



COPY

U.S. Department of Justice

National Security Division

Washington, D.C. 20530

APR 8 2008

Marcia Hofmann
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA. 94110

Re: FOIA #08-060

Dear Ms. Hofmann:

This is in further reference to your Freedom of Information Act (FOIA) request seeking access to "all agency records from September 1, 2007 to the present concerning briefings, discussions, or other exchanges that Justice Department officials have had with 1) members of the Senate or House of Representatives and 2) representatives or agents of telecommunications companies concerning amendments to FISA, including any discussion of immunizing telecommunications companies or holding them otherwise unaccountable for their role in government surveillance activities."

We appreciate your agreement to narrow the scope of your request removing the *Statements* and *Written Testimony* by the Assistant Attorney General for National Security before Congress (including the multiple drafts that were generated during the course of finalizing these statements). Six unclassified documents (totaling 24 pages) are being released to you in their entirety. This material is enclosed. We are currently reviewing the remaining thirty-four documents (totaling 191 pages) and completing consults with other agencies and Department of Justice components. We will notify you as soon as our consults are completed. Feel free to contact me at 202-616-5460, if you have any questions.

Sincerely,

GayLa D. Sessoms
FOIA Coordinator

Enclosures (6)

JOHN D. ROCKEFELLER IV, WEST VIRGINIA, CHAIRMAN
CHRISTOPHER S. BOND, MISSOURI, VICE CHAIRMAN

DIANNE FEINSTEIN, CALIFORNIA
RON WYDEN, OREGON
EVAN BAYH, INDIANA
BARBARA A. MIKULSKI, MARYLAND
RUSSELL D. FEINGOLD, WISCONSIN
BILL NELSON, FLORIDA
SHELDON WHITEHOUSE, RHODE ISLAND

JOHN WARNER, VIRGINIA
CHUCK HAGEL, NEBRASKA
SAMMY CHAMBLISS, GEORGIA
ORRIN HATCH, UTAH
OLYMPIA J. SNOWE, MAINE
RICHARD BURR, NORTH CAROLINA

United States Senate

SELECT COMMITTEE ON INTELLIGENCE
WASHINGTON, DC 20510-6476

SSCI #2007-3702

HARRY REID, NEVADA, EX OFFICIO
MITCH MCCONNELL, KENTUCKY, EX OFFICIO
EARL LEVIN, MICHIGAN, EX OFFICIO
JOHN MCCAIN, ARIZONA, EX OFFICIO

ANDREW W. JOHNSON, STAFF DIRECTOR
LEWIS B. TUCKER, MINORITY STAFF DIRECTOR
KATHLEEN P. MCGHEE, CHIEF CLERK

September 18, 2007

The Honorable Kenneth L. Wainstein
Assistant Attorney General for National Security
U.S. Department of Justice
Washington, D.C. 20505

Dear Mr. Wainstein:

The Senate Select Committee on Intelligence will conduct a closed hearing on the implementation of the Protect America Act and proposals to amend the Foreign Intelligence Surveillance Act on Thursday, September 20, 2007 at 2:30 p.m. in Room SH-219 of the Hart Senate Office Building. We request that you appear at this hearing to provide testimony and respond to questions. We also have requested that the Director of National Intelligence present testimony at the hearing and have invited other senior representatives from the Department of Justice, the Federal Bureau of Investigation, and the National Security Agency to appear and be prepared to respond to Member questions.

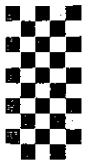
We request that a written copy of your testimony be provided to the Committee no later than Wednesday, September 19, 2007. We ask that you limit your oral remarks to ten minutes.

If your staff has any questions or would like to discuss this hearing further, please have them contact Ms. Christine Healey, of the Committee staff, at (202) 224-1700.

Sincerely,

John D. Rockefeller IV
Chairman

Christopher S. Bond
Vice Chairman



514-5778

Classification UNCLASSIFIED

3-9836



U.S. Senate
Select Committee on Intelligence

Fax Cover Sheet

To: KENNETH WAINSTEIN

From: ROCKEFELLER/BIND

SSCI#: 2007-3702

Date: 9/18/07

Time: 1200

Page 1 of 2

Prepared by: L Shepard

Note to Recipient:

If you did not receive every page of the facsimile, please call (202) 224-1771.

