

Mr. Dempsey.

Mr. DEMPSEY. Congresswoman, the Wilson bill has two different provisions on attack, one which would allow warrantless surveillance by the President for 60 days following an armed attack against a territory of the United States, and the other of which would allow warrantless surveillance by the President for 45 days following a terrorist attack against the United States. The 45 days could be renewed an unlimited number of times.

Now the current rule is 15 days in case of declaration of war.

Now, actually I don't think that is the most radical portion of this bill. I think that perhaps the declaration of war concept a little bit has fallen out of use, clearly, both internationally and in terms of the way the United States uses its Armed Forces.

Ms. JACKSON LEE. That is unfortunate. We have, I think, violated the Constitution. And by the way, it is Article I, Section 8. I may have misspoke before.

Mr. DEMPSEY. Up or down, I won't go into that. I think there could be some modification to the time of war provision of FISA without being radical. But what I think is radical are the ways in which various things, war or no war, attack or no attack, various things are being defined as not being electronic surveillance at all for allowing the Government to collect information on U.S. citizens and going far beyond, far beyond what this President has said he is doing.

Now we can talk a lot about what is——

Ms. JACKSON LEE. Give us an example, because I want to yield to Mr. Deitz.

Mr. DEMPSEY. First of all, it would allow the—as I read it—the scooping up on an untargeted basis. I used the word "vacuum cleaner." Mr. Deitz doesn't appreciate the use of the word vacuum cleaner, so I will simply say scooping up without targeting, without particularity, scooping up large numbers of foreign-to-domestic calls.

Ms. JACKSON LEE. Such as a telephone data, if you will, broad sweep.

Mr. DEMPSEY. Yes. That is the way I read it for international communications, both wire and wireless into and out of the United States, including Internet. Secondly, it would allow the—I say vacuum cleaning—but large-scale collection of the transactional information related to communications. And as I read it, it would be for the purely domestic acquisition, purely domestic calls, monitoring who is calling whom. This is the other sort of program that has received much less attention and which has not been formally acknowledged by the Administration. But the monitoring basically of who is calling whom. Information that is not constitutionally protected under Supreme Court decisions dating back to the seventies, but which is clearly important, clearly significant both to the Government and to citizens. That information could be collected wholesale or in large quantities.

Ms. JACKSON LEE. And may have no value. Let me——

Mr. DEMPSEY. Does have some.

Ms. JACKSON LEE. It may or may not. You are talking about wholesale vacuum cleaning. It may or may not have any wholesale value. That is where I have some questions.

Mr. Deitz, let me have you answer the question why we could not have a classified briefing in detail after the fact, on the appropriateness of what the President is doing. And then, secondarily, this broad reach that is obviously what has been occurring already, we find that Justice Diggs Taylor said you don't even have approval after the fact. Which I can't imagine how that would injure any of what we were attempting to do in the safety securing of this Nation. It is just a broad reach with no protections whatsoever.

And I don't think the—as I said, the idea was to fall victim to 9/11, if you will, by turning on ourselves and denying the protections of what I think is a valuable document, and that is the Constitution.

Mr. DEITZ. Congresswoman Jackson Lee, I will try to answer both of your questions as economically as I can. I am not the person who decides who on the Hill gets briefings and who does not.

Ms. JACKSON LEE. But you can carry the message back.

Mr. DEITZ. I certainly can do that. I know that traditionally the HPSCI and SSCI Committees have been the ones to oversee the programs at NSA and other intelligence committees and other intelligence agencies, and certainly there is always a concern, without being specific about anybody here, there is always a concern that the more people who are aware of programs, the likely—the more likely it is to have leaks. And so that is always an issue but, again, I did not make that decision.

In terms of why not—the notion underlying the authority of the President, the TSP, is that it is outside FISA; that under the President's Article II authority he doesn't need FISA approval to conduct certain kinds of foreign intelligence. And what underlies that concern, I believe, was the need for speed and agility in acquiring terrorist information that jeopardizes this country.

Ms. JACKSON LEE. Then what prevents you from getting approval after the fact? I don't mind updating and we already updated FISA under the PATRIOT Act, but what is wrong with the post-approval for some actions that you say are necessary by the President.

Mr. COBLE. Will the gentlelady yield to me?

Ms. JACKSON LEE. I will be happy to yield.

Mr. COBLE. Mr. Deitz, if you could wrap it up.

Ms. JACKSON LEE. Thank you for your indulgence.

Mr. DEITZ. There are two answers to your inquiry. The first is I don't believe FISA contemplates such a conference to get that. But it is worth noting. And I stress this: that very soon after the President's program began, General Hayden briefed all of the very senior people on the Hill and the HPSCI and SSCI folks and the presiding judge of the FISA court, and when that presiding judge retired and a new presiding judge came in, briefed that presiding judge. So there was an attempt to, if you will, do a Justice Jackson under the Steel Seizure Case to try to make sure that people on the Hill and the other two branches of Government were apprised of this program.

Ms. JACKSON LEE. I will end on this note. Maybe we should look at the post-approval, because I know I am not sure if he was speaking about the judge who resigned out of frustration because the Administration couldn't find their way to adhere to the law, and I would also say with all due respect I don't think any of us can accept a badge of honor in who leaks the most. Because certainly I think the Administration has their share of major leaks, and certainly I don't think that is sufficient excuse. We have people dying. We have people on front lines in various wars based upon faulty intelligence, and I think the American people are due at least the accuracy of what we are doing, but they also deserve the protection of the Constitution which is a living document. And I would hope we would be able to have legislation that is not as broad as Congresswoman Wilson's.

I think there are other legislative initiatives, Harman-Conyers, that really makes some sense. And I think the Administration is not going anywhere unless they do this in a bipartisan manner.

Mr. COBLE. Folks, it is going to soon be supper time because—I think because of the importance of this issue we will have a second round, and I would urge the Members, if we can, to try to comply with the 5-minute rule if we can best do it.

Ms. JACKSON LEE. Thanks, Mr. Chairman.

Mr. COBLE. You bet.

Mr. Alt, this may have been broached before, but in your testimony you state that any legislation addressing FISA should provide the President with the ability to conduct foreign intelligence surveillance for fixed renewable periods of time without obtaining a FISA warrant.

Elaborate on that, and as you elaborate on it, do you think these bills comprise to providing such flexibility?

Mr. ALT. Essentially what I was looking for on that was making sure the President was able to continue the program that he has in place, that he has a flexibility, because quite frankly, it is shown to be necessary in dealing with al-Qaeda. I think that Wilson's bill is reasonably good on this. As I suggested, for instance, with regard to the attacks on the U.S., I personally think that the trigger needs to be a bit lighter and give a bit more discretion to the Administration, which is to say I don't think, quite frankly, the American people want to have to wait until there is an attack on the U.S. in order to implement provisions, the sorts of terrorist surveillance provisions that are constitutionally permissible today.

One of the things I think that we need to look at, oftentimes I think people sort of throw up the constitutional barrier as one to attempt to put in additional restrictions and legislation, and quite frankly what we are dealing with here today is largely a question of policy. You know, to what extent does Congress wish to attempt to apply additional restrictions above and beyond what the Constitution requires upon the President's ability to carry out these sort of surveillance programs. In that context, quite frankly, I think most people would want greater ability to do this, with some oversight to make sure that it actually is targeted at foreign surveillance rather than targeted at potentially purposely domestic surveillance, the sort of things that were involved in the Keith case.

Mr. COBLE. The distinguished gentleman from Virginia.

Mr. SCOTT. Thank you, Mr. Chairman. I want to make a couple of comments. When you are talking about this burden, some wiretap procedure, the procedures are ex parte. That is, only one side is there. They are uncontested because there is nobody there to contest it. So it cannot, although procedurally you have to do it, it is not—it is not a contested situation.

As I understand,the present situation, they are only doing people who are known al-Qaeda members, which is different from what the—some of these bills will allow. Al-Qaeda, you are talking terrorism. Foreign intelligence is not limited to terrorism, and that is one of the problems with some of these bills. You open it up to anything under the foreign intelligence. That could be a trade deal or anything else. Doesn't have anything to do with crimes or terrorism. So at least what has been leaked out so far, we are better off, as Mr. Dempsey has said, just leaving it be legal or illegal because it is better than owning up to anything and everything.

One of the areas that I would like to get into is the standard you need before a wiretap. We said you don't want to wait until an attack. Well, what do you need to do a wiretap? What standards? Probable cause? Reason to believe what? And before we get into that and who gets the check and balance, is the President satisfied you need it, that is it; or should you have a warrant?

And before we get into that, Mr. Chairman, I would like to yield such time as he may consume to the gentleman from California, a Member of the Committee, Mr. Schiff.

Mr. COBLE. Without objection. Mr. Schiff.

Mr. SCHIFF. Mr. Chairman, I want to thank you and Mr. Scott for yielding me time today. I want to begin by referring to the com-

ments of the testimony of Mr. Deitz that the technology should not be central. It shouldn't be the technology that matters. It should be the targets that really matter. I agree with that.

You also testified that where you are dealing with foreigner A talking to foreigner B on foreign soil, this shouldn't be the subject of FISA. And I agree with that, too. The problem is this: We are being asked to make sweeping changes to the Foreign Intelligence Surveillance Act essentially in a vacuum. None of us in this Committee understands why foreigner A is talking to foreigner B on foreign soil that invokes FISA. I assume there are technological reasons that may be true, but none of us here understand how in your view technology is central, when technology shouldn't be because we haven't been briefed on the program.

We might as well have the lights out in this Committee room because as a practical matter, we are all sitting here in the dark. And you may say, Mr. Deitz, it is traditional to brief the Intelligence Committee and not to brief this Committee in a classified hearing. That is fine. But don't come to this Committee and ask us to make sweeping changes to our laws and ask us to fulfill our obligation of protecting the Constitution and do it in the dark. That is, I think, the discomfort you are hearing from some of the Members of this Committee.

We will do whatever is necessary to protect the country, but we won't buy a pig in a poke, particularly when we can't be sure that it will actually even improve the security of the country. We can't tell if the changes that you are proposing at this point are necessary. And we are not moved, I think many of us, by the argument that administrative burden—that you have got analysts who have to talk to lawyers in this department and that department should overcome concerns about the Constitution.

I have never seen a situation where the concern over administrative load somehow superceded devotion to the Constitution. That is not a very powerful argument for us to change the law.

So I would encourage the Subcommittee Chairman to stick to your guns and request a classified hearing for the Members of the Full Committee. There is nothing that precludes you, by law or anything else, from fully briefing this Committee. We are under the same classified admonitions, the same criminal penalties as the Intelligence Committee Members, and if you are going to ask this Committee to make these changes, I think you have to give us information where we can satisfy ourselves that we are doing our constitutional duty.

I would like to finish my comment and invite you to respond.

Mr. Bradbury.

Mr. COBLE. Mr. Schiff, keep in mind you are not a Member of the Subcommittee so don't push us too far, but go ahead.

Mr. SCHIFF. I am merely asking that Mr. Scott be given the same liberal timing as in the first round.

