S. HRG. 109–1055

FISA FOR THE 21ST CENTURY

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

JULY 26, 2006

Serial No. J–109–101

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

43–453 PDF WASHINGTON : 2008

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

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00001 Fmt 5011 Sfmt 5011 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

COMMITTEE ON THE JUDICIARY

ARLEN SPECTER, Pennsylvania, *Chairman*

ORRIN G. HATCH, Utah
CHARLES E. GRASSLEY, Iowa
JON KYL, Arizona
MIKE DEWINE, Ohio
JEFF SESSIONS, Alabama
LINDSEY O. GRAHAM, South Carolina
JOHN CORNYN, Texas
SAM BROWNBACK, Kansas
TOM COBURN, Oklahoma

PATRICK J. LEAHY, Vermont
EDWARD M. KENNEDY, Massachusetts
JOSEPH R. BIDEN, JR., Delaware
HERBERT KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois

MICHAEL O'NEILL, *Chief Counsel and Staff Director*
BRUCE A. COHEN, *Democratic Chief Counsel and Staff Director*

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00002 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

Page

Kennedy, Hon. Edward M., a U.S. Senator from the State of Massachusetts, prepared statement 293
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont 3
prepared statement 296
Specter, Hon. Arlen, a U.S. Senator from the State of Pennsylvania 1

WITNESSES

Alexander, Lt. General Keith B., Director, National Security Agency, Chief of the Central Security Service, Washington, D.C. 11
Bradbury, Steven G., Acting Assistant Attorney General, Office of Legal Counsel, U.S. Department of Justice, Washington, D.C. 12
Cunningham, H. Bryan, Principal, Morgan & Cunningham LLC, Denver, Colorado 38
Dempsey, James X. Policy Director, Center for Democracy and Technology, Washington, D.C. 40
DeRosa, Mary B., Senior Fellow, Center for Strategic and International Studies, Technology and Public Policy Program, Washington, D.C. 44
Hayden, General Michael V., Director, Central Intelligence Agency, Office of the Director of National Intelligence, Langley, Virginia 6
Schmidt, John, Partner, Mayer, Brown, Rowe & Maw LLP, Chicago, Illinois ... 41

QUESTIONS AND ANSWERS

Responses of Lt. General Keith B. Alexander to questions submitted by Senators Specter, Schumer, Feinstein, Kennedy, Durbin and Feingold 50
Responses of Steven G. Bradbury to questions submitted by Senators Specter, Leahy, Kennedy, Feinstein, Feingold, Schumer and Durbin 84
Questions submitted by Senator Specter to Bryan Cunningham were not received by the time of print. 146
Responses of James X. Dempsey to questions submitted by Senators Specter, Feinstein and Kennedy 147
Questions submitted by Senator Specter, Senator Feinstein and Senator Kennedy to Mary B. DeRosa were not received by the time of print. 156
Responses of Michael V. Hayden to questions submitted by Senator Specter, Schumer, Feinstein, Leahy, Kennedy and Durbin 162
Responses of John Schmidt to questions submitted by Senators Specter and Kennedy 182

SUBMISSIONS FOR THE RECORD

Alexander, Lt. General Keith B., Director, National Security Agency, Chief of the Central Security Service, Washington, D.C., statement 188
American Civil Liberties Union, Caroline Fredrickson, Director, Washington Legislative Office, and Lisa Graves, Senior Counsel for Legislative Strategy, Washington, D.C., letter 194
Bradbury, Steven G., Acting Assistant Attorney General, Office of Legal Counsel, U.S. Department of Justice, Washington, D.C., statement 201
Constitutional Law Scholars and former Government Officials, letter 208
Cunningham, H. Bryan, Principal, Morgan & Cunningham LLC, Denver, Colorado, statement and attachment 218
Dempsey, James X. Policy Director, Center for Democracy and Technology, Washington, D.C., statement 265

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00003 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

Page

DeRosa, Mary B., Senior Fellow, Center for Strategic and International Studies, Technology and Public Policy Program, Washington, D.C., statement 278
Hayden, General Michael V., Director, Central Intelligence Agency, Office of the Director of National Intelligence, Langley, Virginia, statement 287
Los Angeles Times, July 16, 2006, article 299
New York Times:
June 15, 2006, article 301
July 16, 2006, article 303
Patriots to Restore Checks and Balances, Washington, D.C., letter 306
Schmidt, John, Partner, Mayer, Brown, Rowe & Maw LLP, Chicago, Illinois, statement 308
Washingtonpost.com:
July 15, 2006, article 314
July 26, 2006, article 316
Washington Post, July 16, 2006, article 317

FISA FOR THE 21ST CENTURY

WEDNESDAY, JULY 26, 2006

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 9:05 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Arlen Specter, Chairman of the Committee, presiding.

Present: Senators Specter, DeWine, Cornyn, Leahy, Kennedy, Feinstein, Feingold, and Durbin.

OPENING STATEMENT OF HON. ARLEN SPECTER, A U.S. SENATOR FROM THE STATE OF PENNSYLVANIA

Chairman SPECTER. Good morning, ladies and gentlemen. The Judiciary Committee will now proceed with our hearing on the proposed legislation which would submit the surveillance program for constitutional review to the Foreign Intelligence Surveillance Court.

Wiretapping has been going on in the United States involving U.S. citizens some 4½ years without having the traditional judicial approval. Since it was publicly disclosed in mid-December, the Judiciary Committee has held five hearings and has considered a variety of proposed bills leading to the legislation which we have before us today, which has been meticulously negotiated and has the agreement of the President to refer the surveillance program to the FISA Court if the legislation is approved. There may be modifications, subject to the agreement of the President. The Foreign Intelligence Surveillance Court is well suited to handle this review because of its expertise in the field and because of its secrecy, the White House insists that there not be public disclosures.

Moving to the substance of the bill, I first want to take up two items where critics do not face reality on these two major points:

First, there is a contention that the bill is defective because it does not retain the Foreign Intelligence Surveillance Court as the exclusive place to determine wiretapping. The reality is that since the President has put his program into effect, the Foreign Intelligence Surveillance Act, administered by the Foreign Intelligence Surveillance Court, is, in fact, not the exclusive remedy. The President claims that he has inherent Article II power to conduct the wiretapping aside from the Court. Three appellate courts appear to agree with that, but it depends upon what the program is. The constitutional requirements are that there has to be a balancing of the value to security contrasted with the intrusion into privacy, and that can only be determined by judicial review. And in a context

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00005 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

where the President is demonstrably unwilling to have the program subjected to public view, it would have to be determined by the FISA Court if it is to be ruled on constitutionally at all.

The second point where the critics are objecting which I submit does not face the reality is the contention that the proposed legislation expands the Article II power of the President of the United States. A statute cannot do that. The Constitution is supreme. If the President has the constitutional authority under Article II, that supercedes the statute, and a new statute may not add to nor diminish the President's constitutional power.

The legislation has received a considerable amount of commentary, a considerable amount of critical commentary. And, candidly, I welcome the dialog because I am personally convinced that when the legislation is fully understood and faced with the reality of this surveillance going on, unchecked constitutionally in the absence of any better way to do it, when this legislation is fully understood with those factors, there will be acceptance.

The commentary today in one of the major papers says that the legislation adds a provision: "Nothing in this Act shall be construed to limit the constitutional authority of the President to collect intelligence with respect to foreign powers and agents of foreign powers." Well, this bill does not add that. That provision is in the current Foreign Intelligence Surveillance Act, and it is there because it deals with embassies, foreign embassies, foreign residences of people in the United States representing foreign governments. And there has never been a requirement that there would have to be court approval to have wiretapping in that situation.

The commentary today says that the bill explicitly acknowledges an alternative source of power. Well, the bill does not. Article II power is what it is.

Now, I would have preferred to have had some other provisions, candidly. I would like to have had the program mandatory so that the President would have to submit it to the FISA Court. But I could understand the President's refusal to do that in light of his being unwilling to bind future Presidents and make an institutional change in the powers the President has. But my goal is to solve the current problem. The President has made a firm commitment to me, later confirmed by his White House personnel publicly, a firm commitment—may the record show that Mr. Steven Bradbury, who negotiated for the President, is nodding in the affirmative—made a firm commitment to submit the program to the FISA Court.

Now, I would like to have a mandate, but this President is not going to give a mandate and yield to that kind of legislative authority. And even the statute did provide a mandate, if a future President challenged it under Article II powers, Article II powers are what they are, and the statute could not bind a future President.

It really seems to boil down, to me, in many quarters that if the President agrees with it, there must be something wrong with it. There is a widespread sense that there is something amiss with Presidential agreement. Well, this legislation was negotiated in a way that I characterize as "fierce." When we come to Mr. Steven Bradbury, the Acting Assistant Attorney General for the Office of Legal Counsel, we will get into some of the details on that.

In light of the President's commitment, I think it is fair to say that this legislation is a breakthrough. Today's commentary refers to other bills which are pending, some by members of the Intelligence Committee who know the details of the program. Well, none of the bills does what this bill does. None of the bills reaches judicial review of the program.

We have had two recent decisions by United States district courts. Last week, the chief judge of the district court in San Francisco, Judge Walker, made a determination that a suit, *Hepting* v. *AT&T*, would go forward. But a close reading of that 72-page opinion shows it goes forward under very limited ways. And Judge Walker has put so many hurdles on state secrets that it is highly doubtful that that case will last much longer. Yesterday, a Federal judge in Chicago hearing *Terkel* v. *AT&T*, dismissed the case on grounds of state secrets. And when you read those cases, the obstacles are enormous.

If there is a sense to modify the provision in the legislation which gives exclusive jurisdiction to the FISA Court, that can be done. We would not have the President's commitment, but the President talked about making modifications subject to his approval.