Classification Unclass

SILVESTRE REYES, TEXAS, CHAIRMAN

ALCEE L. HASTINGS, FLORIDA, VICE-CHAIRMAN
LEONARD L. BOSWELL, IOWA
ROBERT E. (BUD) CRAMER, JR., ALABAMA
ANNA G. ESHOD, CALIFORNIA
RUSH D. HOLT, NEW JERSEY
C.A. DUTCH RUPPERSBERGER, MARYLAND
JOHN F. TIERNEY, MASSACHUSETTS
MIKE THOMPSON, CALIFORNIA
JANICE D. SCHAKOWSKY, ILLINOIS
JAMES R. LANGEVIN, RHODE ISLAND
PATRICK J. MURPHY, PENNSYLVANIA

PETER HOEKSTRA, MICHIGAN, RANKING MEMBER
TERRY EVERETT, ALABAMA
ELTON GALLEGLY, CALIFORNIA
HEATHER WILSON, NEW MEXICO
MAC THORNBERRY, TEXAS
JOHN M. MCHUGH, NEW YORK
TODD TIAHRT, KANSAS
MIKE ROGERS, MICHIGAN
DARBELL E. ISSA, CALIFORNIA

NANCY PELOSI, SPEAKER
JOHN A. BOEHNER, REPUBLICAN LEADER

U.S. HOUSE OF REPRESENTATIVES
PERMANENT SELECT COMMITTEE
ON INTELLIGENCE

H-405, THE CAPITOL
WASHINGTON, DC 20515
(202) 225-7690

MICHAEL J. DELANEY
STAFF DIRECTOR

MICHAEL MEERMANS
MINORITY STAFF DIRECTOR

September 24, 2007

Assistant Attorney General Kenneth Wainstein
U.S. Department of Justice
National Security Division
950 Pennsylvania Avenue
Room 2200C
Washington DC, 20530

Dear Mr. Wainstein:

Enclosed are transcript pages containing your remarks at the Permanent Select Committee on Intelligence hearing on Thursday, September 20, 2007, on FISA. These transcript pages have not been revised or edited and are not for quotation or duplication.

In order to ensure the accuracy of your transcribed statements prior to publication of the hearing record, please review your statements and make only technical, grammatical, and typographical corrections. Please initial each correction in the margin, and fax the corrected transcript pages to the Committee, attention of Ms. Courtney Littig, Chief Clerk, at (202) 226-5068, by Friday, October 5, 2007.

Once you have faxed your corrections to the Committee, or if you have chosen not to make changes, please return the hard copy originals by mail to H-405, the Capitol. If the Committee does not receive your corrections by October 5th, the Committee will publish your statements as they appear in the enclosed transcript pages. If you have any questions, please contact the Chief Clerk at (202) 225-7690.

Thank you in advance for your attention to this matter.

Sincerely,


Silvestre Reyes
Chairman

JOHN CONYERS, JR., Michigan
CHAIRMAN

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

LAMAR S. SMITH, Texas
RANKING MINORITY MEMBER

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

ONE HUNDRED TENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6216

(202) 225-3951

<http://www.house.gov/judiciary>

September 12, 2007

The Honorable Kenneth Wainstein
Assistant Attorney General for National Security
Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Mr. Wainstein:

The House Committee on the Judiciary will hold a hearing on Tuesday, September 18, 2007, at 11:00 a.m. in room 2141 Rayburn House Office Building. The hearing is on Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights.

I would like to invite you to testify at this hearing. Please prepare a written statement for submission to the Committee prior to your appearance. The written statement may be as extensive as you wish and will be included in the hearing record. To allow sufficient time for questions at the hearing, please briefly highlight the most significant points of the written statement in an oral presentation lasting five minutes or less. Oral testimony at the hearing, including answers to questions, will be printed as part of the verbatim record of the hearing. Only transcription errors may be edited subsequent to the hearing.

To facilitate preparation for the hearing, please send an electronic copy of your written statement and curriculum vitae to the Committee 48 hours in advance of the hearing. The Committee will publish the statement on our website and, therefore, requests that you provide the documents in Word Perfect, Microsoft Word, or Adobe Acrobat. Please number all pages of the written statement, and attach a cover page with your name, position, date, and the title of the hearing. These documents may be e-mailed to Lou DeBaca on my staff at Lou.DeBaca@mail.house.gov.

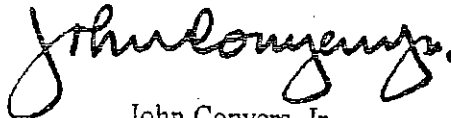
The Honorable Kenneth Wainstein
Page Two
September 12, 2007

In addition, the Committee requests that you provide 50 copies of your written statement to Lou DeBaca, 2138 Rayburn House Office Building, Washington, DC, 20515, 48 hours in advance of the hearing. Due to delays with our current mail delivery system, the copies should be hand delivered in an unsealed package. If this is not possible, please bring the copies with you the day of the hearing. Should you intend to introduce a published document or report as part of your written statement, I ask that you provide 60 copies for the hearing. Should such material be available on the Internet, please prepare a page containing citations to such material and provide the Committee with 50 copies.

If you have any questions or concerns, please contact Lou DeBaca on my staff at 202-225-3951.

I look forward to your participation in the hearing.

Sincerely,

A handwritten signature in black ink, reading "John Conyers, Jr." in a cursive style.