I really, with respect to Mr. Bradbury, don't think your comments shed much light here. You continue to rely on the authorization to use military force, as if the *Hamdan* decision has never been issued. And what concerns me about that is the *Hamdan* decision had a phrase, I think a passage that was completely pertinent to the NSA program, and said that nothing Congress did in the

AUMF gives any hint that we are intended to change the law about tribunals, and the same can be said about the NSA program. And if we continue to rely on that kind of constitutional reasoning, we are going to be back here with the Court striking down what we pass out of here in the Wilson bill. And the question is not whether FISA or Congress can encroach on the Commander in Chief's inherent Constitutional authority. Of course we can't. No one is suggesting we can. That is a—that is a constitutional problem. The question is whether FISA is encroaching. I don't believe it is. And to say that we can't encroach is really to add very little to the debate.

I have three questions that I would like to pose.

Why is it, Mr. Deitz, that when Foreigner A talks to Foreigner B on foreign soil this is covered by FISA, because I don't understand that.

Number two, why can't the administrative burdens you alluded to be overcome either with greater resources or minor changes that accommodate the—the internal department approval, which seems to be a bigger problem than the 72 hours after the fact. Why can't that administrative burden be overcome with resources?

And, third, why are you coming to us now? Why during the PATRIOT reauthorization where we made changes to FISA did the Administration tell the Senate we didn't need to change FISA because it was working just fine as it was? Why now?

Mr. Bradbury, you say this is the most criticized program in NSA history. That may be true. But the only reason that may be true is because the *New York Times* leaked it, or this Committee would know nothing about this still. So you get little credit for the oversight we are doing about this program, because it wasn't invited by the Administration by any means.

Those are the three questions that I have.

Mr. DEITZ. I will try to be as brief as I possibly think I can. I think twice before, I have referred to the fact that I would be delighted to explain the technology problems that we now face and that the proposed legislation of Senator Specter and the proposed legislation of Congressman Wilson would help to alleviate, and it has to do—I do not as general counsel of NSA, I do not want to be in the position of helping or laying out a legal memo for terrorists to follow while negotiating U.S. law. So that is why I am not longing to do it publicly, but I am willing to do that privately in appropriate circumstances. And, again, I have offered that twice.

I don't expect you all to buy a pig in a poke. I wouldn't either.

Mr. SCHIFF. Does that mean, Mr. Deitz, this argument of why when Foreigner A talks to Foreigner B on foreign soil it is covered by FISA, and that you will do that in a classified session?

Mr. DEITZ. The question of burdensome, the burdensome nature. This is not something that can be addressed through providing more resources. It has to do with the speed of watching what terrorists are doing on the communications networks. Some is not like in a normal judicial context where you can have a temporary restraining order or some way of holding everything stable while you move the judicial process. This is equivalent to stopping in the middle of a battlefield.

Mr. SCHIFF. Mr. Deitz, if I can interject here. If the problem is the pre-approval, not the 72 hours, then why not have a good-faith exception or good-faith safe harbor that where you have to act safely, and in the 72 hours after the fact the judge says well, you know, actually we don't think you had probable cause, where you can show you acted in good faith. You have a safe harbor. Why wouldn't, you know, something along those lines be adequate instead of, you know, the problem that Mr. Dempsey alluded to, there are people planning attacks on this country.

In the Cold War days, you are saying things have changed since the Cold War days. In the Cold War days we risked being annihilated by nuclear weapons from the Soviet Union. You could argue then as now that we can't wait until we are annihilated to do surveillance without a warrant.

Mr. DEITZ. That is a very different context, Congressman, and made it in some respects very much easier, because there we were attempting to obtain communications on dedicated lines. Today terrorists are using the same telephone lines and same Internet connections that all the rest of us are now using. So you simply can't go let us tap into the Minsk-Moscow line and obtain the intelligence we need. We are all on the same big giant network. And terrorists understand how those networks work, and we also know they understand how U.S. law works.

Mr. SCHIFF. They must understand it better than we do on the Committee.

Mr. DEITZ. When you last mentioned the most scrutinized program, this wasn't after the fact. When we began the Presidential TSP program, we knew that we had to do this program absolutely correctly and so from the moment that program began, I as the chief counsel at NSA, helped create a rigorous oversight program that eventually we were able to get the Inspector General involved in.

Mr. SCHIFF. So when Mr. Bradbury had said this is the most scrutinized program, I assume what you mean was scrutinized by Congress, not scrutinized within the NSA.

Mr. DEITZ. I thought he was referring to both.

Mr. COBLE. Mr. Schiff, I realize that Mr. Scott controls the time, but Mr. Bradbury has to leave at 4. So if you can wrap it up.

Mr. SCHIFF. I would be happy to. If I can make one last point and wrap up and yield to the Committee for whatever additional comments they wish to make.

When the PATRIOT bill came up, which I supported, the argument was made and I think it was a fair one, that technology had changed, that our laws had not changed; that we had a system where, you know, you used to go up on the stationary phone with a warrant and now people are using phones disposably and calling cards, et cetera. You were able to share enough about that with us to give us a comfort level that these changes are necessary.

Right now you are not able to share anything with us about why these changes weren't sought in the PATRIOT bill, why they weren't sought in the PATRIOT reauthorization, why they are somehow necessary now. So we don't have any of that information. And it is essentially an argument that you ought to trust us or you ought to trust people in the Intelligence Committee, because we

don't trust you on the Judiciary Committee to keep what we tell you in a classified hearing classified. That is troubling to me. And I would again urge that this Committee demand the information that we need to make intelligence decisions. And I yield to the Committee or the witnesses on any time I have remaining.

Mr. DEMPSEY. If I may, very briefly.

Mr. COBLE. Very briefly. I am wanting to wrap this thing up now.

Mr. DEMPSEY. Congressman Schiff, I think that on foreign to foreign, there has been a windfall to the intelligence agencies, which is good, which is that a large number of foreign-to-foreign communications pass through the United States. This is one of the changes in technology that they don't talk about quite so much because it benefits them. They talk about the changes to technology that make things harder for them, but this is one that makes it easier for them. A lot of foreign-to-foreign communications pass through the United States. There is a concern, apparently, that because FISA is territorial that somehow it applies. I read the text. I don't see it. But whatever the reason is—and that reason maybe can be given in a classified briefing—I think fixing that is a much narrower solution than what we see in the Wilson bill or some of the other legislation.

Another technology change that has occurred is that while a lot of international communications used to come by satellite, they now come by fiber. And FISA draws a distinction between radio and wire; requires a warrant for wire, doesn't require a warrant for a lot of radio stuff. Now, fine. Let's be technology neutral.

But another technological change that has occurred, and a sort of cultural or corporate change, is I think the corporations are much more willing to cooperate with the Government, and have the technical capability in many cases inside the United States to cooperate with the Government to isolate communications to and from a target, so that you can, wire or radio, have the kind of specificity that FISA had applied to the wire side.

Now, again, that is something I think that can be somewhat talked about publicly. I have no classified information here but I think everything I said is pretty true. These are much narrower problems than what is being dealt with in this legislation, and I think the challenge for this Committee is to work partly in public hearings, partly in closed sessions, and nail down each one of these problems and figure out what is the narrow solution that will work, provide the flexibility, but provide the checks and balances.

Mr. SCHIFF. Thank you for the time, Mr. Dempsey. I think you hit the nail right on the head.

Mr. COBLE. Thank you, sir. Mr. Bradbury, I realize you have to depart at 4 o'clock.

The gentleman from Arizona.

Mr. FLAKE. Thank you, Mr. Chairman.

Mr. Bradbury, in the Wilson bill, the process for FISA applications are streamlined so that applicants no longer have to give an explanation about why they are looking for a wiretap or wire to wear—I am sorry—why they are looking to wiretap a person or search a person's home. That is, the language we have actually pre-

vents some kind of fishing expeditions. This one seems to get rid of that.

Do you have any concerns about that and why should we believe that we won't have fishing expeditions?

Mr. BRADBURY. Congressman, we actually would have some suggestions for Congresswoman Wilson on some of those provisions. We think a balance can be struck that streamlines the process, reduces the paperwork that Mr. Deitz described, but provides the necessary amount of information that the Court should have to make assessments for FISA orders.

Mr. FLAKE. Let me just echo what Congressman Schiff said about we are working in the dark here and it is difficult for us to recognize what streamlining means. We continually hear this but we don't have a—hear a good explanation and we are being asked to make sweeping changes without a good understanding of what is being streamlined, what point A is and how far we need to move to streamline to point B.

Mr. Deitz, with regard—let's go back to the minimization again.

Again, currently you say you have an Executive Order which requires you to, I guess, comply with the FISA regulations with regard to holding onto information longer than 72 hours.

Can you give the same unequivocal statement that you gave with regard to no other programs ongoing at this point, that you are disregarding of information pursuant to that Executive Order, information that is being gathered by an unintended target of investigation?

Mr. DEITZ. Let me first say the minimization rules long antedate FISA. The minimization rules have been around for a lengthy period of time. There are rules, and I don't think I am comfortable enough to give them to you here, but I would be happy to provide them. There are rules about how long materials that ought to be minimized can be kept before being discarded. So let me make it more positive. There is not in a bin somewhere in the basement of NSA a collection of all of the stuff that should have been minimized that is now being collected someplace else. That is not true.

Mr. FLAKE. So information is discarded after 72 hours?

Mr. DEITZ. I don't know if it is 72 hours. I don't have that rule off the top of my head.

Mr. FLAKE. Is it close?

Mr. DEITZ. I don't know the answer to that. I don't want to give it to you in a bad way. I will endeavor to provide that information to you.

Mr. DEMPSEY. The 72-hour rule only applies to surveillance conducted under 1802 of FISA, which is the so-called embassy exception which hasn't been used that much and which would be greatly broadened by the Wilson legislation. So I think I—the 72-hour rule only applies to information collected under 1802, that is, warrantless surveillance of a dedicated facility where there is no reasonable likelihood that a U.S. person's communications would be intercepted inside the United States. There is not a heck of a lot of that anyhow, so it is my understanding it hasn't been much used.

Mr. FLAKE. Do you concern—share the concern I have with regard to the Wilson bill with striking subsection 4 with regard to the minimization procedures?

Mr. DEMPSEY. Because of the broad expansion of 1802, so they are both striking the minimization requirement and saying that now you can conduct a warrantless surveillance inside the United States where you expect that you will acquire the communications of U.S. persons and keep them longer than the 72 hours.

Mr. FLAKE. Thank you. What if you go to a FISA judge that turns you down? Can you go to another?

Mr. BRADBURY. There are 11 district judges that sit on the FISA court, appointed by the Chief Justice. They are all excellent judges. The Department has a good relationship with the Court. The Department does not forum shop. The Department comes up 1 week at a time, and as intelligence matters come up, we don't have the luxury of waiting a week or 2 weeks, typically. So you bring it to the judge who is available at that time and each judge operates separately, though they work very well together.

Mr. FLAKE. I understand there are current prohibitions against forum shopping that would be knocked out with the Wilson legislation; is that your understanding?

Mr. BRADBURY. I am not familiar with that.

Mr. FLAKE. With regard to forum shopping, can you—usually I believe it is prohibited from going to one judge if another has turned you down. But the Wilson language, I understand, would turn that—get rid of that provision or prohibition.

Mr. DEMPSEY. There is such a provision in the Specter legislation, I think, but I am not sure if it is in Wilson.

Mr. COBLE. Thank you.

Mr. FLAKE. Thank you, Mr. Chair.