There are a number of changes which modernize the FISA Court which we will get into. I have talked longer than I customarily do, but I have done so because of the complexity of this issue and what at least I think is the lack of understanding of the legislation and its applicability.

We started a little early today because the Prime Minister of Iraq is scheduled to address a joint session at 11, and we may lose members by that time, and we also have a vote scheduled at 10.

I am pleased now to yield to the distinguished Ranking Member, Senator Leahy.

STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Senator LEAHY. Thank you, Mr. Chairman, and thank you for convening this hearing. I am especially delighted to welcome General Hayden to his first appearance before this Committee since he assumed his new duties. I spoke with the General yesterday and told him how pleased I was to see the level of professionalism that he has brought to the agency and the appointments he has made. "Independence" and "competence" were the two watchwords that led me to believe that he would serve well as the Director of the CIA, and I said so at the time I voted for his confirmation. Again, we need some straight talk today in navigating this very difficult issue.

There are two sets of issues relating to the Foreign Intelligence Surveillance Act that are now before this Committee. First, what is the extent of the administration's warrantless wiretapping in violation of FISA, and how should we in Congress react? After 7 months and four hearings, we remain largely in the dark about what the administration is doing and continues to do because the administration has stonewalled this Committee's bipartisan efforts at oversight. But the answer is clear: We must demand and we

must ensure that this administration, and the next administration which will follow in 2½ years, actually follows the law.

Second, does the FISA law itself need to be revised? It has been amended six times at this administration's request in the 5 years since 9/11. But even though we have done that six times at the administration's request, they now say it needs "modernization." That modernization is the focus of today's hearing. The Democratic members of this Committee asked for such a hearing, and I compliment the Chairman on having it.

But the issues of compliance and modernization are completely separate issues. Whether or not FISA is in need of fine-tuning is a legitimate consideration, but FISA's possible imperfections provide no excuse for the administration's flouting of existing law. By the same token, the Bush-Cheney administration's outrageous disregard for existing law does not mean that we in Congress should shirk our responsibility to improve the law if there is a need to.

So I am ready to consider Section 9 on its merits. But I have serious grounds for skepticism.

If Section 9's provisions are, as claimed, needed to bring FISA up-to-date with the 21st century, why haven't we heard about them before now? As I said, we have amended it six times at the administration's request. In July 2002, former Attorney General Ashcroft testified that the 2001 PATRIOT Act had "modernized our surveillance tools to keep pace with technological changes." In March of this year, in the reauthorization of the PATRIOT Act, we made all the amendments of FISA that the administration requested. In fact, the President then took credit for updating the law.

So if FISA as amended is too "quaint" to meet the challenges of the 21st century, the Bush-Cheney administration owes the Congress and the American people an explanation for why they did not speak up before now.

Now, to the extent I have been able to figure out the highly complex language of Section 9, it seems to me to permit vast new amounts of warrantless surveillance of telephone calls involving American citizens. It would appear to authorize unrestricted, unregulated Government surveillance of American citizens talking to relatives, colleagues, and trading partners overseas, without any showing that that is necessary to protect our National security. But to the extent that the administration's witnesses can explain to us today, in practical and concrete terms, why these make sense, I will listen.

But let me turn to the rest of the bill. It has been called a compromise. But this Vermonter does not believe that we should ever compromise on requiring the Executive to submit to the rule of law, no matter who is President. And I am sad to say that I see the bill less as a compromise and more as a concession. It would abandon our oversight role and confine oversight to a single judge on a secret court, whose decision on the one program the Bush-Cheney administration has agreed to submit for review is appealable only by the Bush-Cheney administration. And even that oversight would not be required by the bill itself.

Now, I know the Chairman got the best deal he could. The President, the Vice President, and their legions can be hardheaded rather than flexible bargainers. I make these observations respectfully,

but also to express my reluctance to compromise FISA and the minimal protections—the minimal protections—it provides for Americans.

Section 8 would repeal FISA's exclusivity provision and affirmatively embrace the President's claim of sweeping inherent authority. The result is to make FISA optional. The President can use it or not use it, at his option.

It is astounding that we are considering this proposal. FISA was never intended to give Presidents choices. It was enacted to prevent abuses of Executive power and protect Americans' liberties by prohibiting the Government from spying on its citizens without court approval. The Bush-Cheney administration has chosen to simply ignore it. I am wondering now are we going to reward its flouting of the law by saying, in effect, "Oh, please excuse us for passing that law. We didn't mean to. We didn't expect you to follow it. We will never do that again." That is like arresting a burglar with three bags of cash and saying, "Leave one bag here, and we will all be OK with that."

Defenders of the bill have argued that Section 8 is "meaningless" because the President has whatever constitutional authority the Constitution says, and Congress cannot limit that authority through legislation. If the best we can say on behalf of proposed legislation is that it is a waste of ink, but then we should not be enacting it. But I do not believe that, when it goes to the secret FISA Court, the administration will adhere to the position that Section 8 is meaningless. The administration is insisting on that for a reason.

As the Supreme Court recently explained in its *Hamdan* decision, the constitutional scope of Presidential power depends on the legislation that Congress has enacted, even in times of war. The Constitution grants Congress the express power to set rules for the military and the express power "To make all laws which shall be necessary and proper for carrying into execution" all the powers vested by the Constitution in the Federal Government, including those of the President.

In the absence of Congressional action, the President may well have some measure of unilateral authority. That is what the precedents the administration always cites suggest. But once Congress acts, as it did in FISA, the President is no longer free to do whatever he wants to do. As the Court said in *Hamdan*, "Whether or not the President has independent power, absent Congressional authorization," Congress, of course, may place limitations on those powers.

That was the whole point of FISA: to limit the President's power to spy on ordinary Americans by making FISA the sole means by which foreign intelligence wiretaps may be conducted in the United States. Waiving FISA's exclusivity provision would not be meaningless. It would completely gut FISA. It would give the President a blank check to carry out warrantless wiretapping whenever he chooses or whenever the next President chooses. I could not in good conscience acquiesce in such a sweeping signing away of Americans' liberties in any circumstances. I am certainly not going to do it at the behest of an administration that has continuously broken the law.

Thank you, Mr. Chairman. I will put my full statement in the record.

[The prepared statement of Senator Leahy appears as a submission for the record.]

Chairman SPECTER. Thank you, Senator Leahy.

Would any other members like to make an opening statement?

[No response.]

Chairman SPECTER. Well, then, we will turn to our first witness, the distinguished Director of the Central Intelligence Agency, General Michael Hayden.

General Hayden comes to this position with a very distinguished record. He received his bachelor's degree from Duquesne University in 1967; master's, also from Duquesne, in Modern American History. We have not only an intelligence officer but a Renaissance man with us here today. Extensive course work in the Armed Forces Staff College, the Air War College, Defense Intelligence School. He has had ranking positions which we will include in the record. He has had many awards, honors, which we will include in the record. And one we will know specifically is that he is a Pennsylvanian, from Pittsburgh. That is too important just to be included in the record.

General Hayden. Thank you, Senator.

Chairman SPECTER. We are honored, General Hayden, that you would testify before this Committee on your first occasion since becoming Director of the Central Intelligence Agency, and we look forward to your testimony.

STATEMENT OF GENERAL MICHAEL V. HAYDEN, DIRECTOR, CENTRAL INTELLIGENCE AGENCY, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, LANGLEY, VIRGINIA

General HAYDEN. Thank you, Mr. Chairman, Senator Leahy. Thanks for the opportunity to speak before your Committee today. The work that you and we have before us is truly important: How do we best balance our security and our liberty and continue the pursuit of valuable foreign intelligence? Let me congratulate the Committee for taking on the task of examining and, where appropriate, amending the Foreign Intelligence Surveillance Act.

This task of balancing security and liberty is one that those of us in the intelligence community take very seriously and, frankly, it is one to which we turn our attention every day.

If I can be permitted one anecdote, within days of the 9/11 attacks, I actually addressed the NSA work force. At the time I was the Director of that Agency. It was a short video. I was talking to an empty room, but the video was beamed to our work force throughout Fort Meade and globally. And most of what I said was what you would normally expect at a moment like that. I tried to inspire. It was important. The Nation was relying on us. I tried to comfort. Look on the bright side: a quarter billion Americans wished they had your job today. And I ended the talk by trying to give some perspective. I said all free peoples have had to balance the demands of liberty with the demands of security. And, historically, we Americans had planted our flag well down that spectrum toward liberty. And so I ended my talk by simply saying here was

our challenge: "We at NSA were going to keep America free," I said, "by making Americans feel safe again."

Now, that was not an easy challenge. The Joint Inquiry Commission, which I think most of you know was comprised of the House and Senate Intelligence Committees, would later summarize our shortcomings in the months and years leading up to the September 11th attacks. The Commission, sometimes harshly, criticized our ability to link things happening in the United States with things that were happening elsewhere.

Let me just quote from some of the JIC's, the Joint Inquiry Commission's Systemic Findings, and here I am quoting.

". . . NSA's cautious approach to any collection of intelligence relating to activities in the United States."

Again quoting, "There were also gaps in NSA's coverage of foreign communications, and the FBI's coverage of domestic communications."

And, again, ". . . NSA did not want to be perceived as targeting individuals in the United States."

And, finally—and here the Commission was talking about one end U.S. conversations. By that I mean conversations in which one of the communicants was in the United States of America. The Commission said, ". . . there was insufficient focus on what many would have thought was among the most critically important kinds of terrorist related communications, at least in terms of protecting the homeland."