John Conyers, Jr.
Chairman

SILVESTRE REYES, TEXAS, CHAIRMAN

ALCEE L. HASTINGS, FLORIDA, VICE-CHAIRMAN
LEONARD L. BOSWELL, IOWA
ROBERT E. (BOB) CRAMER, JR., ALABAMA
ANNA G. ESHOO, CALIFORNIA
RUJIK D. HOLT, NEW JERSEY
C.A. DUTCH RUPPEBERGER, MARYLAND
JOHN F. TERREY, MASSACHUSETTS
MIKE THOMPSON, CALIFORNIA
JANICE D. SCHAKOWSKY, ILLINOIS
JAMES R. LANGRISH, RHODE ISLAND
PATRICK J. MURPHY, PENNSYLVANIA

PETER HOEKSTRA, MICHIGAN, RANKING MEMBER
TERRY EVERETT, ALABAMA
ELTON GALLEGLY, CALIFORNIA
HEATHER WILSON, NEW MEXICO
MAC THORNBERY, TEXAS
JOHN M. McHUGH, NEW YORK
TODD TIAHRT, KANSAS
MIKE ROGERS, MICHIGAN
DARRELL E. ISSA, CALIFORNIA

NANCY PELOSI, SPEAKER
JOHN A. BOEHNER, REPUBLICAN LEADER

U.S. HOUSE OF REPRESENTATIVES
PERMANENT SELECT COMMITTEE
ON INTELLIGENCE

H-405, THE CAPITOL
WASHINGTON, DC 20515
(202) 225-7690

MICHAEL J. DELANEY
STAFF DIRECTOR

MICHAEL MEERMANS
MINORITY STAFF DIRECTOR

September 11, 2007

Mr. Kenneth Wainstein
Assistant Attorney General, National Security Division
United States Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530

Dear Mr. Wainstein:

On Thursday, September 20, 2007, the House Permanent Select Committee on Intelligence will hold a hearing on the Foreign Intelligence Surveillance Act (FISA) and authorities for the National Security Agency (NSA) surveillance activities. The hearing will take place from 10:00 am until 1:00 pm. We will notify you as to the location once a hearing room has been designated. We cordially invite you to testify in this hearing that will begin as an open session and then move to a closed session.


On August 4, 2007, Congress passed legislation to adopt a temporary revision of FISA. The Committee seeks to understand the impact of these changes on the civil liberties of American citizens and the need for permanent modification to FISA. This hearing is one in a series of hearings the Committee will convene in the coming weeks to assess the future of FISA.

In preparing your testimony, please consider the following issues: (1) the legal authorities given to the NSA after September 11, 2001, to include the way in which the NSA operated under those authorities; (2) the legal authorities NSA operated under beginning in January 2007, after the President brought the publicly described "Terrorist Surveillance Program" to the Foreign Intelligence Surveillance Court, to include the way in which those authorities have evolved; (3) how NSA will operate under the legal authorities passed by Congress on August 4, 2007; (4) the impact the temporary changes have had on intelligence collection; (5) the question of retrospective liability for private sector entities that may have assisted the U.S. government in conducting surveillance after September 11, 2001; and (6) any permanent changes Congress should consider making to FISA when the temporary authorities expire.

Please provide your statement for the record by close of business on September 17, 2007 along with the names of any supporting attendees. Please limit your oral testimony to five minutes.

Questions regarding this hearing may be directed to Ms. Wyndee Parker, Deputy Staff Director and General Counsel, at 202-225-7690.

Sincerely,



Silvestre Reyes
Chairman



Peter Hockstra
Ranking Member

FISA Questions

General Questions

1. What are the consequences if the Congress does not reauthorize the Protect America Act?
2. Critics of the Protect America Act have suggested that it was passed in the dead of night, without sufficient consideration by Congress. When did the Administration propose legislation to modernize FISA and how many hearings were held on that topic prior to the vote on the Protect America Act? And how many further hearings have been held in the two months since we passed that Act?
3. Some argued that if a terrorist overseas happens to call into the United States, our intelligence agencies should have to go to the FISA Court to intercept that call. Why is this not a workable approach? What about a provision that requires the Intelligence Community to go to the FISA Court for authorization to collect a terrorist's calls if he calls into the United States more than a handful of times. Is that a workable approach?
4. Is it true that under the Protect America Act, as well as under the legislation reported out of the Senate Select Committee on Intelligence, all communications obtained are subject to minimization procedures just like communications obtained under FISA previously? Haven't those minimization procedures worked to protect the privacy of United States persons for the nearly 30 years they have been in place?

Senate and House Proposals

5. Does the Administration have any major concerns with the legislation recently reported out of the Senate Select Committee on Intelligence?
6. How does the legislation reported out of the Senate Select Committee on Intelligence compare to the RESTORE Act that was scheduled to be voted on in the House floor a few weeks ago?
7. It is my understanding that the RESTORE Act would require us to continue to obtain individual court approval to target persons overseas with respect to certain categories of intelligence. Isn't this a step backwards from the Protect America Act?
8. Both the Senate Intelligence Committee bill and the RESTORE Act contain sunset provisions. Haven't we given these questions more than enough consideration to put these new authorities on permanent footing, so that our intelligence professionals will have the certainty they need going forward?