Mr. COBLE. The distinguished gentleman from Massachusetts.

Mr. DELAHUNT. I want to just raise the unfortunate reality that I have read the transmittal to the Chairman of the Full Committee, Mr. Sensenbrenner, and it would appear that my muscle has become flaccid because the transmittal implicates a response to questions that were posed by the Attorney General on April 6th, some 4 or 5 months ago, as opposed to a response to the Wexler—you know, to the Wexler resolution of inquiry. So we are back to square one, if you will.

I want to be very brief. I just wanted to pick up something that Mr. Deitz said, you know, regarding scrutiny and the preparation that was given to the TSP.

Because it would appear that that scrutiny—and maybe he can clarify, Mr. Bradbury, you can clarify—certainly did not meet some of the concerns and qualms that prominent career professionals had in the Department of Justice. Reports were that there was great consternation among some members of the Department of Justice about the program. And in fact, on one occasion, there was a transmission or transmittal to the office of—the Oval Office I guess, in particular to the Vice President or his counsel, Mr. Addington, that there would not be a reauthorization, as was part of the Executive Order presumably creating the thing, and that there were negotiations going on that resulted in some sort of a compromise.

Mr. Bradbury? Mr. Deitz?

Mr. BRADBURY. Congressman, those matters relate to internal deliberations of the Executive Branch, and we are really not at liberty to discuss the discussion of the Executive Branch where it involves legal advice on decisions that the President is going to make. I would say that I think the Attorney General has made a comment or two in the past on those allegations and those news articles, and I would just refer you to those. It is really not, I think, appropriate for us here today to comment on that.

Mr. DELAHUNT. Mr. Deitz, would you care to——

Mr. DEITZ. I have nothing to add. I have no idea what goes on inside the Department of Justice. I am in the NSA.

Mr. DELAHUNT. I guess I would ask unanimous consent to submit for the record an article, I think it is from—it is Newsweek, entitled "Palace Revolt," where there is considerable attention to this issue.

So, Mr. Alt, I see where you are affiliated with the Ashcroft Center.

Mr. ALT. That is incorrect. Ashburn.

Mr. DELAHUNT. My apologies. But it would appear that some career professionals within the Department of Justice had some issues with the program as originally constituted. Presumably they were constitutional in nature. So that just simply to dismiss the concerns expressed here today as having no basis in constitutional law or constitutional jurisprudence, I would think that members of the Department of Justice—and let me reiterate that it is the Department of Justice as headed by the former Attorney General John Ashcroft that raised these very issues—if you presume there is some accuracy regarding the report out of Newsweek.

Mr. ALT. If I can respond to that. It has been a while since I have seen that article but I have read that piece. And my understanding is that as to how they related that the dispute didn't necessarily go to questions about the ability to perhaps do warrantless surveillance in the absence of FISA as a Fourth Amendment question, which I think is what we have been discussing today, what are the provisions which are what the Constitution requires in terms of what searches may be done? It went to the interpretation of Presidential power, the Presidential authority essentially under something like Justice.

Mr. DELAHUNT. Reclaiming my time. But clearly you heard Mr. Bradbury talk about one of the rationales for all of the—father program is the President's inherent constitutional power. I would call that a constitutional issue.

Mr. ALT. It is, but not actually one before the Committee, because you are looking at what Congress is going to authorize the President to do. That naturally would change the level of authority that the President would have. Under Justice Jackson's famous Steel case analysis of three levels of Presidential power were you to give the President authority under FISA to do this, his power would be at the highest ebb. The FISA court, by the way, suggested that even at the lowest ebb, even if FISA attempted to restrict the President's power, his inherent authority is sufficient. So there is an internal tussle at Justice, according to this article, as to the authority of the President if he was acting contrary to FISA; which,

again, there is debate about this, but it doesn't go to the Fourth Amendment question which is what most of the Members have been objecting to today, suggesting that in fact performing these sorts of warrantless wiretaps would tramp upon the Constitution, even if Congress permitted them to do so.

Mr. DELAHUNT. Reclaiming my time. My reading of it and I think the concerns that were expressed, while maybe some Members did not distinguish between Fourth Amendment and and Article II powers, they are part of the larger constitutional issue that I think this Committee, being the Judiciary Committee, ought to be interested in.

Mr. Dempsey, if you can do it quickly.

Mr. DEMPSEY. I have not been talking today only about what is constitutional and what is unconstitutional. I have been talking about what works. And the lesson of American history is that unfettered executive power does not work. And in 1978 Congress said we will take this Presidential power and we will limit it, and every court that has ever considered it has upheld that Constitutionally and it has well served our country. So I think that the focus and the checks and balances work and we should stick with them.

Mr. COBLE. The gentleman's time is expired.

The distinguished gentleman from Texas, Mr. Gohmert.

Mr. GOHMERT. Thank you. I realize we are running out of time and I will be brief with respect to my friend, the gentleman from Massachusetts. Interesting opportunity to admit some problems with flaccidity, but in any event to follow up on what he was addressing, we do need answers to requests that were made. We had made requests before I got here under the PATRIOT Act. It took, it seemed, like 9 months or so to get answers. And it sure does help us be able to support things that should be supported if we have answers and can substantiate the things that we believe are going on, but until we get answers we can't.

But let me comment. My friend from Texas had indicated there has been no declaration of war. So under the Constitution there is no war. Is it just—I can't let that go. She is right. There has been no declaration of war under the Constitution. But the fact is, in 1979 when I was at Fort Benning, Georgia, in the Army, we knew that an act of war was committed against the United States. When you attack a U.S. Embassy, you are attacking that country, and that happened. We refused to recognize that. We had a war declared against us by a foreign country: Iran.

In 1984, I believe it was, our barracks in Beirut was attacked. Our military was attacked. That is an act of war. And we did not do anything about it, though my hero, Ronald Reagan, was President.

In 1993 another act of war was committed, this time on this continent, at the World Trade Center. We refused—and the Administration refused to recognize that as an act of war. After that, things like the Khobar Towers, the U.S. Embassy, the infrastructure, the USS Cole. All of these acts of war were committed and they were not recognized as what they were: acts of war against this Nation.

So we can continue to play a game and act like we are not at war, and maybe we are not. But if we are not, it is a one-sided war and it is going to—and it is against this country, and we can figu-

ratively bury our heads in the sand and pretend there is not a war going on. And if we do that, we will leave our, figuratively, our rear ends exposed. And if you believe the reports of obesity in this country, that would leave what we call in the Army a target-rich environment here in the country, and we cannot afford to allow that to happen.

I appreciate the efforts of the NSA and Mr. Deitz, you said I don't know what goes on inside the DOJ. Mr. Bradbury, I am glad to know they don't have you under surveillance at this time to know what you are doing in the DOJ, but I appreciate that admission. But seriously, we do need answers to the requests that have been made. Please don't play games with us. You know, there are those who want to help, but we can't if we are having games played with us. And we all do need to work together, and I hope we can work in a bipartisan manner to address the war that has been declared against us, whether people want to recognize it or not.

I yield back my time.

Mr. COBLE. Finally someone beat the red light. Congratulations to Texas.

The gentlelady from Texas, Ms. Jackson Lee. The pressure is on you for 5 minutes.

Ms. JACKSON LEE. It sure is, Mr. President, how challenging. This very issue in front of us, it is challenging, and that is what America is all about, that is what this democracy is all about, accepting challenges, if you will, unsurmountable tasks and really accomplishing them. And my good friend from Texas, I am always glad to be the clean-up hitter on his comments and for the opportunity to correct the, I think, the incorrect interpretation of my remarks. I want to remind him that the unfortunate attack on Pearl Harbor generated the response of the United States Congress to declare war. I will fault Presidents, Democratic and Republican, who have failed to come to the United States Congress and ask for a declaration of war, whether it was Vietnam, whether it was the Iran hostage situation or any other situation. I think that chips away at the edges of the constitutional structure of Government that the Founding Fathers were, frankly, very wise on.

We saw that misuse and abuse of the Constitution just a few years ago when we took to task a President on the basis of some private acts, and we utilized the Constitution in that instance. So the Constitution can be used or misused. What I would like to see is have it used appropriately.

And I want to go back to this whole point of certainty by both Mr. Bradbury and Mr. Deitz, that they seem to be just clear that no abuse of domestic-to-domestic intelligence gathering has occurred. I can't be that trustworthy and, as well, that confident. And frankly, I am going to raise again the point we need the kind of briefing that will assure us that this is in fact the case.

I am looking at Mr. Dempsey's comments in his statement, and he made a point that I think is worth putting on the record again. I am not sure if he said it in his remarks. In the other body, Senator Feinstein, one of the Members of the Special Senate Intelligence Committee that received classified briefings about the President's program concluded that the appropriate legislative response would be a bill that narrowly focused on the issues of the

Administrations that caused it to circumvent FISA; namely, the need for more resources, which is what Mr. Deitz said was needed. And particularly he made a point about we can't waste the time of analysts. We need more analysts. Let us give you more resources narrowly focused on the issues the Administration said it needed, and that is, of course, more resources, greater speed in approving FISA's application, and more flexibility to begin wiretapping in an emergency situation.

Ms. JACKSON LEE. And those are reasonable responses. The Wilson bill, and I think the DeWine—and I have not given all of my attention—far exceeds any of that. The Wilson bill also does the unpardonable, which it closes the door to congressional oversight as I have interpreted it.

So if I can get a quick response to this question: Mr. Dempsey, I don't know if you dabble in classified and intelligence matters, and if you are speaking from that perspective or strictly the constitutional perspective. But if we look at the logistical aspect, don't you think it would be worthy if Members of Congress who are duly elected to represent the people, who by the way have made—across partisan lines, raised their voice of outrage on this lawn mower, vacuum cleaner, if you will, sweeper suction pipe, whatever you want to say, of data collecting, would it not be logistically appropriate for Members of Congress in classified briefings to understand the A, B, Cs and craft legislation that, one, may not suffer constitutional frailties and/or punish the American people for the existence of their citizenship?

Mr. DEMPSEY. I think that the Intelligence Committees are not a creation of the Constitution. I think the oversight, their responsibility, is held by Congress as a whole. I think if you go back to the original drafting of FISA, it was done by the Intelligence Committees and they received—in classified session and in public session—fully the information that they needed to draft that legislation.

Ms. JACKSON LEE. It gave the Judiciary some jurisdiction.

Mr. DEMPSEY. So I think that this Committee continues to have full authority.

The fact is, of course, the President can stiff you, and as Congressman Lungren said, then your only real power is the power of the purse. And I think that, you know, those kinds of disputes have played out over history in terms of the push and tug between the President and the Executive Branch.

I think we are in one of those pushes and pulls right now. I think we have a President with some radical notions of Executive authority. All Presidents have asserted executive authority and have resisted congressional oversight.

Ms. JACKSON LEE. If I can reclaim my time, because I do want the Administration to be able to answer, frankly. I think the push and pull is valid, but I think leaving us empty handed and with a bag of money as our only option of oversight is both frustrating and also pocked with holes. We need to write legislation that, frankly, in this instance of the war on terror—undeclared war but in terms of what we are engaged in, the precipitous acts of terror which we have to address, the Congress has not divided, except for my good friends' failure sometimes to fully question their own Ad-

ministration on the tools. And therefore I don't think we should be relegated to cutting your money off.