Now, for NSA the challenge was very acute. NSA intercepts communications, and it does so for only one purpose: to protect America, to protect the lives, the liberties, and the well-being of the citizens of the United States from those who would do us harm. By the late 1990s, that had become increasingly difficult. The explosion of modern communications in terms of volume, variety, and velocity threatened to overwhelm us as an agency.

The September 11th attacks exposed an even more critical and fundamental fault line. The laws of the United States do, and should, distinguish between the information space that is America and the rest of the planet.

The laws of the United States do, and should, distinguish between the information space that is America and the rest of the planet.

But modern telecommunications do not so cleanly respect that geographic distinction. All of us exist on a unitary, integrated, global telecommunications grid in which geography is an increasingly irrelevant factor. What does "place" mean when one is traversing the Internet? There are no area codes on the World Wide Web.

And if modern telecommunications muted the distinctions of geography, our enemy seemed to want to end the distinction altogether. After all, he killed 3,000 of our countrymen from within the homeland.

In terms of both technology and the character of our enemy, "in" America and "of" America were no longer synonymous.

I testified about this challenge in open session to the House Intel Committee in April of 2000. At the time I used a metaphor, an example, and I created some looks of disbelief when I said that if Osama bin Laden crossed the bridge from Niagara Falls, Ontario,

to Niagara Falls, New York, there were provisions of U.S. law that would kick in and offer him some protections and would actually affect how NSA could now cover him. Now, at the time that was just a stark hypothetical. Seventeen months later, after the attacks, that was the reality we were facing.

The legal regime under which NSA is operating, the Foreign Intelligence Surveillance Act, had been crafted to protect American liberty and American security.

But the revolution in telecommunications technology has extended the actual impact of the FISA regime far beyond what Congress could ever have anticipated in 1978. And, frankly, I do not think anyone could make the claim that the FISA statute was designed to deal with a 9/11 or to deal with a legal enemy who likely already had armed combatants inside the United States.

Because of the wording of the statute, the Government looks to four factors in assessing whether or not a court order is required before NSA can lawfully intercept a communication—and, again, you will not find these articulated as such in the statute. But the impact of the statute is that we look to four things so that we can decide whether or not a court order is needed before NSA does what it does routinely, and those factors are: who is the target, where is the target, how do we intercept the communication, and where do we intercept the communication. And, frankly, Mr. Chairman, the bill before the Committee today effectively re-examines the relevance of each of those factors and examines the criteria we now want to use going forward to use each of them. Let me just talk about each of them for a moment.

Who is the target?

The FISA regime from 1978 onward focused on specific court orders, against individual targets, individually justified and individually documented. That was well suited to a stable, foreign entity on which we wanted to focus for extended periods of time for foreign intelligence purposes. It is not as well suited to provide the agility to detect and prevent attacks against the homeland.

Looked at another way, FISA's careful, individualized processes exact little cost when our goal is long-term surveillance and exhausting intelligence coverage against a known and recognizable agent of a foreign power. The costs are different when our objective is to detect and prevent attacks. The costs are different when we are in hot pursuit of communications entering or leaving the United States involving someone we believe to be associated with al Qaeda.

Now, in this regard, extending the period for emergency FISAs to 7 days and allowing the Attorney General to delegate his authority to grant emergency orders is very welcome and I believe very appropriate.

So, first of all, who is the target?

Second, where is the target?

As I said earlier, geography is becoming less relevant. In the age of the Internet and a global communications grid that routes communications by the cheapest available bandwidth available each nanosecond, should our statutes presume that all communications that touch America be equally protected?

As the Chairman noted earlier this week, we do not limit our liberties by exempting from FISA's jurisdiction communications between two persons overseas that happen to get routed through U.S. facilities.

Frankly, I think our limited resources should focus on protecting U.S. persons, not those entities who might get covered as a result of technological changes that have extended the impact and then the protection of FISA far beyond what its drafters could ever have intended.

I know that Senator DeWine among others has been concerned about the allocations of these resources and FISA backlogs. And, frankly, now as Director of CIA, who must provide the predicate for FISA orders, I share his concerns in allocating resources and hope the legislation will help us properly focus resources on protecting the legitimate privacy rights of U.S. persons.

Now, beyond who and where is the target, there is the question of how do we intercept the communication.

For reasons that seemed sound at the time of enactment, the current statute under which we operate makes a distinction between collection "on a wire" and collections out of the air. Now, when the law was passed, almost all local calls were on a wire and almost all long-haul communications were in the air. Now, in an age of cell phones and fiber-optic cables, that is totally reversed—with powerful and unintended consequences for how NSA can lawfully acquire a signal. Legislators in 1978 should not have been expected to predict the future of global telecommunications, and neither should you. My view is that the statute we develop should be technology neutral.

And then, finally, beyond how do we intercept the communication, there is a question of where. Where do we intercept it?

A single communication can transit the world even if the communicants are only a few miles apart. That happens routinely. And in that transit, NSA may have multiple opportunities to intercept it as it moves and as it changes medium. As long as a communication is otherwise lawfully targeted, I believe we should be indifferent to where the intercept is achieved. Signals intelligence is a difficult art and science, particularly in today's telecommunications universe. Intercept of a particular communication—one that would help protect the homeland, for example—is always probabilistic. It is never deterministic. No coverage is guaranteed. We simply need to be able to use all the technology tools we have.

In that light, as I said earlier, there are no communications more important to the safety of the homeland than those affiliated with al Qaeda with one end of the communication in the United States. And so why should our laws make it more difficult to target the al Qaeda communications that are most important to us—those entering or leaving this country.

Because of the nature of global telecommunications, we are playing with a tremendous home field advantage, and we need to exploit that edge. We also need to protect that edge, and we need to protect those who provide it to us. The proposed legislative language that requires compulsory compliance from carriers is a very important step in this regard.

After 9/11, patriotic Americans from all walks of life assisted us, the intelligence community, in ensuring that we would not have another attack on our soil. Even prior to 9/11, we received critical assistance across the intelligence community from private entities. As Director of NSA, as Deputy DNI, now as Director of CIA, I understand that Government cannot do everything. At times, we need assistance from outside Government.

Whatever legal differences and debates may occur about separation of powers, Article II, and other critical and very important issues, those people who help to protect America should not suffer as a part of this debate. I would urge the Committee to recognize the importance of those efforts of these Americans and provide appropriate protections.

One final and very important point. Many of the steps contained in the proposed legislation will address the issue raised by the Congressional Joint Inquiry Commission: back again, one end U.S. conversations, communications that that Commission characterized as, again quoting, "among the most critically important kinds of terrorist related communications . . . ."

That means my friend here, General Alexander, and his agency, NSA, will bump up against information to, from, or about U.S. persons. Let me stress that NSA already routinely deals with this challenge and knows how to handle it while protecting U.S. privacy. I was very happy to note that the draft bill contains quite a bit of language about minimization and minimization procedures. Minimization is the process that NSA uses to protect U.S. privacy, to protect U.S. identities. The same rules of minimization that NSA now uses globally, rules that are approved by the Attorney General and thoroughly briefed to Congress, will be used under any activities that are authorized by the pending legislation.

Let me close by saying that we have a great opportunity here. We can meet the original intent of the FISA Act to protect our liberty and our security by making the legislation relevant to both the technologies and the enemies we face.

Thank you very much, and I know my colleagues have opening statements, but after them, I would be very happy to take questions.

[The prepared statement of General Hayden appears as a submission for the record.]

Chairman SPECTER. Thank you very much, General Hayden.

We now turn to Lt. General Alexander, who is now the Director of the National Security Agency. His bachelor's degree is from West Point; master of science in business administration from Boston University; master's degree in physics from the Naval Postgraduate School; another master's degree in national security strategy; has had a distinguished array of assignments and awards, and they will all be made a part of the record.

We appreciate your service, General Alexander. We appreciate your coming in today, and the floor is yours.

STATEMENT OF LT. GENERAL KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CHIEF OF THE CENTRAL SECURITY SERVICE, WASHINGTON, D.C.

General ALEXANDER. Thank you, Mr. Chairman. Good morning, Mr. Chairman, Senator Leahy, and members of the Committee. Sir, I have submitted a formal statement for the record. I will provide a brief summary of that statement at this time.

Chairman SPECTER. Your full statement will be made a part of the record.

General ALEXANDER. Thank you, sir.

I am pleased to be here today to provide testimony in support of the National Security Surveillance Act of 2006, which would amend the Foreign Intelligence Surveillance Act of 1978. The changes proposed in the bill are, I believe, intended to recapture the original Congressional intent of the statute—ensuring the rights of the American people, our original Congressional intent, in providing for our Nation's security.

As General Hayden indicated in his remarks, this is an important conversation not only for the intelligence community that will be called on to abide by the statute, but for all the American people. Advances in technology have had some unanticipated consequences in how the National Security Agency carries out its duties.

While some of the specifics that support my testimony and support passage of this bill cannot be discussed in open session, and while I would be happy to elaborate at any time, sir, the content of that, let me succinctly say that communications technology has evolved in the 28 years since the bill was established in 1978 and today in ways, as General Hayden says, that were unforeseen by the folks who built that bill. The stunning technological changes in the communications environment that we have witnessed since the enactment of FISA have brought within the scope of the statute communications that we believe the 1978 Congress did not intend to be covered.

A tremendous communications infrastructure has emerged in the United States, and both our own citizens and foreign persons outside the country use its awesome capabilities. The drafters of the FISA did not and could not have expected to anticipate this. The result, though, as General Hayden's testimony suggested, is that the U.S. Government is often required by the terms of the statute to obtain a court order to conduct surveillance of a target, of a foreign individual operating overseas but using that infrastructure. We believe the United States should be able to acquire communications of foreign intelligence targets overseas without a court order and that it ought not to matter whether we do so from the United States or elsewhere or how a particular communication makes its way from Point A to Point B.