9. The *Washington Post* described an amendment proposed by Senator Wyden, which would require new court approval of efforts to surveil U.S. persons overseas, as an “unnecessary and potentially disruptive precedent.” Do you agree? My understanding is that this amendment would impose requirements in the intelligence context that go beyond what we require in the criminal context for physical search warrants overseas. Is that correct?
10. Hasn't the existing process of surveilling U.S. persons overseas – which requires an individualized determination of probable cause by the Attorney General before surveillance can begin – served us well for decades? Senator Bond and three other Senators (including Senator Hatch) on the Intelligence Committee said in their report that this authority has “worked well” – why would we change it, when the very purpose of this legislation is to get the FISA Court out of the business of approving surveillance on overseas targets?

Immunity

11. Isn't it true that electronic surveillance for law enforcement and foreign intelligence purposes depends in great part on the assistance of private electronic communications service providers? What message does it send to companies if we do not protect them when they agree to help us?
12. Do you think that private electronic communications service providers are less likely to assist the government with its lawful surveillance activities if they are subject to potentially massive lawsuits based on allegations that they assisted the government?
13. Shouldn't private electronic communications service providers be entitled to rely, in good faith, on the government's representation that a particular intelligence activity was authorized by the President and was lawful?
14. Isn't it simply unfair to permit these companies – who are alleged merely to have done their patriotic duty and assisted the government in the aftermath of the horrific terrorist attacks of September 11, 2001 – to be subject to lawsuits brought by trial lawyers from across the nation?
15. Where a person has provided assistance to the Government pursuant to a written request or order, but it would harm the national security for the request for assistance to be disclosed, doesn't it make sense to create a procedure whereby cases challenging such assistance are dismissed without harming national security?

The Need for Permanent FISA Modernization

Changes in Communications Technology Have Drastically Expanded the Scope of FISA

- Congress enacted FISA in 1978 to regulate the use of electronic surveillance in the United States for foreign intelligence purposes.
 - Judicial review under FISA was designed to apply primarily to surveillance activities within the United States—where privacy interests are critically at stake—and not to overseas surveillance against foreign intelligence targets—where privacy interests are minimal or non-existent.
- However; as a result of changes in telecommunications technology since 1978, the scope of activities covered by FISA expanded to cover a wide range of intelligence activities that Congress intended to exclude in 1978.
 - This unintended expansion has hampered our intelligence capabilities and caused us to expend resources on obtaining court approval to conduct intelligence activities directed at foreign persons overseas.
- For example, prior to the passage of the Protect America Act of 2007, the Government often needed to obtain a court order before intelligence collection could begin against a target located overseas.
 - As a result, considerable resources of the Executive Branch and the FISA Court were being used to obtain court orders to monitor the communications of terrorist suspects and others abroad.
 - In essence, we effectively granted constitutional protection to foreign terrorists suspects overseas.
 - Moreover, this requirement sometimes slowed, and may have blocked, the Government's efforts to conduct surveillance that was potentially vital to the national security.
 - This expansion of FISA also diverted resources that would be better spent on protecting the privacy interests of United States persons here.

The Protect America Act Was a Step in the Right Direction

- The Protect America Act updated the definition of “electronic surveillance” to exclude surveillance directed at persons reasonably believed to be outside the United States.
 - The Protect America Act represented the right solution—allowing our intelligence agencies to surveil foreign intelligence targets located outside

the United States without prior court approval.

- The benefits provided by the Protect America Act have demonstrated the critical need to reauthorize the Act and to make its core authorities permanent.
 - Prior to the passage of the Protect America Act, the Director of National Intelligence testified that the Intelligence Community was unable to obtain the information that it needed to collect in a timely manner to protect the United States.
 - The Protect America Act has allowed us temporarily to close intelligence gaps that were caused by FISA's outdated provisions.
 - If we are to stay a step ahead of terrorists who want to attack the United States, Congress should make the core provisions of the PAA permanent to ensure that these intelligence gaps must remain closed.