What we should be doing is writing the right kind of legislation that is not one-sided, that is not Republican legislation, but is bipartisan legislation. And the only thing the Administration has come here to say is, go ahead with the Republican legislation, which I think is full of holes.

So I would offer to say, why can't we—and again you are going to offer the policy question, so I will let you be the person to take the message back—get the facts and write legislation that answers the Administration's concerns, but provides the oversight that the American people deserve? And, again, I might say to you that the British busting of that terrorist act was confined, as I understand it, to their guidelines utilizing the Secretary of State. It was good police work and good intelligence, and it didn't engage in the obliteration of their provisions of constitutional soundness or their provisions of soundness or the rights of their citizens. And so I offer to say we don't need to either.

Mr. Bradbury, will you try to answer the question?

Mr. BRADBURY. Thank you, Congresswoman.

I would just point out that Representative Wilson's bill includes a section 9 on congressional oversight. And in her provision she has a provision, subsection 3 on page 17, that says each report submitted under this subsection shall include reports on electronic surveillance conducted without a court order.

So there is an oversight provision in Representative Wilson's bill.

Ms. JACKSON LEE. And you don't mind if we could make the oversight broader and stronger in compliance with our understanding of the need? Again, I don't think you are going to go anywhere with the single bill written by a single Republican that the Administration has now adopted. And I think my friends have made a point very well taken. Ninety days out before an election is not a time to play politics with who writes a bill. The bill needs to be bipartisan because that is what the American people are wanting, a bill that fills all the holes that we think are now in the President's private or secret program.

Mr. BRADBURY. I am sorry; I wanted to also add that under the National Security Act, the Intelligence Committees receive oversight briefings of all kinds on intelligence programs of the United States, including surveillance programs of the NSA and other agencies that are outside the scope of FISA. So those oversight reports are going to go on.

Ms. JACKSON LEE. But you are the implementer and you are the Department of Justice and that is the oversight under this Judiciary Committee and that is where part of the failure is.

Yes, sir?

Mr. DEITZ. If I could make two small points, Congresswoman Jackson Lee. The first is—well, my testimony is designed to show the shortcomings of FISA. Even if we had all the resources in the world, why should we spend those resources on FISA's protecting non-U.S. persons? And that is what the current FISA does in many contexts. In other words, it is not just restricted to protecting U.S. persons. It is now protecting people that have no entitlement to

constitutional protection. And so that is why NSA is—my testimony reads the way it does and why we are supporting changes.

Second is just a small point. One has to be very careful in comparing British warrants with U.S. warrants. In fact, our Fourth Amendment reflects the difference between U.S. warrants and British warrants.

Thank you.

Ms. JACKSON LEE. Mr. Chairman, let me just conclude and thank you for your courtesies. That is—you have just answered our request to have the kind of classified briefings for this Committee, Judiciary, so that I can be convinced that we are spending resources and protecting the rights of other than citizens due the constitutional privilege. You are saying it, of course, but my question is—and you won't be able to answer it, and I will put it on the record—that there are certainly merits to ensure that our citizens' rights are protected, and if by chance there is a spillover of either coverage or resources to make sure that our citizens' rights are protected, so be it.

But in an explanation that is classified I assume you could be more probative and more detailed in your response. I don't think we have gotten anywhere to convince us that we cannot do this within the confines of a constitutional premise of FISA initiative that is either secure or more secure or more helpful to any executive, whether it is this one or the next one. And I believe it is going to be very difficult to do this if my good friends run over us without the facts that are necessary to write the right kind of legislation.

Mr. DEITZ. If I can just say, Congresswoman, I have a couple of times today averred to the fact that in closed session I would be happy to go into details, as much detail as you want, explaining precisely what the problems are with FISA as it exists today.

Mr. COBLE. Mr. Deitz, I didn't hear what you said. You said there is a difference between American and British what?

Mr. DEITZ. Under the Fourth Amendment—actually the British general warrants.

Mr. COBLE. Okay. I did not——

Mr. DEITZ. General warrants in England, as we are always tweaking our British colleagues, British warrants still exist.

Ms. JACKSON LEE. But it is under a procedure, Mr. Chairman; that is the difference.

Mr. COBLE. You indicated, Mr. Dempsey, that the Intelligence Subcommittees formulated FISA, but I think that the Judiciary Committee was also involved.

Ms. JACKSON LEE. Thank you, Mr. Chairman. And I indicated that we had the jurisdiction.

Mr. DEMPSEY. Mr. Chairman, if I did say that, I misspoke. I meant to say that it was the Judiciary Committees that played a major role in that.

Ms. JACKSON LEE. You misspoke.

Mr. COBLE. We have run a marathon today, and I am going to recognize the distinguished Ranking Member who wants to conclude this marathon.

Mr. SCOTT. Thank you, Mr. Chairman. I appreciate the opportunity to say a final word.

We have been asked to expand the situations where there would be warrantless searches, warrantless wiretaps, and what has leaked out so far are situations which clearly ought to be—people ought to be able to get a warrant. If you have a known al-Qaeda member calling in the United States, you ought to be able to get a warrant.

Again, we don't know what is going on. We have been told that the witnesses before us won't tell us what is going on. Mr. Deitz has indicated he will tell us the problems, but has indicated what is going on is above his pay grade as to who gets to know that.

Since what has been leaked out are obviously situations for which you could get a warrant, we are not talking about whether you wiretap or not, but whether you will get a warrant before or after you begin the wiretap.

In a democracy, we have checks and balances. The Administration witness makes it clear that the Administration believes that the check and balance means the Executive Branch checking on itself.

Some of us—and traditionally the case has been, the check and balance means another branch of Government gets to review the situation, and in this situation it is the court, getting a warrant through a court. And what they are asking now is to go warrantless, which means essentially no checks and balances from the other branch.

Finally, Mr. Chairman, I think a number of us are unwilling to consider any legislation without knowing exactly what is going on, particularly since several of the bills will again expand the situations where there will be warrantless searches and warrantless wiretaps without any articulated reason, because the situations that have been articulated are clearly situations where a warrant can be obtained today.

Mr. COBLE. I thank the gentleman. The marathon concludes.

Mr. Deitz, in conclusion, I would like to reiterate what I said earlier. That is that you and the NSA people do appear regularly before the House and Senate Intelligence Committees and the Republican and Democrat leadership. So I want everyone to understand that clearly.

Mr. Bradbury, we are going to get you out of here belatedly, but I thank you all for your testimony. We appreciate your contribution.

In order to ensure a full record and adequate consideration of this important issue, the record will be left open for additional submissions for 7 days. Within that—also any written question that a Member wants to submit should be submitted within the same 7-day period.

This concludes the legislative hearing, Legislative Proposals to Update the Foreign Intelligence Surveillance Act (FISA).

Thank you all for your cooperation, and the Subcommittee stands adjourned.

[Whereupon, at 4:17 p.m., the Subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

PREPARED STATEMENT OF THE HONORABLE ROBERT C. SCOTT, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF VIRGINIA AND RANKING MEMBER, SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

Mr. Chairman. I want to thank you for holding this hearing on the various proposals to address the NSA domestic surveillance issue. However, this is a much broader issue than encompassed by the various proposals and certainly more broad than any one witness from the minority side can hope to adequately address in a 5 minute statement. So, I am hopeful that this is merely the start of a series of hearings on this subject area. I look forward to working with you to fully explore the issue of how our government can appropriately and effectively conduct surveillance on those who would harm Americans without the government harming Americans through violations of their rights, freedoms, privacies and protections under law.

When law enforcement or intelligence officials have something or someone on which they deem it appropriate to conduct surveillance, I find it insulting and disingenuous to our system of laws and procedures for someone to suggest it is inconvenient to comply with them by obtaining a warrant or a court order. And it is not adequate or consistent with our system of checks and balances of government authority and power to suggest that notifying Congress under circumstances where members can go to jail for discussing what you tell them. Unfortunately, under the proposals before us that are likely to get consideration, here we go again using terrorism as a basis to greatly expand the government's authority to conduct surveillance on innocent Americans in the U.S. without having to prove to a court, or any other detached entity, that there is any reasonable basis for such surveillance.

First of all, we don't even know what kind of surveillance is currently being done by NSA. The logic used by the Administration to listen in on calls applies equally to wholly domestic calls as to foreign calls. Yet, without any public or otherwise effective oversight and assessment of whether what the President, through the NSA, is doing in secretly conducting surveillance on Americans is legal, we are not only designating it as legal in the majority proposals, but greatly expanding his opportunity to do so.

We have seen in numerous instances that this Administration sees itself as above traditional boundaries of law. We saw this with the process for declaring people as enemy combatants, including some who are American citizens, holding them indefinitely with no end in sight and depriving them of all rights and remedies to even contest their designation. And when the Administration finally did have to acknowledge the necessity for charging and trying the accused persons, the decision was made to try them through military tribunals. We also saw this same approach in the policies promoted by the torture memorandum leading to the Abu Ghraib torture incidents. In addition, we saw it with the Attorney General's decision to listen in on Attorney/client conversations for detained persons and now with the previously secret decision to listen in on conversations of Americans coming into or going out of the country, and whatever else they are doing in the NSA domestic program. We don't know because we have not called upon them to account to this oversight committee. All of these activities avoid any approval or scrutiny of the courts. We only find out what the true nature of what is happening when it is brought into the courts through challenges to its constitutionality as we found with the *Padilla* and *Hamdan* cases. And now we see it with the NSA case brought by the ACLU which is working its way through the courts after the initial finding of unconstitutionality. So, instead of moving now to try to cloak the Activity in a veil of legitimacy through legislation, we should await the court's final determination, or simply

have the Administration proceed on its indication that it would seek the FISA court's approval of its activities.

It is simply unacceptable to Americans that a call made or received by a citizen in this country can be listened to or otherwise intercepted by the government without approval, or review by a court with authority to authorize or deny such interception based whether good cause is shown under law. To do so is tantamount to operating under a police state and at variance with some of the most important principles upon which this nation was founded.

And all of this done without any presentation or indication of a need for such sweeping additional government authority over citizens' private affairs, or any credible evidence or findings of any inadequacies in current law to justify such a drastic change in law. The one productive thing of note the Wilson/Sensenbrenner and Specter bills do, by analogy, is confirm that the current NSA surveillance activity is patently illegal or there would not be a need for such sweeping expansion of foreign intelligence surveillance powers.

So, I hope we will carefully study this issue, Mr. Chairman, and move to require the Administration to come into compliance with existing law. There is no inconsistency in protecting us from terrorism and remaining a country which operates under the rule of law. We should first assure complyiance with existing law and then determine whether any changes are needed to provide for greater effectiveness and efficiency on the part of law enforcement, not try to change the law provide for what law enforcement is doing after the fact. I look forward to the testimony of our witnesses on this important issue.