But because of the way the statute defines "electronic surveillance," we frequently fail to make the most of one of the greatest advantages we have over our foreign adversaries: ready access to their communications present on a vast communications infrastructure located in our own Nation.

We believe that the FISA of the future must contain a few critical provisions if the Government is to be successful in gathering intelligence about its adversaries.

First, the statute needs to be technology neutral. Determinations about whether a court order is required should be based on considerations about the target of the surveillance rather than the particular means of communication or the location from which the surveillance is being conducted.

Second, we must retain a means to compel communications companies to provide properly authorized assistance to the Government, and we must insulate those companies from liability when they do so.

Third, the statute's definition of "agent of a foreign power" should be sufficiently broad to include visitors to the United States who may possess foreign intelligence information, even though they are not working on behalf of any foreign government.

The Senate bill that we are looking at would effect the required changes.

In closing, let me again express my thanks to the entire Committee for taking up this difficult but crucial issue—balancing the security of this country and the civil liberties of our people. And thank you for allowing those of us who will implement that balance the opportunity to participate in this hearing.

[The prepared statement of General Alexander appears as a submission for the record.]

Chairman SPECTER. Thank you very much, General Alexander.

We now turn to Steven Bradbury, Acting Assistant Attorney General, Office of Legal Counsel. He had been the Principal Deputy Assistant Attorney General in the same Department. Bachelor's degree from Stanford; a law degree from Michigan magna cum laude; has had a distinguished career in private practice and was a law clerk to Judge Buckley of the D.C. Court of Appeals.

At the outset, Mr. Bradbury, I want to publicly acknowledge your legal abilities and your courtesies in working through the drafting of the legislation which we are considering today, jointly with Michael O'Neill, the Chief Counsel and Staff Director of the Judiciary Committee.

We are pleased to have you here today, and we look forward to your testimony.

STATEMENT OF STEVEN G. BRADBURY, ACTING ASSISTANT ATTORNEY GENERAL, OFFICE OF LEGAL COUNSEL, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, D.C.

Mr. BRADBURY. Thank you, Mr. Chairman. It has been a pleasure to work with you and Mr. O'Neill, and it is a pleasure to be back before the Committee today.

Mr. Chairman, Senator Leahy, Senator Kennedy, members of the Committee, foreign intelligence surveillance is a critical tool in our common effort to prevent another catastrophic attack on the United States. The enemies we face operate in obscurity through secret cells that communicate globally while plotting to carry out surprise attacks from within our communities. We all recognize the fundamental challenge the war on terror presents to a free society: to detect and prevent the next 9/11, while steadfastly safeguarding the

liberties we cherish. Maintaining the constitutional balance between security and liberty must be the polestar in any legislative effort to reframe the FISA statute.

The past 28 years since the enactment of FISA have seen perhaps the greatest transformation in modes of communications in the history of the world.

Innovations in communications technology have fundamentally transformed how our enemies communicate and, therefore, how they plot and plan their next attacks. It is more than a little ironic that al Qaeda is so expert in exploiting 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 confronts the threat of al Qaeda with a legal regime geared more toward traditional case-by-case investigations.

The limitations of the traditional FISA process and the acute need to establish an early warning system to detect and prevent further al Qaeda attacks in the wake of 9/11 led the President to authorize the Terrorist Surveillance Program. As he has described, that program, which has been the subject of prior hearings before this Committee, 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.

This Committee is currently considering several pieces of legislation addressing FISA and the Terrorist Surveillance Program. I want to thank the Chairman again for his leadership on these issues and for his hard work in crafting a comprehensive approach that will help us fight terrorists more effectively and gather critical foreign intelligence more efficiently. I also wish to thank Senator DeWine, who has also introduced a bill, cosponsored by Senator Graham, which represents a very positive approach to the issues presented by the Terrorist Surveillance Program. The administration urges the Committee to approve both of these bills promptly, and we look forward to working with the Congress as a whole as this legislation moves ahead and with the Intel Committees, in particular, where technical changes can be appropriately discussed to ensure that FISA as amended will provide the Nation with the tools it needs to confront our adversaries.

Fundamentally, Chairman Specter's legislation recognizes that in times of national emergency and 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 surveillance targeted at the terrorists and designed to detect and prevent the next attack.

At the same time, however, Chairman Specter's legislation will provide an important new role for the judicial branch in the review of such Presidential programs, in addition to oversight by the Intelligence Committees of the Congress. His bill would add a new title to FISA under which the FISA Court, subject to certain requirements, would have jurisdiction to issue an order approving a program of terrorist surveillance authorized by the President. This legislation would create for the first time an innovative procedure

whereby the Attorney General will be able to bring such a surveillance program promptly to the FISA Court for a judicial determination that it is constitutional and reasonable, in compliance with the requirements of the Fourth Amendment. The FISA Court would also be authorized to review the particulars of the program and the minimization procedures in place, to help ensure that the surveillance is focused on the terrorist threat and that information collected about U.S. persons is properly minimized. The availability of these procedures and the ability of the FISA Court to issue an order approving a program of electronic surveillance will strongly encourage Presidents in the future to bring such programs under judicial supervision.

As Chairman Specter has announced, in response to this proposal and the other positive innovations contained in the Chairman's bill, the President has pledged to the Chairman that he will submit his Terrorist Surveillance Program to the FISA Court for approval, if the chairman's legislation were enacted in its current form, or with further amendments sought by the administration.

Chairman Specter's legislation would also protect sensitive national security programs from the risk of disclosure and uneven treatment in the various district courts where litigation may be brought. Under his bill, the United States, acting through the Attorney General, could require that litigation matters putting in issue the legality of alleged communications intelligence activities of the United States be transferred to the FISA Court of Review, subject to the preservation of all litigation privileges. The Court of Review would have jurisdiction to make authoritative rulings as to standing and legality under procedures that would ensure protection of sensitive national security information and promote uniformity in the law.

In addition to the innovations I have described, Chairman Specter's legislation 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 in protecting the Nation from the unique threats of international terrorism.

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, and today we urge the Committee to give speedy approval to the bills introduced by Chairman Specter and Senator DeWine.

Thank you.

[The prepared statement of Mr. Bradbury appears as a submission for the record.]

Chairman SPECTER. Thank you very much, Mr. Bradbury.

After consultation with Senator Leahy, we are going to set the rounds at 7 minutes for members, and we will proceed to that now.

General Alexander, there would be much more comfort by everyone, including myself, if we could have individualized warrants so that the FISA Court would function as it does now. An application is made. There is a showing of what the Government contends is probable cause, and there is an individualized determination on

granting the warrant. Now, it has been reported that the program in operation is so massive that that cannot be accommodated.

If any of this requires going into closed session, gentlemen, we are prepared to do that. But to the extent you can comment publicly, I think there is great merit in it so that there is an understanding of the program to the maximum extent consistent with national security.

So my question to you, General Alexander: would it be possible with additional resources to structure a program, to get what information you are getting here on an individualized basis?

General ALEXANDER. Sir, let me answer that this way—and I would ask Steve to make sure I say it exactly correct. But as General Hayden, Steve, and I have laid out for you, if you take away the foreign portion of that, where the true bill asks us to get a warrant on a U.S. person in the United States, if you take out foreign, overseas, other targets that we are talking about, which your bill does do, you are now back to a manageable level. And getting a court order for everyone in the United States is doable and one that we think should be done in that regard, and it is in the statute.

So the real issue is intermixed into the domestic is the foreign. Your bill separates that and makes it manageable.

Chairman SPECTER. Well, let me focus the question more pointedly in light of what you just said. Is it possible to have individualized warrants where your focus is on a foreign speaker, but your invasion necessarily involves a citizen in the United States? Would it be practical to have individualized warrants and still carry out the program which you have now?

General ALEXANDER. Well, there is the technology part of the thing that we each discussed briefly which would—

Senator FEINSTEIN. Could you speak up, please?

General ALEXANDER. Yes, ma'am. This is the part that we each discussed briefly in that if overseas we are collecting a foreign—going after a foreign target, no matter who that person is talking to, we are authorized under Executive order to collect that communications. That is the where. If we collect it here and it happens to go to a U.S. person, we have to stop and get a court order.

So the predominant number of our targets are foreign targets, and the question is: If we make every foreign application, because we are using the infrastructure in the United States, an application that we have to do here in the United States, you have cut out the most important advantage that we have—our communications infrastructure.

Chairman SPECTER. General Hayden, let me move to another question with you. You said that there has been some help, assistance, in not having another attack on our soil. One of the key factors is evaluating the intrusion on privacy. How valuable is the information which is obtained? Can you amplify in open session whether information obtained has prevented another attack? Or to what extent has that information been of significant value for national security in weighing the balancing act of invasion of privacy?

General HAYDEN. Yes, sir, Senator. In open session I will have to speak in generalities, but I can say with great confidence in all three positions—CIA, DNI, and particularly NSA—in broad terms,

the support we get from the broader community of America in all of its shapes and forms has been absolutely invaluable in helping in this case NSA do its mission.

Chairman SPECTER. Can you say whether it has ever prevented another attack?

General HAYDEN. I can say that the program that we are talking about here, the Terrorist Surveillance Program, has been used to disrupt and degrade enemy activity, to break up cells. Can I claim that, you know, there was a sniper on the roof with a round in the chamber and we intercepted it at that point? No. But we have gotten information we would not otherwise have had, and it has enabled us to disrupt clear al Qaeda attempts to do harm inside the United States.