**Senate Judiciary Committee Hearing on "FISA Amendments: How to Protect
Americans' Security and Privacy and Preserve the Rule of Law and Government
Accountability"**

Wednesday, October 31, 2007

**Questions Submitted by U.S. Senator Russell D. Feingold to Kenneth L. Wainstein
Assistant Attorney General**

1. The Senate Intelligence Committee bill provides new authority for targeting individuals 'reasonably' believed to be located overseas. That determination of the target's physical location prevents warrantless wiretapping of Americans inside the United States, so it is critical that the government establish effective procedures to make sure it only uses this authority to target people overseas. Under the bill, the government starts using its targeting procedures before submitting them to the court for approval. If the court ultimately rejects those procedures, and determines that they are not reasonably designed to ensure that only overseas targets are wiretapped using these new authorities, what does the bill say would happen to all the communications involving U.S. persons that were acquired using the unlawful procedures before the court rejected them?
2. Does the Justice Department believe that private sector liability for unlawful surveillance plays any role in the enforcement of U.S. privacy laws and in providing disincentives to engage in unlawful behavior?
3. The Intelligence Committee Report on the FISA bill declassified for the first time the fact that after September 11, 2001, the administration provided letters to communications service providers seeking their assistance with communications intelligence activities authorized by the President. What is the Justice Department's position as to whether those letters comply with the statutory immunity provision in existing law, which is in Section 2511(2)(a) of Title 18?
4. Five weeks ago, I asked DNI McConnell whether the administration could provide this Committee with information about how much U.S. person information is looked at and how much is disseminated, under the new authorities provided in the Protect America Act. He told me that the information was already being compiled and should be ready in a matter of weeks. As far as I am aware, that information has not yet been provided. When will the Judiciary Committee get that information?
5. The Senate Intelligence Committee bill, like the Protect America Act, amends FISA's definition of "electronic surveillance." The consequences of that change are unclear. Does the Administration believe that it is necessary to amend that key definition? Would the legislation have the same effect if it added new authorities

but allowed the new definition of electronic surveillance in the Protect America Act to expire?

6. The Intelligence Committee bill permits the executive branch to begin surveillance based on its own procedures, and requires that they be submitted to the court only after the fact. What would be the harm in having the court review and approve the procedures prior to using them, with a provision for going forward without prior judicial review in an emergency?
7. Do you agree that there is a greater potential for intrusions on Americans' privacy rights, mistaken or otherwise, if the government is intercepting international communications in the United States, as opposed to when the interception occurs overseas?
8. Do the new authorities provided in the Intelligence Committee-passed FISA bill authorize the acquisition, from inside the United States, of any foreign-to-foreign communications in which a target is not a communicant? Do they authorize such acquisition of any foreign-to-domestic communications in which a target is not a communicant? Do they authorize such acquisition of any domestic-to-domestic communications in which a target is not a communicant?
9. As defined in Section 2510(15) of Title 18, the term "electronic communication service" is quite broad, and covers "any service which provides to users thereof the ability to send or receive wire or electronic communications." Does the Department of Justice believe that Title I of the FISA bill reported by the Senate Select Committee on Intelligence, S. 2248, which applies to providers of electronic communication services as defined in Section 2510 of Title 18, covers libraries that provide Internet access to their patrons or places of business that provide their staff with Internet access?
10. The Protect America Act contains a provision that permits communications service providers directed to conduct surveillance under that law to file a petition with the FISA Court challenging the legality of the directive.
 - a. Will you commit to notifying the Judiciary and Intelligence Committees if any such petitions are filed with the FISA Court challenging the Protect America Act, and will you share with those committees any court action, as well as the pleadings in those proceedings, redacted as necessary?
 - b. Will you commit to announcing, publicly, the fact that such a petition has been filed?

Senator Edward M. Kennedy
Questions for the Record
Senate Judiciary Committee hearing on "FISA Amendments: How to Protect Americans'
Security and Privacy and Preserve the Rule of Law and Government Accountability"
Held on October 31, 2007

*To Kenneth L. Wainstein, Acting Attorney General, National Security Division, U.S.
Department of Justice*

1. Thank you, Mr. Wainstein, for sharing your views on FISA with the members of this Committee. I regret that I was unable to attend the hearing in person. As the history of our surveillance laws teaches us, it's essential that we have a very careful and—to the fullest extent possible—public consideration of FISA legislation.

I was present at the creation of the FISA law, and I worked closely with a Republican Attorney General to draft its provisions. Together, we found a way to provide our intelligence agencies with the authority they needed, and also build in checks and balances to prevent abuse of that authority. FISA proved that we do not have to choose between civil liberties and national security.

Unfortunately, the Protect America Act was enacted this summer in a much less thoughtful process. It was negotiated in secret and at the last minute. The Administration issued dire threats that failure to enact the law before the August recess could lead to disaster. We need to correct that failure by engaging in a thorough, deliberative process before we enact more legislation.

It is encouraging that the Administration has finally agreed to share documents with members of this Committee and the Senate Intelligence Committee on its warrantless surveillance program. We had requested these documents for many months, because they are clearly relevant to the Administration's arguments on FISA.

But the Administration has not yet shared any documents with members of the House Judiciary or Intelligence Committees, whose new FISA bill it has criticized. This selective information-sharing is troubling because it suggests that the Administration will only work with those lawmakers who already agree with it.