PREPARED STATEMENT OF THE HONORABLE JOHN CONYERS, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN AND RANKING MEMBER, COMMITTEE ON THE JUDICIARY

Let me state at the outset that I strongly support intercepting each and every conversation involving al Qaeda and its supporters - whether in the United States or abroad. Having said that, I have serious concerns about this Committee taking up legislation that simply codifies an unlawful surveillance program and which further and unjustifiably expands the president's authority. My concerns include the following:

First, it has yet to be explained why we need to gut the Foreign Intelligence Surveillance Act (FISA) and the Fourth Amendment in order to protect our citizens. The current law already allows for streamlined court approved wiretaps and includes an emergency exception which allows wiretapping without a court order for up to 72 hours. If the Attorney General needs more resources, additional time, or the ability to delegate this responsibility to other trusted officials, I am sure the Members of this Committee could come together to do that. However, there appears to be no cause to revamp FISA on the fly and permit the wholesale interception, storage, and unlimited usage of the contents of the communications of innocent Americans without a warrant.

Second, this Committee continues to be handicapped by the fact that nearly nine months after we first learned of the warrantless surveillance program, there has been no attempt to conduct an independent inquiry into its legality. Not only has Congress failed to conduct any sort of investigation, but the Administration summarily rejected all requests for special counsels as well as reviews by the Department of Justice and Department of Defense Inspector Generals. When the DOJ Office of Professional Responsibility finally opened an investigation, the President himself squashed it by denying the investigators security clearances. Furthermore, the DOJ has completely ignored the numerous questions posed by this committee, the Wexler Resolution of Inquiry we previously adopted, as well as our request for a full classified briefing on the program.

Third, we have not received a shred of evidence that the domestic spying program has led to actionable intelligence involving terrorism. FBI Director Mueller has stated that the warrantless surveillance program had not identified a single Al Qaeda representative in the United States since the September 11 attacks. A former prosecutor stated that "[t]he information [from the program] was so thin, and the connections were so remote, that they never led to anything, and I never heard any follow-up." An FBI official said the leads were "unproductive, prompting agents to joke that a new bunch of tips meant more calls to Pizza Hut."

So, given that emergency wiretaps are permitted under FISA, there has yet to be an independent review of the facts surrounding the domestic spying program, and the program has not yielded meaningful intelligence, how is it possible that this

Committee and this Congress appear to be on the verge of ratifying and enlarging an unlawful program two weeks before we adjourn? The GOP Leadership told The New York Times last week - they want to spend the next few weeks "concentrat[ing] on national security issues they believe play to their political strength." In other words, its politics, plain and simple.

If Congress were really serious about fighting terrorism, we would fully implement the 9/11 Commission recommendations. If we were truly interested in airline security, we would have developed a system to identify liquid explosives and to screen and inspect commercial air cargo. If we really cared about port security, we would screen more than 3% of containers before they enter our country, and secure our chemical plants. If we really cared about nuclear proliferation, we would work with the members of the former Soviet Union to adequately secure their "loose nukes." If we were serious about capturing or killing bin Laden, we wouldn't have outsourced the job to Afghanistan or broken up the CIA's bin Laden unit. And if we truly wanted to prevent terrorism, instead of spending $2 billion per week occupying Iraq, we would use those funds to protect our nation and secure our borders.

I believe that the lesson of the last five years is that if we allow intelligence, military and law enforcement to do their work free of political interference, if we give them requisite resources and modern technologies, if we allow them to "connect the dots" in a straight forward and non-partisan manner, we can protect our citizens. We all want to fight terrorism, but we need to fight it the right way, consistent with our Constitution, and in a manner that serves as a model for the rest of the world. This bill does not meet that test.

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON LEE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

I thank the Chairman and Ranking Member. I am also happy to welcome the witnesses who will help us understand whether there is a need to update the Foreign Intelligence Surveillance Act of 1978. I look forward to hearing their testimony. I must say, however, that I am very skeptical of the need to update FISA. I believe the statutory framework established by the Congress is more than adequate to the present crisis. What is needed is for the President to comply with the law and for the Congress to exercise oversight over the executive branch.

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. Proponents of changing this scheme bear a heavy burden of justification and so far, there has been no justification at all on the public record. To the contrary, the statements of the Bush Administration indicate that FISA is working well (when it is followed) and offer no justification for major changes to the Act.

In terms of the President's warrantless surveillance programs, there is still nothing on the public record about the nature and effectiveness of those programs to indicate that they require a legislative response, other than to reaffirm the exclusivity of FISA and insist that it be followed. This is accomplished by 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 Ranking Members of the Judiciary and Intelligence Committees, Mr. Conyers and Ms. Harman.

The Bush Administration must explain to Congress why it is necessary to change the law and Congress must satisfy itself that any recommended changes would be constitutionally permissible. Congress needs this information both to responsibly carry out its duty to legislate and to fulfill its obligation to oversee surveillance activities inside the United States, ensuring that they protect national security, safeguard civil liberties, and comply with the Fourth Amendment.

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. As Chairman Hoekstra himself recently said in his letter to the President, "Congress simply should not have to play Twenty Questions to get the information that it deserves under our Constitution." 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 in-

formation 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.

Before Congress can even begin to discuss amending FISA, it must consider how the statute works, the technology used, and the operational reality of NSA activities inside the United States. The Bush Administration has not identified any technological barriers to the operation of FISA. Moreover, most of the legislative proposals to amend FISA do not attempt to "modernize" the law, but rather erode Fourth Amendment protections since available technology *allows* the interception of more communications. In addition, it is important to note that in the Patriot Act and in subsequent legislation, Congress has repeatedly amended FISA to loosen its standards in response to the Bush Administration's request to "modernize" the statute. 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.

Although expansion of FISA surveillance authority is inappropriate, Congress should consider ways to improve FISA compliance, accountability, oversight, and transparency. As stated above, this requires a thorough investigation. Congress can and must conduct a thorough investigation without compromising national security. This is what happened thirty years ago during the Church Committee's investigation of domestic surveillance during the Cold War.

Thank you for convening this hearing Mr. Chairman and welcome to the witnesses.

I yield back the remainder of my time.

PREPARED STATEMENT OF THE HONORABLE JANE HARMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Thank you, Mr. Chairman, for allowing me to speak on this important issue.

As one of the few members of Congress briefed on the Domestic Surveillance Program, I know that all domestic surveillance can be conducted under the Foreign Intelligence Surveillance Act of 1978 (FISA). That is how Ranking Member Conyers and I arrived at the "Lawful Intelligence and Surveillance of Terrorists in an Emergency by NSA Act" (The LISTEN Act). The Act makes clear that any attempt to listen in on Americans must be conducted in accordance with FISA and Title III. It reiterates that FISA and Title III are the exclusive ways to conduct electronic surveillance of U.S. persons on U.S. soil and that the Authorization to Use Military Force, passed in October 2002, did not constitute authority to engage in electronic surveillance outside of FISA.

The President and Attorney General claim that the FISA process is too slow. For that reason, the LISTEN Act provides tools to process emergency warrant applications quickly, and authorizes funds to increase capabilities at the NSA and Department of Justice. It would require the President to report to Congress a plan for increasing resources and personnel and new information technology systems at the National Security Agency and the Department of Justice if he feels the current procedures are inadequate for fast and effective lawful surveillance.

The LISTEN Act is a narrowly-tailored bill, which gives the President precisely what he has said he needs, and no more.

Since we introduced it, the LISTEN Act has generated a strong record of support. Since then, the number of co-sponsors has increased to 64, including all 9 HPSCI Democrats, and we have received additional letters of support, from former Congressman Bob Barr, the ACLU, the Center for Democracy and Technology, the American Bar Association, the Open Society Policy Center and former Reagan Justice Department attorney Bruce Fein.

FISA has been modernized in 12 ways since 9/11 - we have enacted every change requested by the President.

I support the notion that FISA should be technology neutral - that is, that the legal protections should be the same whether the interception takes place on a fiber line or over the airwaves.

But some of the other proposals out there - including Congresswoman Wilson's bill - go well beyond that - and propose major changes to FISA that, in my view, are not necessary and are potentially very dangerous.

The many complicated loopholes of the Wilson bill and other proposals basically give the President a blank check to ignore the requirements of FISA. These bills basically make surveillance without a warrant the rule rather than the exception. We need to be extremely careful here.

Our Constitution requires particularized suspicion. The LISTEN Act preserves that. The Constitution isn't broken, and neither is FISA. I think we should follow a version of the Pottery Barn rule here - if it ain't broke. . .don't break it.

Thank you, Mr. Chairman.

LETTER FROM THE HONORABLE SHEILA JACKSON LEE TO THE HONORABLE F. JAMES SENSENBRENNER, JR., AND THE HONORABLE JOHN CONYERS, JR.

May 12, 2006

Hon. F. James Sensenbrenner, Jr., Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

Hon. John Conyers, Jr., Ranking Member
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

Re: Request for Hearing into NSA Domestic Surveillance Program

Dear Chairman Sensenbrenner and Ranking Member Conyers:

The shocking revelations that the National Security Agency has been secretly collecting the phone call records of tens of millions of Americans, using data provided by AT&T, Verizon, and BellSouth make it more important than ever for the Judiciary Committee to launch an immediate investigation of the massive NSA domestic surveillance program.

The collection of phone call records of tens of millions of Americans constitutes an invasion of privacy unprecedented in the history of the nation. Compounding this breach of public trust is the fact that the massive database was compiled with the secret but voluntary assistance of several major American corporations. According to the report published in USA Today yesterday, the usefulness of the NSA's domestic phone-call database as a counterterrorism tool is unclear. Also unknown is the extent to which the database has been used for other purposes. These and other subjects should be the focus of the hearings the Judiciary Committee should hold to ensure that the rights of American citizens are not being abridged by the NSA domestic surveillance program ordered by the White House.

Thank you for the serious consideration you will give this request. Please let me know if you would like additional information. I am available to discuss this matter with you at your earliest convenience.

Very truly yours,
Sheila Jackson Lee
Member of Congress

LETTER TO THE HONORABLE PETER HOEKSTRA AND THE HONORABLE JANE HARMAN FROM CAROLINE FREDRICKSON, DIRECTOR OF THE WASHINGTON LEGISLATIVE OFFICE, AND LISA GRAVES, SENIOR COUNSEL FOR LEGISLATIVE STRATEGY, AMERICAN CIVIL LIBERITIES UNION (ACLU)

WASHINGTON
[illegible]

July 27, 2006

The Honorable Peter Hoekstra, Chairman
The Honorable Jane Harman, Ranking Member
House Permanent Select Committee on Intelligence
United States House of Representatives
Washington, DC 20530

Re. Opposition to H.R. 5825, Reducing the Protections for US Persons under the Foreign Intelligence Surveillance Act

AMERICAN CIVIL
LIBERTIES UNION
WASHINGTON
[illegible]
915 15TH STREET, NW
WASHINGTON, DC 20005
[illegible]
[illegible]
www.aclu.org

CAROLINE FREDRICKSON
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
[illegible]

OFFICERS AND DIRECTORS
NADINE STROSSEN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

KENNETH B. CLARK
CHAIR, NATIONAL
ADVISORY COUNCIL

RICHARD ZACKS
TREASURER

Dear Congressman Hoekstra and Congresswoman Harman:

On behalf of the American Civil Liberties Union, and its hundreds of thousands of activists, members and fifty-three affiliates nationwide, we write to share with you our views on H.R. 5825, a bill that is intended to "update" the Foreign Intelligence Surveillance Act (FISA) but which basically endorses the wish list of the National Security Agency (NSA) to the detriment of Americans' rights. We strongly oppose the expanded surveillance powers proposed by this bill, which some have called the "NSA Wish List" bill, because it grants unchecked surveillance power to the agency. We ask that this letter be submitted for the record in the hearing on this bill and related proposals to weaken the civil liberties protections against warrantless surveillance of Americans.