Chairman SPECTER. General Hayden, moving to another issue, when you have the information going to the FISA Court with its secrecy provisions, contrast that with going, say, to a district court, say in San Francisco, with respect to the complexity of the issues, as to the explanation of the nature of the program—and I am open to having other courts besides the FISA Court consider the program. I am not concrete on that. In order to get the President's signature to a modified bill, we have to have his agreement. But when we had the negotiations, we talked about changes to the bill. The President wants some improvements in the bill. They would have to be negotiated to his satisfaction. And in wrestling with this issue of consolidation in the FISA Court, we have done so because we know that the FISA Court has a background in the program, has an understanding of the national security risks, knows the details of the program. And we are considering whether it ought to be another court, so that is an advantage in having other judges and not necessarily having in a secret court. And we have to work through the question as to a public disclosure. When we had an opinion of the FISA appellate court, it was made public, and I think the decision of the FISA Court would reach the public one way or another.

But contrast, if you will—and my red light is not quite on yet. Contrast, if you will, taking the cases to district court, like San Francisco, contrasted with the FISA Court.

General HAYDEN. Mr. Chairman, I am personally delighted that these issues would be placed in front of a court that, No. 1, is most knowledgeable about this whole universe of activity and understands in actually, I think, very clear terms what NSA does as a matter of routine and understands the care with which the agency guards privacy and can make an accurate assessment of the issue that is placed in front of the Court. And I would then add that having it in front of a single court I think actually helps the cause of justice so that there is a unitary national view as to what constitutes the correct balance, the correct line, as Steve has mentioned earlier, between security and liberty.

Chairman SPECTER. Senator Leahy.

Senator LEAHY. Thank you, Mr. Chairman.

General Alexander, in my opening statement I mentioned that FISA has been amended six times in the last 5 years. Now, to my knowledge, the administration never in that time asked for any of the changes that are contained in Section 9 of the Chairman's bill. To the contrary, the administration has repeatedly said that the

2001 PATRIOT Act updated and modernized FISA. And so if Section 9s provisions were so essential, why didn't we hear about them before now? Why this sudden demand for an overhaul of FISA?

General ALEXANDER. Sir, I don't know the exact answer for why it was never brought forward, but I can tell you there was great concern about revealing to an adversary an advantage that we had by making public some of the things that we could do. That has happened in the press—

Senator LEAHY. Well, let me follow that a little bit. I am told that this request originated at the NSA. Is that correct?

General HAYDEN. Yes, sir.

Senator LEAHY. So I would ask this of you, General Alexander, and then General Hayden. Earlier this year the administration said it did not ask Congress to authorize the so-called Terrorist Surveillance Program, according to what you started to say, because talking about it may tip off our enemy. Do you think our discussion today about possible amendments to FISA is doing that?

General ALEXANDER. I do not believe the amendments that have gone in the past have gone to the extent that we are talking about in this change of this bill here. Specifically, we have never brought forward the specifics on the advantage that we have in our home communications, our U.S.—

Senator LEAHY. Do you believe this discussion is tipping off our enemies in any way?

General ALEXANDER. We have to be concerned, sir. Clearly, we do not want to give any advantage to our adversaries, and so the hesitancy is not just my own ignorance on this, but making sure that I do not say something that would—

Senator LEAHY. General Hayden.

General HAYDEN. Yes, sir. When the program began the Terrorist Surveillance Program, we at NSA felt we had two lawful approaches in which to conduct our operations against al Qaeda—one is outlined in the traditional FISA Act, one under the President's authorization. We were quite happy to use both authorities, and we did. And in discussions as to whether or not we should move what had been authorized by the President under both his constitutional authorities and the administration's reading of the AUMF, in the discussions of whether or not we should move that under the FISA Act, it really was a compelling concern as to how much of this could be discussed in open session.

What has happened in the last 7 months is much of this program has already been put out into the public domain. That inoculates some of the discussion we are having today against some of the down sides. But, Senator, there will be questions, I am sure, you will ask any of the three of us that we will not be able to answer in open session.

Senator LEAHY. Let me ask Mr. Bradbury, when Attorney General Gonzales testified last week, he agreed with Senator Specter that the language in his bill that repeals FISA's exclusivity provision and recognizes the President's inherent authority to collect foreign intelligence is essentially meaningless. To quote the Attorney General, "It does not change the status quo."

If that is the case, can I assume you would have no objection to striking this language in the bill if all it does is state the status quo? Yes or no.

Mr. BRADBURY. I am not able to answer that yes or no, Senator. I will say this: In our approach to these issues—and I think it is reflected in the legal analysis presented in our paper back in January on this program—it has always been our approach to endeavor to avoid a constitutional clash between the branches. And we think that is the way a court would address these issues.

Senator LEAHY. But the Attorney General said—do you agree with the Attorney General when he says all this does is state the status quo?

Mr. BRADBURY. Well, the status quo certainly is the case, Senator, that the President has authority under Article II—

Senator LEAHY. Do you agree with the Attorney General?

Mr. BRADBURY.—and the status quo is as the Court of Review—

Senator LEAHY. But my question—

Chairman SPECTER. Let him finish his answer.

Senator LEAHY. But he is not answering my question.

Chairman SPECTER. Well, let him answer.

Senator LEAHY. Do you agree with the Attorney General?

Mr. BRADBURY. I agree that as the Court of Review, the FISA Court of Review has stated that the FISA statute cannot take away the President's constitutional authority.

Senator LEAHY. OK. So I do not know whether you agree with the Attorney General or not. I will let you discuss it with him whether you agree with him or not.

Suppose the Government wants to monitor a telephone conversation or e-mails coming into the United States from American soldiers who are serving in Iraq. Now, let's stipulate it does not apply—it is not being done—this is for you, Mr. Bradbury. It is not being done for law enforcement purposes, so Title III does not apply. Now, under current law, if the Government acquires these communications off wires in the United States, it would need a warrant. What about under the new definition of "electronic surveillance" in the Chairman's bill? Would the Government still need a warrant to intercept communications from our men and women in Iraq to their family members back at home?

Mr. BRADBURY. If you are talking about a communication which is international and if you are not targeting a person in the United States to try to collect information about that person in the United States, it would not fall within the amended definition of "electronic surveillance."

Senator LEAHY. So you would not need a warrant to collect it. They are e-mailing to their parents, spouses, and what-not back home. You would not need a—

Mr. BRADBURY. If you are attempting to collect information about persons in the United States, which you—

Senator LEAHY. No, no.

Mr. BRADBURY. It depends—

Senator LEAHY. No, no. I left out—I said there is no law enforcement. It simply—

Mr. BRADBURY. Well, it does not have to—Senator, it does not have to be law enforcement. Any effort to collect information about

persons in the United States would fall within the definition of "electronic surveillance" if you are targeting those persons. So you really need to look at—and that is, I think, the fundamental point that the Generals have made, is what we believe the statute ought to focus on is who is it you are trying to collect information about and—

Senator LEAHY. I made it very clear. I said that you have a soldier in Iraq—let's make it even clearer. A soldier in Iraq is sending an e-mail to his wife. He is not of any interest to law enforcement. He is not suspected of doing any crime or anything else. Would you need a warrant to collect that e-mail or could you just pick it up and put it into your Government banks?

Mr. BRADBURY. Well, I will say, Senator, that today under existing law, if you are collecting that internationally flowing communication anywhere else in the world, you can do that without any court approval. That is done today pursuant to Executive Order when it is done for national security purposes.

Now, these agencies operate for national security purposes and not simply to eavesdrop on people's private conversations when there is not any national security interest or foreign intelligence—

Senator LEAHY. Would your message be, then, that somebody sending an e-mail to their spouse back here from Iraq, they probably better be pretty careful what they say, that it is going to be in a Government data base somewhere?

Mr. BRADBURY. No, I would not because, as I have tried to just indicate, all of the authorities of these agencies, when they are operating today, Senator, under Executive Order—it is called Executive Order 12333, which we have existed under since the 1970s. The only collection that these agencies can do under that Executive Order is for foreign intelligence purposes. That is quite apart from any statutory requirements under FISA. So there is no listening in except for foreign intelligence purposes. And that is the fundamental point. It does not matter whose communication you are listening in to or where it is collected. It has to be for foreign intelligence purposes.

Senator LEAHY. That does not answer the question, but I will go into it on my next round.

Chairman SPECTER. The vote is under way. We are going to adjourn very briefly. Senator Cornyn and I are going to be very swift in moving over and back, and when we come back, we will pick up with Senator Cornyn.

We stand in recess for just a few minutes.

[Recess 10:10 a.m. to 10:27 a.m.]

Chairman SPECTER. The Committee will resume.

Senator Cornyn.

Senator CORNYN. Well, thank you, Mr. Chairman, and I want to express my gratitude to the witnesses for being here today to talk about this important subject. I would hope that we could all start from a basic premise, and that is that we should use all legal means available to us to collect information from our enemies that would help us fight and win the global war on terror. I think that we would all agree with that. I am confident you would. Sometimes I wonder when I hear some of the public debate.

But I want to maybe start with you, Mr. Bradbury. Early on, when the New York Times broke the story about the Terrorist Surveillance Program, there were allegations that there had been a violation of the law, that this was unlawful. But as the Chairman pointed out, my recollection is there have been at least three courts that have expressly acknowledged the President's inherent power under the Constitution to collect foreign intelligence during a time of war. Is my recollection correct?

Mr. BRADBURY. That is correct, Senator. The Fourth Circuit, the Second Circuit, other circuits—in fact, more than three, and then, of course, the FISA Court of Review acknowledged that.

Senator CORNYN. Well, that was going to be my next point. The very court that Congress created to oversee the decisions of the Foreign Intelligence Surveillance Court and the FISA Court of Review has acknowledged in a written opinion the President's inherent authority under Article II to conduct, in essence, this battlefield intelligence gathering. Isn't that right?

Mr. BRADBURY. That is correct, Senator.