Questions:

1. Why won't the Administration share the documents on its warrantless surveillance program with the House Intelligence and Judiciary Committees? Aren't these committees equally important players in this legislative debate?
2. White House press secretary Dana Perino was recently asked why the Administration was willing to share documents with the Senate Intelligence Committee but not with any others. She said it was because the Intelligence Committee's leaders "showed a willingness" to grant amnesty to the telecommunications companies. "Because they were

willing to do that," Ms. Perino said, "we were willing to show them some of the documents that they asked to see." Asked to clarify these disturbing comments several days later, a White House spokesman said that what the Administration did was "not exactly" a quid pro quo.

- a. Do you stand by these descriptions of the Administration's behavior?
- b. These documents contain information that is clearly relevant to our responsibilities as lawmakers. How can you defend a policy of sharing them only with the committees that agree with the White House's preferences?

2. This Administration has asserted a view of executive power that is breathtaking in its scope. It has claimed the authority to wiretap Americans without warrants, despite the clear statement in FISA that it provides the "exclusive" means for conducting foreign intelligence surveillance. As we know from Justice Jackson's opinion in the Steel Seizure Cases, the President's authority is at its weakest when he acts contrary to a congressional enactment. Yet here, the President defied clear statutory language.

Questions:

1. If Congress enacts a FISA bill, will the President accept that he is bound by it? In particular, if we pass a bill that gives the President less power to conduct surveillance than he is now exercising, will he comply with it?
2. If we do not extend the Protect America Act and do not pass any other new laws, will the Administration comply with FISA?
3. Are any electronic surveillance programs currently being conducted outside the authority of FISA as amended by the Protect America Act?
4. Do you agree that new legislation should reaffirm that FISA is the sole means by which the Executive branch can conduct electronic surveillance outside of the criminal context?

3. As you know, the Administration is asking Congress to grant broad immunity for any past violations of the law by telecommunications companies that provided surveillance information. The Senate Intelligence Committee's bill grants this amnesty; the House Intelligence and Judiciary Committees' bill does not.

I have yet to hear a single good argument in favor of amnesty for the telecoms, but there are many reasons to be against it. Under FISA, communications carriers already have immunity from liability if they act pursuant to a court warrant or a certification from the Attorney General. In this way, FISA protects carriers who follow the law, while enlisting their help in protecting Americans' rights and the integrity of our electronic surveillance laws.

The Administration's proposal for immunity will help shield illegal activities from public scrutiny, but it will do nothing to protect our security or liberty. Instead, it will deprive plaintiffs of their rightful day in court, send the message that violations of FISA can be ignored, and undermine an important structural safeguard of our surveillance laws.

It's especially disturbing that the Administration apparently encouraged communications companies to break the law, and that those companies apparently went along. It's wrong to allow the Executive Branch to pick and choose which laws it obeys, and to ask others to help it break the law.

Questions:

1. Isn't it true that under FISA, companies that acted pursuant to a court order or an Attorney General certification already have immunity from liability?
 - a. Is it fair to say, then, that none of the telecoms being sued had one of these two documents, because if they did, they would already be off the hook?
2. In your testimony, you suggested that it would be "unfair" to the telecommunications companies to let the lawsuits proceed. I found this argument most unconvincing. Telecommunications companies have clear duties under FISA, and they have highly sophisticated lawyers who deal with these issues all the time. It is precisely because fairness and justice are so important to the American system of government that we ask an independent branch—the judiciary—to resolve such legal disputes. There is nothing fair about Congress stepping into ongoing lawsuits to decree victory for one side.
 - a. If a company violated its clear duties and conducted illegal spying, doesn't fairness demand that it face the consequences?
3. If Congress bails out any companies that may have broken the law, won't that set a bad precedent? What incentive will companies have in the future to follow the law and protect Americans' sensitive information?
4. If your concern is that carriers not be bankrupted, would you support something more specific than complete amnesty—for example, a cap on damages?
 - a. If not, why not? Are you worried that courts will rule that the President's warrantless surveillance programs were illegal?
5. As you know, the President has said he will veto any FISA bill that does not grant retroactive immunity. At the same time, he and the Director of National Intelligence have said that if Congress does not make major changes to FISA, American lives will be sacrificed. If we take him at his word, then, the President is willing to let Americans die on behalf of the phone companies

- a. That's hard to believe. So why does the President insist on amnesty for the phone companies as a precondition for any FISA reform?

4. As you know, the Senate Select Committee on Intelligence recently reported a FISA bill, the "FISA Amendments Act of 2007," which has now come to this Committee on sequential referral. This bill would make major revisions to our surveillance laws in a variety of areas.