We are particularly disappointed in the bill, given the independent, non-partisan approach the lead sponsor of this legislation had taken earlier this year when the revelations of warrantless surveillance of Americans first arose. It appears that the well-intentioned desire to restore this Committee's proper role as one of the important checks on national security surveillance in this country has somehow been joined by an opportunistic effort by the Administration to re-write FISA to reduce the rights of people in the U.S.

The result, unfortunately, is that the bill seems to endorse the President's extremely controversial claim that he need not abide by FISA and he should be given free rein to search Americans' communications or homes for extended periods without check. It is fair to say the bill authorizes far more than the President has admitted. We hope the sponsors of this bill will reconsider this approach and instead restore the rule of law by embracing the common sense approach charted by the Ranking Member.

We have two overarching concerns about H.R. 5825, which embodies scores of changes to FISA, changes we believe would result in legalizing a range of unauthorized surveillance programs without Congress being fully informed about what it is approving. First, the bill allows warrantless surveillance of all international calls and e-mails of Americans and businesses in the U.S., without any evidence that they are conspiring with al Qaeda or other foreign terrorist organizations. Second, because the bill pre-approves warrantless searches whenever U.S. territory is attacked, it in effect allows foreign terrorists to decide when fundamental constitutional rights are to be suspended.

Warrantless Wiretaps of Americans' International Calls and Emails. It has often been said that the devil is in the details and in this case it is in the definitions. One of the most profound changes in the law wrought by this bill is that it would redefine "electronic surveillance" so that it does not include "electronic surveillance" of Americans' international calls and e-mails. This across-the-board change would allow the monitoring of any and every phone call made to or from an American resident or citizen to friends, family members or businesses abroad. The same exemption for warrantless surveillance would apply to e-mail communications-- if any person in the electronic communication were abroad, the contents of the e-mail would have no privacy protections against U.S. government monitoring. This change is made worse by a provision that states that Americans' communications are only protected if the NSA "reasonably believes" all the senders and recipients are in the U.S.; if the NSA does not so believe, it need not seek a warrant.

These changes are unwarranted and unconstitutional. The bill would authorize the government to monitor calls and emails to or from Americans that are international, even if there is no evidence the person is conspiring with al Qaeda or doing anything wrong. (If an American were conspiring with an agent of al Qaeda, the government could get a warrant from the Foreign Intelligence Surveillance Court.) The bill's authorization of the warrantless surveillance of the communications of millions of innocent Americans is totally unjustified and would fundamentally alter the privacy of people in this free society. In the guise of "modernizing" FISA, the bill would destroy it and the rights it was written to protect.

Allowing warrantless monitoring of international calls and emails would turn back the clock to when the NSA, through Operation Shamrock, was obtaining the records of every single international telegraph sent by American residents and businesses. The Church-Pike Committee conducted extensive investigations into that secret operation's massive invasion of Americans' privacy and, quite properly, sought to end such unwarranted intrusions in the name of national security. That Committee was not afraid to hold public hearings and conduct investigations into the shocking revelations that the NSA was monitoring international telegrams, the precursor to e-mail, when a whistleblower revealed it. See "National Security Agency Reported Eavesdropping on Most Private

Cables," New York Times, Aug. 1, 1975. That Committee's thorough, non-partisan investigation produced the following details and documents about what was really going on, including:

- when the surveillance of Americans' communications began (through the disclosure of letters to and from participating companies);
- which companies initially refused but later cooperated and how such cooperation was obtained (there were claims that ITT would be the "only non-cooperative company on the project");
- how the government dealt with fears by the companies that the project was illegal or the FCC would learn they were violating regulations;
- that the Attorney General gave assurances that companies would be protected against any consequences;
- that responsible Administration officials had been unaware of the program for most of its existence;
- that the program was extracting information on innocent Americans;
- whether NSA employees and other government employees were also monitored by the NSA (they were);
- how many files were created by the NSA on American citizens;
- whether the files on Americans were focused on foreign threats or included "many prominent Americans in business, the performing arts, and politics, including members of Congress" (they did).

See Church Committee Report, Book III pp. 733-783. Ultimately, the predecessor to this Committee learned that millions of Americans' telegrams had been monitored by the NSA, with over a 100,000 analyzed each month.

Given the recalcitrance of the Administration, including its refusal to disclose even how much money is being spent on the unauthorized surveillance of people in this country, it would be difficult to believe this Committee has been given answers to these and related questions along with the documents needed to verify the Administration's claims. Yet, this Committee is rushing to consider legislation that would undo the lengthy deliberations of Congress to prevent such warrantless surveillance from ever happening again. We think it fair to question the wisdom of altering the protections for Americans at this juncture and in the face of such intransigence by the Administration.

There is no doubt the country faces significant national security challenges in the aftermath of the attacks of September 11th, but it is also fair to say that our nation–while abiding by FISA–faced and triumphed over foes at least as powerful as those who launched the September 11th attacks. When FISA was passed, America was in the deep winter of the Cold War facing a threat of nuclear annihilation with Soviet nuclear

warheads aimed at every major American city. And, it should go without saying that even in times of war the President is not a law unto himself—FISA's rules and criminal penalties have not been repealed, the Fourth Amendment has not been suspended, and the Constitution with its bedrock principle of checks and balances was not destroyed on September 11th. We must not allow our legacy of liberty to be rendered moot. Nothing less than the rule of law is at stake.

Expanding Warrantless Searches of Americans if the US Were Attacked. The bill would allow Americans' homes and businesses to be searched and domestic conversations to be wiretapped without any judicial check for extended periods. The bill would replace FISA's rules that say the President must get a warrant except for the first two weeks after a declaration of war, and instead would add provisions that allow warrantless physical searches and electronic surveillance of Americans in this country without any judicial check for two months in the case of a "armed attack."

And if there were a "terrorist attack" on any US territory, the bill would allow the President to monitor any Americans' conversations he chooses, without any judicial check, in 45-day increments. It would not matter whether the incident were small or far away—at a disco thousands of miles away in Guam or an embassy in Africa or through a lone gunman in the US—the President would be able to authorize the government to listen to the conversations of anyone in this country he thinks might be communicating with terrorists or who might have foreign intelligence information, without any judicial check at all. This "authorization" means Americans have rights only at the discretion of terrorists. Under this bill, their actions automatically trigger a statutory grant of extraordinary power to the Executive Branch to conduct secret searches, repeatedly, over a long period, and without judicial review. That is simply wrong for our country.

The bill requires blind trust that the President and future presidents will never misuse such a grant of power to secretly wiretap anyone they want. The bill also takes Congress out of the equation by not requiring a declaration of war nor even an authorization for the use of military force under the War Powers Act. The Constitution, however, does not give Congress the power to suspend the Fourth Amendment or delegate to the President such a "right" for unlimited 45-day period of warrantless surveillance. Congress cannot waive Americans' individual rights, let alone waive them in advance.

The bill is not saved by the provision that at the end of 90 days, the President would have the "option" of seeking a court order to continue to wiretap a US person he deems to be communicating with a terrorist. Under the bill, warrants are plainly not a mandatory check. The bill allows the President to opt out of the warrant requirement by informing each member of the Intelligence Committees whom he is still spying on

and why. Secret notice to Congress is no substitute for preventing warrantless surveillance of Americans. And the Committee does not perform a judicial function in adjudicating—along with granting or denying—individual surveillance of which it is informed.

These so-called emergency provisions of the bill grant vague and wide-reaching powers to the President. The war on terror is by its nature undefined and indefinite, and the President would be cast as the sole arbiter of this renewable warrantless surveillance period for decades to come. There is no retroactive check on the President to ensure he did not abuse this power and no way, other than the power of the purse, to stop the emergency the President declared from being extended repeatedly. Current law much more reasonably allows a one-time 15-day exemption in addition to three-day emergency wiretaps that are then subject to judicial check, unlike the searches allowed by this bill.

This unprecedented power transfer to the President comes when the Administration has shown itself unwilling to operate within the laws as written and willing to break the law whenever it finds the rules inconvenient. In front of the Senate Judiciary Committee last week, Attorney General Gonzales offered a novel legal argument: that no act by the President is illegal until the Supreme Court says it is. Department of Justice Oversight Before the Senate Judiciary Committee, 109th Cong. (July 18, 2006). This presumptuous claim of legality in the face of the plain language of statutes and decades of precedent is troubling in and of itself. If Congress now rewards the President with broad latitude to spy on Americans without a warrant, for any kind of attack and for as long as he wishes, our liberties may never recover.

In addition to these overarching concerns, we have further concerns about the substantial changes to the definitions of FISA that we would like to discuss with the Committee. The bill includes substantial revisions of 50 USC § 1802, allowing the government to sweep up Americans' conversations through a dragnet as long as the net is directed at the communications of foreign countries. In cities like Washington, DC, New York, Miami, Chicago, or San Francisco, for example, where local trunk lines include calls from foreign embassies, Americans' conversations could also be accessed. Current law requires no warrant if the target is a foreign embassy here and there is no substantial likelihood of intercepting Americans' conversations through the surveillance used on these foreign government communications. The bill would inexplicably delete that important protection while also changing the law to allow more American conversations to be kept, even though "unintentionally acquired." The bill would also expand warrantless access by allowing the Attorney General to obtain "stored communications" from landlords and other persons without a court order and compensate them for the secret cooperation. It is unclear how far into Americans' homes and businesses, where computers and telephones store emails and voicemails, the Attorney General could reach with these

changes.

Among our other concerns is the fact that the bill omits from its definition of a "surveillance device" Carnivore-like devices that extract or analyze data. With this omission, the bill exempts data mining – allowing secret agents of the government to comb through millions of innocent Americans' communications or other data for patterns – from the court order requirements. We are very concerned that this change could be interpreted to allow the government to operate this extensive program to track every call Americans make and receive without a court ever considering its legality, much less its effectiveness. Congress should not be authorizing the data mining of the records of innocent Americans. Our strong concerns about data mining are detailed in our letter to the Committee dated July 17, 2006, which we would ask to be included in the record. That letter also reiterates our endorsement of other legislation on these issues: the Harman-Conyers and Flake-Schiff bills that help restore the rule of law.

We ask the Committee to reaffirm its non-partisan roots and resist political pressure to go along with the White House, which has kept members of this Committee in the dark on matters clearly within its jurisdiction and responsibility. During extensive hearings on the Patriot Act's changes to FISA (at http://www.fas.org/sgp/crs/intel/m071906.pdf), the Administration did not claim it needed additional authorities like those this bill would authorize. We ask the Committee to forbear and hold additional hearings in order to get a better grasp on the extent to which the Administration has engaged in unlawful surveillance of American residents.

We also believe the bill should not move forward on the heels of Attorney General Alberto Gonzales' revelation that the President is blocking a Department of Justice investigation regarding the illegal NSA spying program. Rather than fire the investigators—as President Nixon did during the Saturday Night Massacre—President Bush denied them clearance to investigate. These are simply different routes to the same result: White House interference with a legitimate investigation by the Justice Department. The Committee should be investigating that obstruction and politicization.