Senator CORNYN. Are you aware of any court that has held the Terrorist Surveillance Program to be unlawful?

Mr. BRADBURY. No, Senator. No court has reached that issue.

Senator CORNYN. So the only courts that have spoken to it have held that this is a lawful exercise of the President's authority under the Constitution.

Mr. BRADBURY. The only decisions from courts are that the President generally has authority under Article II to protect the country through foreign intelligence surveillance.

Senator CORNYN. Well, I would hope that—because I think I agree with your assessment. That is certainly my understanding. And I would hope that those who would try to scare people or make allegations of rampant sort of unlawful or rogue conduct would bring their rhetoric down a little bit because, in fact, the only decisions we do have from courts indicate that the President does have that authority under appropriate circumstances.

I want to also ask General Hayden and General Alexander, there was some statement made earlier on in the hearing today that the capability that the NSA has been using, that the U.S. Government has been using, to intercept international communications between al Qaeda operatives and folks here in the United States who may be their allies, that this is somehow unchecked authority. But I just want to ask a little bit about that.

It is my recollection that this program is reviewed every 45 days internally within the NSA and the administration. It is my recollection that it has been briefed to the FISA Court judges, if not all of them, at least the chief judge, and maybe some others, and if you can help me there.

It has also been briefed since the inception to leaders on a bicameral and a bipartisan basis, the leaders of the House and the Senate, as well as the Chairmen and Ranking Members of both the House and Senate Intelligence Committees. Did I summarize that correctly?

General HAYDEN. Yes, sir. That is correct, Senator.

Senator CORNYN. Well, to me that seems like it comes in some conflict with the idea that this authority is unchecked, and that is my conclusion. You do not have to agree or disagree.

One reason I support Senator Specter's bill is because it does acknowledge this authority, but it creates a way to try to accommodate the legitimate concerns that Members of Congress have and to make sure that Congress is a full partner in the process of striking the balance, General Hayden, that you talked about between privacy concerns and our ability to collect intelligence by all lawful means.

Mr. Bradbury, I wonder, though, if you could tell me, do you view this bill to be a substantial change from the status quo? There was some question about that. Or is it a ratification, more or less, by Congress that the President has that authority and then create other procedures that are essentially consistent with what is already happening now?

Mr. BRADBURY. Well, of course, Senator, as the Chairman made clear in his opening remarks, the status quo today is that the President has exercised his authority, both under the Constitution and his view of the Authorization for the Use of Military Force and has established a Terrorist Surveillance Program independent of FISA in an effort to try to detect communications that may be leading to another attack on the country. And so this legislation would recognize that existing fact, but it would make a very substantial change in FISA today by adding a new title that would give the Court jurisdiction to review such a program on a program-wide basis, and that is an important new tool that any President would have going forward. And it is because of that innovative new tool that would really allow for efficient judicial review of such a program in wartime, that the President would take the program then to the Court for its review.

So I applaud, again, the Chairman for the legislation and for that effort, because I do think that is a very important—would be a very important change in the current statutes.

Senator CORNYN. Well, thank you very much for that clarification, and I think you are certainly correct.

I know, General Alexander, there was some question about whether the NSA was intercepting Internet communications between a soldier in Iraq and their family members at home. You are a soldier, are you not, sir?

General ALEXANDER. Yes, sir.

Senator CORNYN. And you certainly, I know, have an interest in not undermining the privacy rights of an American citizen serving his country and defending freedom in Iraq. Are you spending your time targeting American citizen soldiers in Iraq in your spare time?

General ALEXANDER. No, sir, we are not, nor would we. If we do, we have procedures through the Attorney General overseas, if it is against a U.S. person, or a court order here in the United States. And both of those would be followed.

I would tell you, I would be more concerned about other nations looking at our soldiers, which they do, and terrorists. And so the fact that we can do it, others can do it, too. And so the greatest concern is the Operation Security that goes along with the soldier communications, which they in Iraq know very well. And as you

know, sir, from the soldiers there, they treat OPSEC as very important to their own survival.

General HAYDEN. Senator, could I just emphasize a point that General Alexander brought up? The procedures in place today, which will not be affected by the act before the Committee, is that in order to target a protected person, a U.S. person—and that definition goes beyond just citizens of the United States. In order to target a protected person overseas, it now requires, well, now General Alexander to make a case to the Attorney General that this is for foreign intelligence purposes and that the target of the activity is the agent of a foreign power. And that would not be changed by the legislation.

Mr. BRADBURY. I am sorry. Just to emphasize that triply, what I mentioned before in response to the question from Senator Leahy is that there are authorities today under Executive Order to do foreign intelligence surveillance. But those authorities, if you are talking about targeting the communications of a U.S. person, like a U.S. soldier in Iraq, require both that it be for a foreign intelligence purpose and that the Attorney General expressly approve it. And that is under existing Executive Order. That would remain unchanged by this legislation.

Senator CORNYN. Thank you.

Chairman SPECTER. Thank you, Senator Cornyn.

Senator Kennedy.

Senator KENNEDY. Thank you very much, and I want to thank the panel, thank them for their service to the country, impressive backgrounds, experience and commitment.

I was here when we did the FISA legislation. At that time, in 1976, President Ford and Attorney General Levi, worked very closely with the Judiciary Committee, the President and the Attorney General, and we worked out the FISA. It was enormously complex and complicated at that time, and the range of intelligence challenges are like an echo that I hear this morning. Everyone understood that there was cutting-edge, there was new information, dangerous times. And, we were able to work out legislation that only had one vote in opposition to it in the U.S. Senate, and it has worked.

Obviously, there are suggestions and recommendations that could be made, but it worked and it had the confidence of the American people and the confidence of Congress about the protections of rights and liberties and also in getting information. All of us are in the same boat in terms of al Qaeda and the dangers that threaten this country. But as you have all eloquently stated, there is the balance between security and also the liberties with which we have to deal. And that is what many of us had hoped, that we would be able to work within this balance and the administration would work with us. We can handle sensitive and secret information and establish a process that I think would have given the American people the confidence that all of us were working together, Republican and Democrat, the President and the Congress, in a bipartisan way to really get at the core dangers that we were facing in protecting liberties. And that is what I think continues as the challenge, and the fact that we are still working on this is just enormously important.

But that is the departure point, and there still continues to be frustration that we are unable to get to that point and do not have all of the information that we should have in order to legislate. The American Bar Association emphasizes the challenges that we are continuing to face under the circumstances.

I am interested, in the time that I have, if you can just tell us—and we are very conscious of the facts that there is sensitive information on this. But can you tell us now the extent to which this is actually affecting Americans, Americans here at home? What we are talking about is to what extent are they included in this program?

General HAYDEN. Senator, I will start since I was there when the program began.

Senator KENNEDY. Okay.

General HAYDEN. And I mean this very sincerely. Nothing more important to the people conducting this program than the privacy of Americans.

Senator KENNEDY. Good.

General HAYDEN. We understand—

Senator FEINSTEIN. Could you speak up, please?

General HAYDEN. Yes, ma'am. Nothing more important in the conduct of this program than the privacy of Americans. After the story broke in the New York Times, I went out to talk to the NSA workforce that is involved in this, and it struck me that on the walls of the office in which this activity is conducted, there was a large poster that said, "What constitutes a U.S. person?" And the four different approaches by which one could gain the protection of a U.S. person were spelled out there, even in the bowels of the office that is responsible for this program. It is done very carefully. It is very targeted. There is a probable cause standard, before any communication is intercepted, that one or both communicants is, again, to a probable cause standard, associated with al Qaeda.

So I know the sensitivities, Senator, and NSA is a powerful and a secretive organization. Those are the two things our political culture distrusts the most. But this is done with great care.

Senator KENNEDY. Well, I understand that, and the standard then is a probable cause standard. Is that correct?

General HAYDEN. That is correct.

Senator KENNEDY. All right. But the question was: To the extent that Americans are included in this, can you tell us, or is that—what is the extent, what is the range?

General HAYDEN. We have briefed the precise numbers to all members and some members of staff of both Intelligence Committees, Senator.

Senator KENNEDY. But even in the range—if you can't, you can't. But, I mean, are we talking about 20,000? Are we talking 2 million? You can't do—

General HAYDEN. I am not able to.

Senator KENNEDY. Can you tell us whether any of these are under continuing surveillance, that is, they go on for not only just a conversation but whether they are continuing, whether there are Americans that are subject to a continuing—this was an issue when we passed the FISA. Attorney General Levi spoke about this

issue and question in terms of the legality of it, and this is an area that obviously is of concern. Can you tell us?

General ALEXANDER. Sir, if I can give you two things here in open session. The overwhelming focus in our collection is against the foreign entities by a tremendous margin, and everyone who has read into that is amazed when they see that. First and foremost, predominantly foreign. There are U.S. parts to that, and I cannot go into the details of the lengths of that. But it is all focused on the al Qaeda, and it is predominantly foreign.

Go ahead, sir.

General HAYDEN. I would just offer a point to make it very clear. The President has said a communication we believe to be affiliated with al Qaeda, associated with al Qaeda, one end of which is in the United States, and we believe at least one end we have a probable cause standard is al Qaeda. As General Alexander points out, overwhelmingly the end we believe to be affiliated with al Qaeda is a foreign end.

Senator KENNEDY. All right. And so just about the question of continuing and ongoing versus a single conversation, the extent of that, General Alexander?

General ALEXANDER. Sir, I am not sure I understand.

Senator KENNEDY. One thing is where you are listening to a conversation. The other is where you have the wiretap continuing for 24 hours a day.

General ALEXANDER. Right. Sir, we go through a very deliberate process to listen in on any conversation, just because of the sheer resources, whether it is in this program or any other program. And so as we started out, we know it is one end foreign. You cannot physically listen to millions of phone calls, nor would we. We are going to focus it down onto the most important ones, and we have ways and methods to do that that we should not discuss here.