Although I appreciate the work of my colleagues on the Intelligence Committee in drafting this legislation, I have some concerns about their bill. For example:

- As I have said, the bill provides amnesty to telecommunications companies that may have broken the law in cooperating with the Administration on illegal surveillance, even though they already have broad immunity under current FISA law.
- The Intelligence Committee's bill redefines "electronic surveillance" in a way that is unnecessary and may have unintended consequences.
- The bill does not fully close the loophole left open by the Protect America Act, allowing warrantless interception of purely domestic communications.
- The bill does not require an independent review and report on the Administration's warrantless eavesdropping.
- The bill purports to eliminate the "reverse targeting" of Americans, but does not actually contain language to do so. There is nothing analogous to the House bill on reverse targeting, which prohibits such surveillance if "a significant purpose" is targeting someone in the United States.
- Court review occurs only after-the-fact, with no consequences if the court rejects the government's targeting or minimization procedures.

These are just a few of my concerns. But if I understand you correctly, you are generally supportive of the Intelligence Committee bill. Certainly, you seem to like it a lot more than the bill being considered by the House, which contains significantly greater protections for civil liberties.

Questions:

1. My understanding is that you are in favor of the way the Intelligence Committee bill redefines "electronic surveillance." In his written testimony, Mort Halperin described this change as "Alice in Wonderland": "It says that the language in FISA, which defines 'electronic surveillance,' means not what it clearly says, but what the current bill says."

- a. Why should we change the definition of “electronic surveillance”? It’s a central term in FISA, and I see no good reason to replace it and open the door to many unintended consequences.
 - b. Mort Halperin has recommended that we strike out the part of the Intelligence Committee bill that redefines “electronic surveillance,” and then change the requirements for the certification to be given to the FISA court to read “the surveillance is targeted at persons reasonably believed to be located outside the United States.” How would this change affect your understanding of the legislation?
-
2. Unlike the House bill, the Intelligence Committee bill does not require prior judicial authorization before surveillance begins. This is a major departure from how FISA has always worked. It raises serious civil-liberties concerns, and makes it very difficult for courts to cut off surveillance that is illegal under the law. As Mort Halperin has stated: “By definition, if there is no emergency, there is time to go to the court and there is no reason to allow the executive branch to begin a surveillance without first having court approval. Requiring as a matter of routine that court approval must come first will assure that the executive branch gives the matter the full consideration that it deserves before starting a surveillance which will lead to the acquisition of many communications of persons in the United States and Americans abroad. . . . I cannot imagine any public policy argument to the contrary once one concedes that the court needs to play a role and there is an exception for emergencies with ample time limits.”
 - a. How do you respond to Mr. Halperin’s arguments?
 - b. Doesn’t the abandonment of *before-the-fact* court review go against the basic promise of FISA that Americans will not have their communications acquired without a judge confirming that there is a legitimate reason to do so?
 3. If you agree that purely domestic-to-domestic communications should never be acquired without a court order, would you support changes to the bill that would make this point 100% clear? As I read the bill, this is not as clearly prohibited as it could be.
 4. If you agree that warrantless “reverse targeting” of Americans should never be allowed, would you support language in the bill to prohibit its use if “a significant purpose” is targeting someone in the United States?
 - a. If not, why not? The House bill contains this provision, and it’s a sensible way to address the very serious “reverse targeting” concerns that will make Americans afraid for their rights.

**U.S. SENATE COMMITTEE ON THE JUDICIARY
FISA HEARING — OCTOBER 31, 2007
QUESTIONS FOR THE RECORD FOR MR. WAINSTEIN
SUBMITTED BY SENATOR KYL**

An amendment that was added to this bill in the Intelligence Committee by Senator Wyden adds a section to FISA that requires U.S. agents to obtain a warrant to conduct *overseas* surveillance of national-security threats if that surveillance targets a U.S. person.

1. Some advocates of this provision have described it as protecting the rights of U.S. citizens. The bill text, however, appears to cover "U.S. persons" – a category that FISA defines to even include U.S. green card holders. As I read the Wyden amendment, if a Pakistani national came to the United States as an adult for a few years, acquired a green card, and then returned to Pakistan and joined up with Al Qaeda, then under the Wyden amendment, this Pakistani national would be granted privacy rights under FISA that would bar the United States from monitoring his communications with the rest of Al Qaeda without first obtaining a warrant. Is that description accurate?
2. Would Middle Eastern governments be barred from monitoring the communications of this Pakistani green-card holder by any U.S. law if he were inside one of those Middle Eastern countries? In other words, under the Wyden amendment, would it be the case that the law would permit every government in the world – other than our own – to monitor the communications of this Pakistani Al Qaeda member when he is in the Middle East?
- 3A. Again, considering the hypothetical example of a Pakistani national who resides in Pakistan but has acquired a green card: under the Wyden amendment, the United States would be required to get court pre-approval and a warrant if it wanted to monitor this Pakistani in Pakistan in the course of a foreign intelligence investigation. Now suppose that the U.S. thought that this Pakistani green card holder were participating in drug smuggling in Pakistan and the FBI opened a criminal investigation. Would the U.S. be required to obtain a warrant in order to monitor his activities in Pakistan in the course of a drug-smuggling criminal investigation?
- B. What if this Pakistani national were believed to be involved in bribery of a public official while residing in Pakistan and the U.S. opened a criminal investigation of his activities. Would the U.S. be required to obtain a warrant to monitor such activities in Pakistan?
- C. What if the U.S. thought that this green card holder were fencing stolen goods in Pakistan? Would the U.S. be required to obtain a warrant in order to monitor his activities in Pakistan?
4. As I understand it, the Wyden amendment would apply not just when Pakistan-to-Afghanistan communications are routed through the U.S. Rather, it would apply whenever the activities of a U.S. green card holder are monitored overseas as part of a terrorism investigation. As a result, even if the U.S. were participating with the Pakistani government in an investigation inside Pakistan that targeted a Pakistani national who was a U.S. green-card holder, the U.S. would be required to report the investigation to the FISA court and seek a warrant.