Further, the bill fails to take into account recent judicial decisions that reiterated limits on presidential power. In a decision regarding a challenge to the NSA's warrantless surveillance, a federal court held last week that the Constitution protects the privacy of Americans' telephone conversations. See Hepting v. AT&T Corp., No. C-06-672 VRW (D. Calif. July 20, 2006). As the court noted, the NSA's dragnet-style programs monitoring Americans' telephone calls "violate the constitutional rights clearly established in Keith." Hepting at 68 (citing United States v. United States District Court, 407 U.S. 297 (1972)). This bill also ignores the crux of the Hamdan decision.

Already, the Administration has shown its disregard for the civil liberties of ordinary Americans by ordering spying on their communications without the judicial check required by law to protect individual rights. Already, the Administration has shown its willingness to act outside the law. Americans' privacy rights and Fourth Amendment protections are too valuable and too vulnerable for Congress to grant such expanded powers to the Executive Branch. Some might argue that this bill is no blank check, rather it is a check written to the Administration in the amount it wants, diminishing privacy rights and the checks and balances that protect them.

Accordingly, we urge the Committee to investigate thoroughly the ongoing illegal surveillance programs currently being conducted by the Administration, and we hope the Committee will reaffirm its vital role as a check on the Executive. We respectfully ask the members of the Committee to reject H.R. 5825 as a major setback for the civil liberties of all Americans.

Thank you for considering our views.

Sincerely,

Caroline Fredrickson
Director, Washington Legislative Office

Lisa Graves
Senior Counsel for Legislative Strategy

NEWSWEEK ARTICLE, "PALACE REVOLT," DATED FEBRUARY 6, 2006

PALACE REVOLT

They were loyal conservatives, and Bush appointees. They fought a quiet battle to rein in the president's power in the war on terror. And they paid a price for it. A NEWSWEEK investigation.

By Daniel Klaidman, Stuart Taylor Jr. and Evan Thomas
Newsweek

Feb. 6, 2006 issue - James Comey, a lanky, 6-foot-8 former prosecutor who looks a little like Jimmy Stewart, resigned as deputy attorney general in the summer of 2005. The press and public hardly noticed. Comey's farewell speech, delivered in the Great Hall of the Justice Department, contained all the predictable, if heartfelt, ap-

preciations. But mixed in among the platitudes was an unusual passage. Comey thanked "people who came to my office, or my home, or called my cell phone late at night, to quietly tell me when I was about to make a mistake; they were the people committed to getting it right—and to doing the right thing—whatever the price. These people," said Comey, "know who they are. Some of them did pay a price for their commitment to right, but they wouldn't have it any other way."

One of those people—a former assistant attorney general named Jack Goldsmith—was absent from the festivities and did not, for many months, hear Comey's grateful praise. In the summer of 2004, Goldsmith, 43, had left his post in George W. Bush's Washington to become a professor at Harvard Law School. Stocky, rumpled, genial, though possessing an enormous intellect, Goldsmith is known for his lack of pretense; he rarely talks about his time in government. In liberal Cambridge, Mass., he was at first snubbed in the community and mocked as an atrocity-abetting war criminal by his more knee-jerk colleagues. ICY WELCOME FOR NEW LAW PROF, headlined The Harvard Crimson.

They had no idea. Goldsmith was actually the opposite of what his detractors imagined. For nine months, from October 2003 to June 2004, he had been the central figure in a secret but intense rebellion of a small coterie of Bush administration lawyers. Their insurrection, described to NEWSWEEK by current and former administration officials who did not wish to be identified discussing confidential deliberations, is one of the most significant and intriguing untold stories of the war on terror.

These Justice Department lawyers, backed by their intrepid boss Comey, had stood up to the hard-liners, centered in the office of the vice president, who wanted to give the president virtually unlimited powers in the war on terror. Demanding that the White House stop using what they saw as farfetched rationales for riding rough-shod over the law and the Constitution, Goldsmith and the others fought to bring government spying and interrogation methods within the law. They did so at their peril; ostracized, some were denied promotions, while others left for more comfortable climes in private law firms and academia. Some went so far as to line up private lawyers in 2004, anticipating that the president's eavesdropping program would draw scrutiny from Congress, if not prosecutors. These government attorneys did not always succeed, but their efforts went a long way toward vindicating the principle of a nation of laws and not men.

The rebels were not whistle-blowers in the traditional sense. They did not want—indeed avoided—publicity. (Goldsmith confirmed public facts about himself but otherwise declined to comment. Comey also declined to comment.) They were not downtrodden career civil servants. Rather, they were conservative political appointees who had been friends and close colleagues of some of the true believers they were fighting against. They did not see the struggle in terms of black and white but in shades of gray—as painfully close calls with unavoidable pitfalls. They worried deeply about whether their principles might put Americans at home and abroad at risk. Their story has been obscured behind legalisms and the veil of secrecy over the White House. But it is a quietly dramatic profile in courage. (For its part the White House denies any internal strife. "The proposition of internal division in our fight against terrorism isn't based in fact," says Lea Anne McBride, a spokeswoman for Vice President Dick Cheney. "This administration is united in its commitment to protect Americans, defeat terrorism and grow democracy.")

The chief opponent of the rebels, though by no means the only one, was an equally obscure, but immensely powerful, lawyer-bureaucrat. Intense, workaholic (even by insane White House standards), David Addington, formerly counsel, now chief of staff to the vice president, is a righteous, ascetic public servant. According to those who know him, he does not care about fame, riches or the trappings of power. He takes the Metro to work, rather than use his White House parking pass, and refuses to even have his picture taken by the press. His habitual lunch is a bowl of gazpacho, eaten in the White House Mess. He is hardly anonymous inside the government, however. Presidential appointees quail before his volcanic temper, backed by assiduous preparation and acid sarcasm.

Addington, 49, has worked as an adviser to Dick Cheney off and on since Cheney was a member and Addington a staffer on the House Intelligence Committee in the mid-'80s. When Cheney became secretary of Defense in the Bush 41 administration, Addington served at the Pentagon as general counsel. When Cheney became vice president to Bush 43, he brought Addington into the White House as his lawyer. Counsel to the vice president is, in most administrations, worth less than the proverbial bucket of warm spit, but under Prime Minister Cheney, it became a vital power center, especially after 9/11.

Like his boss, Addington has long believed that the executive branch was pitifully weakened by the backlash from Vietnam and the Watergate scandal. Fearful of in-

vestigative reporters and congressional subpoenas, soldiers and spies had become timid—"risk averse" in bureaucratic jargon. To Addington and Cheney, the 9/11 attacks—and the threat of more and worse to come—were perfect justification for unleashing the CIA and other long-blunted weapons in the national-security arsenal. Secretary of Defense Donald Rumsfeld, who disdains lawyers, was ready to go. So, too, was CIA Director George Tenet—but only if his spooks had legal cover, so they wouldn't be left holding the bag if things went wrong.

Addington and a small band of like-minded lawyers set about providing that cover—a legal argument that the power of the president in time of war was virtually untrammeled. One of Addington's first jobs had been to draft a presidential order establishing military commissions to try unlawful combatants—terrorists caught on the global battlefield. The normal "interagency process"—getting agreement from lawyers at Defense, State, the intelligence agencies and so forth—proved glacial, as usual. So Addington, working with fellow conservative Deputy White House Counsel Timothy Flanigan, came up with a solution: cut virtually everyone else out. Addington is a purist, not a cynic; he does not believe he is in any way ignoring or twisting the law. It is also important to note that Addington was not sailing off on some personal crusade; he had the full backing of the president and vice president, who shared his views. But, steeped in bureaucratic experience and clear in his purpose, Addington was a ferocious infighter for his cause. (Addington declined to comment. But McBride, the vice president's spokeswoman, said, "David Addington has a long, distinguished record of public service. He's committed to the president's agenda.")

Inexperienced in national-security law, White House Counsel Alberto Gonzales was steered by more-expert lawyers like Addington and Flanigan. Others, like John Bellinger, the National Security Council's top lawyer, were simply not told what was going on. Addington and the hard-liners had particular disregard for Bellinger, who was considered a softie—mocked by Addington because he had lunch once a month or so with a pillar of the liberal-leaning legal establishment, the late Lloyd Cutler. When Addington and Flanigan produced a document—signed by Bush—that gave the president near-total authority over the prosecution of suspected terrorists, Bellinger burst into Gonzales's office, clearly upset, according to a source familiar with the episode. But it was too late.

Addington was just getting started. Minimizing dissent by going behind the backs of bureaucratic rivals was how he played the game. A potentially formidable obstacle, however, was the Justice Department's Office of Legal Counsel. The OLC is the most important government office you've never heard of. Among its bosses—before they went on the Supreme Court—were William Rehnquist and Antonin Scalia. Within the executive branch, including the Pentagon and CIA, the OLC acts as a kind of mini Supreme Court. Its carefully worded opinions are regarded as binding precedent—final say on what the president and all his agencies can and cannot legally do.

Addington found an ally in an OLC lawyer whose name—John Yoo—would later become synonymous with the notion that power is for the president to use as he sees fit in a time of war. Shortly after 9/11, Yoo wrote, in a formal OLC opinion, that Congress may not "place any limits on the President's determinations as to any terrorist threat, the amount of military force to be used in response, or the method, timing, and nature of the response."

The brainy, pleasant and supremely self-confident Yoo became Addington's main man at Justice, a prolific author of legal opinions granting the president maximum power during wartime. In the winter of 2002, the CIA began catching top Qaeda terrorists—so-called High Value Targets—like Abu Zubaydah. These hard-case jihadists proved resistant to normal methods of interrogation. In the fevered atmosphere of the time, the Bush administration feared a "second wave" attack from Qaeda sleeper cells still inside the United States. The CIA wanted legal permission to use "coercive methods."

An August 2002 OLC memo, signed by the then head of the OLC—Jay Bybee—but drafted by Yoo, gave the agency what it needed. The controversial document, which became famous as the "torture memo" when it leaked two years later, defined torture so narrowly that, short of maiming or killing a prisoner, interrogators had a free hand. What's more, the memo claimed license for the president to order methods that would be torture by anyone's definition—and to do it wholesale, and not just in specific cases. A very similar Yoo memo in March 2003 was even more expansive, authorizing military interrogators questioning terror suspects to ignore many criminal statutes—as well as the strict interrogation rules traditionally used by the military. Secretary of Defense Rumsfeld put some limits on interrogation techniques, and they were intended to be used only on true terror suspects. Perhaps inevitably, however, "coercive interrogation methods" spread from Guantanamo Bay,

which housed terror suspects, into prisons like Abu Ghraib, where detainees could be almost anyone. (Poor leadership in the chain of command and on the ground was partly to blame, as well as loose or fuzzy legal rules.) The result: those grotesque images of Iraqis being humiliated by poorly trained and sadistic American prison guards, not to mention prisoners who have been brutalized and in some cases killed by interrogators in Afghanistan and elsewhere.

In the summer of 2003, Yoo, who stands by his body of work, left the Justice Department and returned to teaching law. His departure came in the midst of a critical power struggle. Addington and Gonzales had both wanted to make Yoo head of the OLC when Bybee went off to take a federal judgeship in March 2003, but Attorney General John Ashcroft balked. Ashcroft's reasons were apparently bureaucratic. (He declined to speak for this story.) According to colleagues, he resented Yoo's going behind his back to give the White House a private pipeline into the OLC. Yoo denied circumventing Ashcroft. "OLC kept the attorney general or his staff fully informed of all of its work in the war on terrorism," he said.