Senator KENNEDY. All right. I am going to run out of time here, but let me ask you: Has any of the information that has been gathered to date in any of this been used in any legal proceedings here in a court or any trials to date?

General HAYDEN. Senator, the process used is the process by which we use any foreign intelligence, and it moves outside of the intelligence community with all the appropriate caveats on it in terms of how it can be used in judicial procedures.

Senator KENNEDY. But can you tell us whether it has or has not been used?

General HAYDEN. I don't know, Senator, again, because we put the caveats on it—

General ALEXANDER. Lead and investigative—

General HAYDEN. Lead and investigative purposes is what it says.

Senator KENNEDY. My time is up, Mr. Chairman. Thank you.

Chairman SPECTER. Thank you, Senator Kennedy.

Senator Feinstein.

Senator FEINSTEIN. Thank you very much, Mr. Chairman, and thank you for the hearing. I would like to just say one thing, and that is, as a member of the Intelligence Committee, I have been briefed on the program. And I am strongly opposed to giving this President or any President the right to collect content—to collect

content on United States persons without a warrant. And today for the first time we heard General Alexander state that if the foreign-to-foreign switching is taken care of, the program is easily accommodatable to an individual warrant for U.S. persons in content collection. Is that not correct, General?

General ALEXANDER. Not quite, ma'am, if I might just state it in my words: that if the foreign selectors that we are going after, which some of those—it depends on where the target is, and this goes back to the definition of "electronic surveillance." And so it is not necessary—if we are going after a terrorist in country A and he is talking to somebody in country B, we are authorized to go after that. If that same terrorist we are targeting happens to go into the United States, we are authorized to collect that overseas also and minimize the U.S. person's data.

The issue that I was describing is now, under the current FISA, if I collect that in the United States, I have to get a warrant for it. So what you would have us do is overseas I could do it and minimize it. Today I lost the advantage of being able to do that in the United States. If that portion of the targeting in the definition of this "electronic surveillance" we believe that is adjusted in this proposal that meets both of those and that that would then allow us to—

Senator FEINSTEIN. And both ends are foreign to foreign?

General ALEXANDER. Not necessarily. The target of the selector is foreign, and the question is where are they calling.

Senator FEINSTEIN. Well, I know those numbers, too.

General ALEXANDER. Right.

Senator FEINSTEIN. And I do not think that those numbers are necessarily prohibitive from a FISA warrant, nor do I believe that it would take that much time for a FISA warrant.

General ALEXANDER. But it would require us, ma'am, if I might, it would require us to get a FISA on every foreign one in advance because we do not know who they are calling until it has happened.

Senator FEINSTEIN. Oh.

Mr. BRADBURY. Senator, may I also just add a point, if I might?

Senator FEINSTEIN. Certainly.

Mr. BRADBURY. In the Chairman's legislation, there would also be a number of other reforms to FISA which would greatly assist in the general ability to get FISAs even for domestic targets. For example, the FISA application process would be streamlined. The amount of information required for an application would be reduced.

Senator FEINSTEIN. That was in my bill, too.

Mr. BRADBURY. Yes, it was.

Senator FEINSTEIN. I believe Senator Specter took it from my bill.

Mr. BRADBURY. Absolutely. It is a good idea, and good ideas should be liberally—

Senator FEINSTEIN. I just wanted to make that clear.

Chairman SPECTER. I had thought that was our bill, the

Feinstein-Specter bill.

[Laughter.]

Senator FEINSTEIN. I am delighted. Yes, it is our bill.

Mr. BRADBURY. In addition—and this may also be in your legislation, Madam Senator—the emergency authorization period would be extended from 3 days to 7 days. The ability to authorize it would be liberalized. And then perhaps most importantly, if the reforms are made to the definition of what is covered, to take out the international communications that are not really historically the primary focus of FISA, that, of course, by itself would free up a lot of resources in terms of the Office of Intelligence Policy and Review that makes the applications to FISA.

So all of those combined would necessarily make it much easier to get quick approvals for those domestic targets of necessary intelligence surveillance.

General HAYDEN. That is why I tried to craft my opening comments about those four criteria, and very frequently NSA is required to get FISAs not because of who is targeted, but because of one of those other three criteria. And what this legislation does is move the legal focus back to who are you targeting rather than these techniques or accidents of how you actually carry it out.

Senator FEINSTEIN. Well, let me raise one other point. Senator Specter's new FISA bill also eliminates the 15-day window on surveillance following a declaration of war. And this could be interpreted to mean that after a declaration of war, the President has unlimited wiretap authority until the end of the war. How long under this new Specter version would a President's authority last? Could it last for decades?

Mr. BRADBURY. Well, Madam Senator, the President's authority to protect the country comes in large measure from his authority under Article II. Of course, with the Terrorist Surveillance Program, that has been in place now since shortly after 9/11.

It is our view, as we tried to explain in—

Senator FEINSTEIN. If you do not mind, let me just interrupt you.

Mr. BRADBURY. Absolutely.

Senator FEINSTEIN. Because it seems to me you are buying into—the administration is buying into a concept, and that is Senator Specter's bill. Therefore, you are tacitly confining your Article II authority within the confines of the Specter bill, as I understand it. So I am asking you the question. One of the amendments made is to delete this 15-day period, which, therefore, once deleted, also has an interpretation that it is without end.

Mr. BRADBURY. Well, there would be no express provision that says in time of war that the limitations of FISA do not apply. The current provision says if there were a declaration of war, none of the requirements or limitations in FISA would apply at all for 15 days. Now, there have only been five declarations of war in the history of the country, and we have not even come close to one since FISA was enacted in 1978.

It is our view of that provision today in the legislation that, in effect, it is a determination by Congress back in 1978, which was not a time of war, that in the event of armed conflict or declaration of war, the branches would come together and that there would be some accommodation made going forward during that wartime.

It is not our view that it was a declaration by Congress that only 15 days of warrantless surveillance in wartime is all you need. I don't think that is what it was intended to mean. It was intended

to give some leeway, all the rules are off, and then during that period there would be some special accommodation made. It was really, in effect, a decision by Congress in the 1970s to punt the question of what would happen during an actual armed conflict.

Senator FEINSTEIN. Mr. Chairman, would you allow me one other question?

Chairman SPECTER. Yes. Proceed, Senator Feinstein.

Senator FEINSTEIN. Perhaps, Mr. Bradbury, you are the one to ask this question of. Is it your contention that the FISA Court is an Article III court?

Mr. BRADBURY. The judges are Article III judges, and, yes, they are serving in a special capacity for purposes of approving these orders. But, yes, they are Article III.

Senator FEINSTEIN. And to what do you attribute that? Where is the justification for finding it an Article III court?

Mr. BRADBURY. They are appointed for life with their compensation fixed, it cannot be reduced. They are Article III judges, and Congress by statute has given them a special assignment at the appointment of the Chief Justice. But that does not mean that they are not Article III judges. They act in their capacities as Article III judges, as does a court that approves, for example, a Title III warrant.

Senator FEINSTEIN. Isn't there a magistrate serving as a FISA Court judge?

Mr. BRADBURY. I am not aware of that. There are 11 FISA Court judges. I believe—don't hold me to this—that they are all district judges appointed by the Chief Justice.

Senator FEINSTEIN. Well, I am a little puzzled, Mr. Chairman, on this one point, because there is nothing in the FISA law that gives this court the ability to make programmatic approvals as opposed to grant warrants, individual warrants. And how when a court gives an advisory approval to a program and the constitutionality of such I think is questionable.

Mr. BRADBURY. Well, may I respond to that?

Senator FEINSTEIN. Yes, please.

Mr. BRADBURY. Interestingly enough, the FISA Court of Review in the *In Re Sealed Case* decision addressed the question of whether a FISA order under the current statute is a warrant or not. And the Court actually concluded that while it has a lot of characteristics of a warrant, the Court did not need to conclude or decide that it was a warrant, because foreign intelligence surveillance could be conducted before and after FISA as long as it is reasonable under the Fourth Amendment, and that the FISA procedures would ensure that any court order approving surveillance would ensure that that surveillance was reasonable under the Fourth Amendment.

So it is not necessarily the case that a FISA order, even an individualized one, is a warrant for Fourth Amendment purposes. And the Fourth Amendment does not require a warrant in all circumstances. In special cases, there can be surveillance done, searches conducted without warrants, as long as they are reasonable, for example, in the area of foreign intelligence investigations and surveillance.

Senator FEINSTEIN. Are you making the argument that a FISA Court order for content collection is not a warrant?

Mr. BRADBURY. Well, the FISA Court of Review concluded that it did not need to decide that it was a warrant for it to be constitutional. So it does not have to be viewed as a warrant, and I would say that you are right that today FISA does not contain any procedure that would allow the FISA Court to give a program-wide order of approval to surveillance. The new title that would be created by the Chairman's bill would enable the Court to do that and would give the Court jurisdiction.

But in terms of Article III and whether there is a case or controversy, I do not see a difference between the program-wide order and the individualized order. There would still be a case or controversy. It would be constitutional. The Attorney General as a result of that order could get an order from the Court that would compel cooperation to do what needs to be done to undertake the surveillance. And just as with a Title III warrant today, where the Government goes in ex parte to a district judge and gets approval for a Title III warrant, this is a similar construct. And it is similar to the FISA process today for FISA orders.

There is the hypothetical person on the other side of the case—not hypothetical. But the people on the other side of the case are those people who would be under surveillance. That is the same in a Title III context or under FISA today. I really think it would function like FISA today. It would just be a program-wide order.