I also understand that while many Middle Eastern governments cooperate with the United States in the war with Al Qaeda, many of these governments do not want other countries or radicalized elements of their own populations to know that they are helping the United States. As a result, many of these governments require that the fact of their cooperation with the United States or the details of joint counterterrorism operations not be disclosed outside of the U.S. intelligence community.

A. Would the Wyden amendment's requirement that the existence of intelligence investigations conducted entirely inside a foreign country be disclosed in U.S. court proceedings violate any of our information-sharing agreements with foreign intelligence services?

B. Should we expect that foreign intelligence services will refuse to share information or otherwise cooperate with the United States in the future if the Wyden amendment requires U.S. intelligence agencies to disseminate intelligence information outside of the intelligence community?

Questions of Senator Patrick J. Leahy
To Kenneth L. Wainstein

Definition of "Electronic Surveillance"

1. Both the Protect America Act and the Senate Intelligence Committee bill would change the definition in FISA of "electronic surveillance" to say that it does not include surveillance of a target overseas, even if that target is communicating with someone in the United States.

First, this is nonsensical – this clearly is electronic surveillance and to have a statute say that black is white is a bad practice. This change would also have consequences for other parts of the statute that use that definition. For example, there is a question about whether it renders inapplicable the civil and criminal liability provisions contained in FISA because those provisions are triggered by unauthorized "electronic surveillance."

Most importantly – it seems entirely unnecessary. The next part of the legislation would set up a new procedure for conducting the surveillance the government wants. There is no need to except it from the definition.

Q: Do you agree that if the statute sets up an alternative procedure to conduct the surveillance in the legislation, there is nothing in changing the definition that would add to the government's authority? If not, please explain in as much detail as possible what the definitional change accomplishes.

Immunity – Takings Issue

2. Retroactive immunity would strip away the rights of plaintiffs in those lawsuits to pursue on-going litigation that alleges violations of constitutional rights.
-

Q: Are there constitutional problems with doing this? Is it a “Taking” that violates the 5th amendment?

If there are no constitutional problems, can you point us to precedent where Congress has stepped in to quash on-going constitutional litigation?

If there are constitutional problems, do the retroactive immunity provisions contained in the Senate Intelligence bill address them?

Role of the FISA Court

The Senate Intelligence Committee bill would require the Government to submit targeting and minimization procedures to the FISA Court for the court’s review, but it would not require an up-front order from the FISA Court. The companies assisting with the surveillance would get their direction from the Attorney General and the DNI, not the Court.

Q: With the Senate Intelligence Committee bill, please describe your understanding of what power the FISA Court would have to stop the

Government from acquiring communications if it determines that the targeting or minimization procedures are flawed?

Immunity – Approval by Counsel to the President

4. The Report accompanying the Senate Intelligence Committee's legislation notes with respect to the "Terrorist Surveillance Program" that the Executive Branch provided the service providers with letters at regular intervals stating that the activities they were being asked to assist the government with had been deemed lawful by the Attorney General. The Report says this is true for all the letters except one. One letter stated that the Counsel to the President, not the Attorney General, had deemed the activities to be lawful.

Q: Even if you argue that the companies acted legally in compliance with FISA through most of this time, you cannot make that argument with respect to the period of time when Mr. Gonzales – then White House Counsel – approved the letters, can you?

Q: Given that the service providers provided assistance without regard for the statutory requirements for certification laid out in FISA and Title III, if we give them immunity now, how can we assure ourselves that they will follow the statutory requirements of FISA in the future and not just accept any written certification that the Administration gives them?

5. You stated more than once in your testimony that if any litigation should occur, it should be directed against the government, not the communications carriers who assisted the government. However, when I asked you how this would be done in light of the government's blanket assertions of state secrets, you responded, "there are many investigations going on right now about the propriety of what was done or not done under the Terrorist Surveillance Program. So in terms of accountability, if there is wrongdoing, that wrongdoing is being ferreted out in ways, very traditional ways, other than litigation."

Q: Please specify what particular avenues, other than litigation, you are suggesting we use to hold any wrongdoers involved in this matter accountable?