Jack Goldsmith, a law professor who was working in the general counsel's office at the Pentagon, was the eventual compromise choice to head the OLC. Goldsmith seemed like a natural fit. He was brilliant, a graduate of Oxford and Yale Law School, and he was conservative. Like Yoo, he was tagged a "New Sovereigntist" for his scholarly argument that international laws including prohibitions on human-rights abuses should not be treated as binding law by the U.S. courts.

But somehow, in the vetting of Goldsmith, one of his important views was overlooked. Goldsmith is no executive-power absolutist. What's more, his friends say, he did not intend to be a patsy for Addington and the hard-liners around Cheney. Goldsmith was not the first administration lawyer to push back against Addington & Co. At the CIA, general counsel Scott Muller had caused a stir by ruling that CIA agents could not join with the military in the interrogation of Iraqi prisoners. But Goldsmith became a rallying point for Justice Department lawyers who had legal qualms about the administration's stance.

Goldsmith soon served notice of his independence. Shortly after taking over the OLC in October 2003, he took the position that the so-called Fourth Geneva Convention—which bars the use of physical or moral coercion on prisoners held in a militarily occupied country—applied to all Iraqis, even if they were suspected of belonging to Al Qaeda.

Addington soon suffered pangs of buyer's remorse over Goldsmith. There was no way to simply ignore the new head of the OLC. Over time, Addington's heartburn grew much worse. In December, Goldsmith informed the Defense Department that Yoo's March 2003 torture memo was "under review" and could no longer be relied upon. It is almost unheard-of for an administration to overturn its own OLC opinions. Addington was beside himself. Later, in frequent face-to-face confrontations, he attacked Goldsmith for changing the rules in the middle of the game and putting brave men at risk, according to three former government officials, who declined to speak on the record given the sensitivity of the subject.

Addington's problems with Goldsmith were just beginning. In the jittery aftermath of 9/11, the Bush administration had pushed the top-secret National Security Agency to do a better and more expansive job of electronically eavesdropping on Al Qaeda's global communications. Under existing law—the Foreign Intelligence Surveillance Act, or FISA, adopted in 1978 as a post-Watergate reform—the NSA needed (in the opinion of most legal experts) to get a warrant to eavesdrop on communications coming into or going out of the United States. Reasoning that there was no time to obtain warrants from a secret court set up under FISA (a sometimes cumbersome process), the Bush administration justified going around the law by invoking a post-9/11 congressional resolution authorizing use of force against global terror. The eavesdropping program was very closely held, with cryptic briefings for only a few congressional leaders. Once again, Addington and his allies made sure that possible dissenters were cut out of the loop.

There was one catch: the secret program had to be reapproved by the attorney general every 45 days. It was Goldsmith's job to advise the A.G. on the legality of the program. In March 2004, John Ashcroft was in the hospital with a serious pancreatic condition. At Justice, Comey, Ashcroft's No. 2, was acting as attorney general. The grandson of an Irish cop and a former U.S. attorney from Manhattan, Comey, 45, is a straight arrow. (It was Comey who appointed his friend—the equally straitlaced and dogged Patrick Fitzgerald—to be the special prosecutor in the Valerie Plame leak-investigation case.) Goldsmith raised with Comey serious questions about the secret eavesdropping program, according to two sources familiar with the episode. He was joined by a former OLC lawyer, Patrick Philbin, who had become national-security aide to the deputy attorney general. Comey backed them up. The White House was told: no reauthorization.

The angry reaction bubbled up all the way to the Oval Office. President Bush, with his penchant for put-down nicknames, had begun referring to Comey as "Cuomey" or "Cuomo," apparently after former New York governor Mario Cuomo, who was notorious for his Hamlet-like indecision over whether to seek the Democratic presidential nomination in the 1980s. A high-level delegation—White House Counsel Gonzales and chief of staff Andy Card—visited Ashcroft in the hospital to appeal Comey's refusal. In pain and on medication, Ashcroft stood by his No. 2.

A compromise was finally worked out. The NSA was not compelled to go to the secret FISA court to get warrants, but Justice imposed tougher legal standards before permitting eavesdropping on communications into the United States. It was a victory for the Justice lawyers, and it drove Addington to new levels of vexation with Goldsmith.

Addington is a hard man to cross. Flanigan, his former White House colleague, described his M.O.: "David could go from zero to 150 very quickly. I'm not sure how much is temper and how much is for effect. At a meeting with government bureaucrats he might start out very calm. Then he would start with the sarcasm. He could say, 'We could do that, but that would give away *all* of the president's power.' All of a sudden here comes David Addington out of his chair. I'd think to myself we're not just dancing a minuet, there's a little slam dancing going on here." But Addington "usually had the facts, the law and the precedents on his side," says Flanigan. He had another huge advantage. He never needed to invoke Cheney's name, but everyone knew that he spoke for the vice president.

Addington was particularly biting with Goldsmith. During a long struggle over the legality of the August 2002 torture memo, Addington confronted Goldsmith, according to two sources who had heard accounts of the conversation: "Now that you've withdrawn legal opinions that the president of the United States has been relying on, I need you to go through all of OLC's opinions [relating to the war on terror] and let me know which ones you still stand by," Addington said.

Addington was taking a clever dig at Goldsmith—in effect, accusing him of undermining the entire edifice of OLC opinions. But he was not making a rhetorical point. Addington began keeping track of opinions in which he believed Goldsmith was getting wobbly—carrying a list inside his suit pocket.

Goldsmith was not unmoved by Addington's arguments, say his friends and colleagues. He told colleagues he openly worried that he might be putting soldiers and CIA officers in legal jeopardy. He did not want to weaken America's defenses against another terrorist attack. But he also wanted to uphold the law. Goldsmith, known for putting in long hours, went to new extremes as he reviewed the OLC opinions. Colleagues received e-mails from him at all hours of the night. His family—his wife, 3-year-old son and newborn baby boy—saw him less and less often. Sometimes he would take his older boy down to the Justice Department's Command Center on Saturdays, just to be near him.

By June 2004, the crisis came to a head when the torture memo leaked to The Washington Post. Goldsmith was worn out but still resolute. He told Ashcroft that he was formally withdrawing the August 2002 torture memo. With some prodding from Comey, Ashcroft again backed his DOJ lawyers—though he was not happy to engage in another battle with the White House. Comey, with Goldsmith and Philbin at his side, held a not-for-attribution background briefing to announce that the Justice Department was disavowing the August 2002 torture memo. At the same time, White House officials held their own press conference, in part to counter what they saw as Comey's grandstanding. A fierce behind-the-scenes bureaucratic fight dragged on until December, when the OLC issued a new memo that was hardly to the taste of human-rights activists but contained a much more defensible (and broader) definition of torture and was far less expansive about the power of the president to authorize coercive interrogation methods. The author of the revised memo, senior Justice Department lawyer Daniel Levin, fought pitched battles with the White House over its timing and contents; yet again, Comey's intervention was crucial in helping Levin and his allies carry the day.

By then, Goldsmith was gone from Justice. He and his wife (who is a poet) and two children had moved to Cambridge, where Goldsmith had taken a job on the Harvard Law faculty. Other dissenting lawyers had also moved on. Philbin, who had been the in-house favorite to become deputy solicitor general, saw his chances of securing any administration job derailed when Addington, who had come to see him as a turncoat on national-security issues, moved to block him from promotion, with Cheney's blessing; Philbin, who declined to comment, was planning a move into the private sector. Levin, whose battles with the White House took their toll on his political future as well, left for private practice. (Levin declined to comment.) Comey was working for a defense contractor.

But the national security/civil liberties pendulum was swinging. Bellinger, who had become legal adviser to Secretary of State Condoleezza Rice, began pushing, along with lawyers in the Pentagon, to roll back unduly harsh interrogation and detention policies. After the electronic eavesdropping program leaked in The New York Times in December 2005, Sen. Arlen Specter announced that the Senate Judiciary Committee would hold hearings that will start next week. The federal courts have increasingly begun resisting absolutist assertions of executive authority in the war on terror. After Cheney's chief of staff, Scooter Libby, pleaded not guilty to perjury charges in the Plame leak case, Addington took Libby's place. He is still a force to be reckoned with in the councils of power. And he still has the ear of the president and vice president; last week Bush was out vigorously defending warrantless eavesdropping. But, thanks to a few quietly determined lawyers, a healthy debate has at last begun.

H.RES. 819, REQUESTING THE PRESIDENT AND DIRECTING THE ATTORNEY GENERAL TO SUBMIT TO THE HOUSE OF REPRESENTATIVES ALL DOCUMENTS IN THE POSSESION OF THE PRESIDENT AND THE ATTORNEY GENERAL RELATING TO REQUESTS MADE BY THE NATIONAL SECURITY AGENCY AND OTHER FEDERAL AGENCIES TO TELEPHONE SERVICE PROVIDERS REQUESTING ACCESS TO TELEPHONE COMMUNICATIONS RECORDS OF PERSONS IN THE UNITED STATES AND COMMUNICATIONS ORIGINATING AND TERMINATING WITHIN THE UNITED STATES WITHOUT A WARRANT

IV

House Calendar No. 203

109TH CONGRESS
2D SESSION

H. RES. 819

[Report No. 109–527]

Requesting the President and directing the Attorney General to submit to the House of Representatives all documents in the possession of the President and the Attorney General relating to requests made by the National Security Agency and other Federal agencies to telephone service providers requesting access to telephone communications records of persons in the United States and communications originating and terminating within the United States without a warrant.

IN THE HOUSE OF REPRESENTATIVES

MAY 17, 2006

Mr. WEXLER submitted the following resolution; which was referred to the Committee on the Judiciary

JUNE 23, 2006

Referred to the House Calendar and ordered to be printed

RESOLUTION

Requesting the President and directing the Attorney General to submit to the House of Representatives all documents in the possession of the President and the Attorney General relating to requests made by the National Security Agency and other Federal agencies to telephone service providers requesting access to telephone communications records of persons in the United States and communica-

tions originating and terminating within the United States without a warrant.

Resolved, That the President is requested and the Attorney General is directed to submit to the House of Representatives, not later than 14 days after the date of the adoption of this resolution, all documents in the possession of the President and the Attorney General, including all legal opinions, relating to requests made without a warrant by the National Security Agency or other Federal departments and agencies to telephone service providers, including wireless telephone service providers, for access to telephone communications records of persons in the United States (other than as authorized under title I of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or chapter 119 or 121 of title 18, United States Code), subject to necessary redactions or requirements for handling classified documents.

110

House Calendar No. 203

109TH CONGRESS
2D SESSION

H. RES. 819

[Report No. 109–527]

RESOLUTION

Requesting the President and directing the Attorney General to submit to the House of Representatives all documents in the possession of the President and the Attorney General relating to requests made by the National Security Agency and other Federal agencies to telephone service providers requesting access to telephone communications records of persons in the United States and communications originating and terminating within the United States without a warrant.

JUNE 23, 2006

Referred to the House Calendar and ordered to be printed

○