Senator FEINSTEIN. Well, you have been more than generous with your largesse, Mr. Chairman.

Chairman SPECTER. How much more time would you like, Senator Feinstein?

Senator FEINSTEIN. Well, you see, I think this is kind of the crux of the matter, and—

Chairman SPECTER. Senator Feinstein, proceed.

Senator FEINSTEIN. If you would just allow me for a minute, essentially there are no holds in your bill on a President's authority. Once there is this programmatic approval by the FISA Court, then individuals in this country can be wiretapped for content. And that wiretapping could go on forever. There is no duration.

I would assume that others could be slipped into that program warrant, perhaps even without review. And what worries me is that once for content—meta data is something else, but for content, once you go to a programmatic approval, it opens the Pandora's box of all kinds of games that can be played with that because there is no timely periodic review of everybody whose content is being collected under that programmatic review, no decisions made as to how long that data can be maintained, when a decision can be made that the content collection should be cut off.

Mr. BRADBURY. Senator, that is not the case. Under the Chairman's bill, all of those things would be addressed by the Court in its review. So, for example, strict requirements would have to be met before the Court would be able to entertain such an application, it would have to be directed at foreign terrorist threats. There would have to be a showing that you could not use traditional FISA process. There would have to be a showing that there is special need for agility and flexibility and that you cannot identify all of the targets in advance. Then there would have to be special mini-

mization procedures proposed and in place to protect any information about U.S. persons that might be caught up in the program.

Then the Court would review it for reasonableness under the Fourth Amendment. The Fourth Amendment is not an open-ended blank check. The Fourth Amendment would not allow things to go on permanently, would not allow things to be general and not focused on the threat. All of those things would be taken into account and reviewed carefully by the Court. It could only be approved for 90 days, and then the Court would review it. You would have to come back in, and in reviewing it and reauthorizing it, the Court is charged under the legislation to look at, well, what has the actual collection been? Has it been focused, as the Attorney General said it would be? Have the minimization procedures been followed? All of those things would be subject to careful judicial review by the FISA Court.

Senator FEINSTEIN. All right. Knowing the numbers, foreign to foreign—

Chairman SPECTER. Senator Feinstein, you are up to 8 minutes over, which is another round.

Senator FEINSTEIN. I appreciate that.

Chairman SPECTER. Why don't you ask your last question?

Senator FEINSTEIN. The last one. Knowing the numbers of the foreign to foreign, you are saying every one of them would be reviewed every 90 days?

Mr. BRADBURY. Well, in the Terrorist Surveillance Program of the President, we are talking about international communications in and out of the United States. And under the Chairman's proposal for this new program-wide order, it would be focused on surveillance where you are talking about communications to or from persons in the United States. So the foreign to foreign would not be the subject of such a program-wide order, but communication surveillance where there is a U.S.—or somebody in the United States is involved could be and would be the subject of such a program, and the Court would be free to ask, as the legislation makes clear, for any additional information the Court desires to review that program and to take a look at it very carefully and closely. So it would be up to the Court in making a judgment as to the reasonableness of the program, the targeted nature of it, et cetera.

Senator FEINSTEIN. Thank you. I appreciate it very much.

Thank you, Mr. Chairman.

Mr. BRADBURY. Thank you, Senator.

Chairman SPECTER. Thank you, Senator Feinstein.

General Alexander, coming back to the question which I asked initially and you have expanded upon, would it be impractical or even impossible to have individualized warrants under the current surveillance program? You had responded in part that it would limit you when you were going after a foreign member, a foreign caller, someone who initiated the call abroad, not knowing whether it was going to be to a domestic location or not. Would you expand upon that?

General ALEXANDER. Yes, sir, and I will take from the testimony that we started out with in that who and where are the key parts of this. Who is the target that we are going after? Is it a foreign terrorist in a country outside the United States? If the target is

outside the country making a call, then we should use every means possible—and I think everybody generally agrees with that—to go after that communication. The issue is if we conduct that in the United States and it happens to stop in the United States, in the United States we would need a warrant; outside the United States we could do it under Executive Order. So we have a problem.

The issue then becomes do I get a court order for every foreign target that I have under the possibility that I could have collected it in the United States. That is what it does to us today. That is impractical. It would cause a tremendous burden on—

Chairman SPECTER. Now, specifically, what is impractical? When you—

General ALEXANDER. The volume—

Chairman SPECTER. Wait a minute.

General ALEXANDER. The volume of—

Chairman SPECTER. Wait a minute. Let me ask the question so we have the framework. It is impossible or impractical to get an individualized warrant when the caller is outside the United States, not knowing whether the recipient will be inside the United States?

General ALEXANDER. Yes, sir. It would be impractical. I am not saying it would be impossible, but it would be impractical because we don't know what the foreign to U.S. number could possibly be. Would the requirement be, hypothetically, if that foreign number called all foreign numbers, you would say good to go. But if they called U.S. number 1, FISA. If he calls U.S. number 2, I have to get a new FISA. U.S. number 3, a new FISA. U.S. number 4, a new FISA. And what I am ending up doing is submitting for calls that have been happening, and what we would do is saturate—

Chairman SPECTER. That is what you would have to do absent the surveillance program?

General ALEXANDER. That is correct.

Chairman SPECTER. But with the surveillance program, you do not have to do that.

Now, you say impractical, but not impossible?

General ALEXANDER. Well, you would not be effective.

In my opinion, sir, from an operational—

Chairman SPECTER. Why not effective?

General ALEXANDER. Because you would be so far behind the target, if you were in hot pursuit, with the numbers of applications that you would have to make and the times to make those, you could never catch up to the—

Chairman SPECTER. So your conclusion is that to have individual warrants, it would not be practical or effective in what you are seeking to accomplish?

General ALEXANDER. That is correct.

Chairman SPECTER. General Alexander, General Hayden, I think it would be useful if you supplemented your oral testimony in writing amplifying so you have an opportunity to present a fuller picture. We have had a pretty good dialog here.

Senator FEINSTEIN. If I might say particularly on—

Chairman SPECTER. Are you on your time, Senator Feinstein? Let me proceed, Senator Feinstein, and we will come back to you after Senator Leahy, if the next vote does not come sooner.

Mr. Bradbury, Senator Feinstein said that there are no holds and no limitations on what the President can do under my bill. But isn't it a fact that what the President can do under my bill is what the President is doing now and that it is measured by whatever his Article II powers are?

Mr. BRADBURY. Well, that is certainly correct.

Chairman SPECTER. And isn't the determination as to whether he has Article II powers to do what he is doing now a balancing test so that on this state of the record, this Committee, not knowing the details of the program, is not in the position to say that it is an exercise within Article II or is it beyond Article II? Is that true?

Mr. BRADBURY. That is true, and I would add that the limitation and the real balancing test comes in through the Fourth Amendment, because whatever the President does is subject to the Fourth Amendment and—

Chairman SPECTER. But we cannot determine that unless we know where the program is on the balancing test. Reasonableness, as you said earlier, depends on the threat and depends upon the invasion of privacy.

Mr. BRADBURY. That is correct.

Chairman SPECTER. And that requires a judicial determination.

Mr. BRADBURY. Well, that is one very effective way to do it, and that is what your legislation would do. It would bring the Court in to make that determination.

Chairman SPECTER. Is there any other way to obtain a judicial determination other than the FISA Court maintaining the secrecy that the President insists upon?

Mr. BRADBURY. Well, I think that is a very good mechanism for doing that. Obviously, there are 30 or so pieces of litigation around the country that have challenged various versions of what has been alleged in the media. We do not think those disparate matters in litigation in various district courts around the country is an effective or appropriate way for any of these determinations to be made.

Chairman SPECTER. Let me move to a series of questions with the minute I have left. Isn't it true as a practical matter de facto that the Foreign Intelligence Surveillance Act is not now the sole means of wiretapping in the United States where you have one party in the United States and one party out of the United States?

Mr. BRADBURY. That is correct. The President's program is outside of FISA.

Chairman SPECTER. So FISA is not the exclusive way. And isn't it also true that no statute, including the one I have proposed, can expand or contract the President's Article II powers?

Mr. BRADBURY. Well, I would say that statutes can reasonably regulate exercises of the President's constitutional authority. But where we see a real issue—and it is a very significant constitutional issue, and that is what the FISA Court of Review is talking about—is an effort to try to eliminate it or snuff it out. And that is where you get a real direct clash between the branches, and that is what we have always endeavored to avoid throughout this discussion. And I think your legislation recognizes that we all want to avoid that situation.

Chairman SPECTER. With Senator Leahy's acquiescence, I am going to pursue this just a bit further. When you talk about reason-

ably regulate, you come to Justice Jackson's famous concurrence in the steel seizure case. He said that when the President exercises his constitutional power, plus a grant of authority from the Congress under Article I, then his power is at a maximum because he has two powers, Article II and Article I.

Mr. BRADBURY. That is correct.

Chairman SPECTER. When he exercises Article II power alone, it is at the medium point, where he faces a situation where Congress has denied him certain authority, as where FISA is in existence, then he relies solely on his Article II power. But isn't that Article II power, whatever it is, as determined by the balancing test on the invasion of privacy versus the national security interest involved?

Mr. BRADBURY. That is right.

Chairman SPECTER. A final question. This provision in the bill has been cited repeatedly as a negative comment: "Nothing in this Act shall be construed to limit the constitutional authority of the President to collect intelligence with respect to foreign powers and agents of foreign powers."

Now, the best illustration of that is a wiretap of a foreign embassy. Isn't it true that that line was in the FISA Act of 1978?

Mr. BRADBURY. It was. I believe, Mr. Chairman, it was amended to take it out at a later point, and this legislation would reinstate it in the bill. But I think the important point is that the FISA Court of Review in its decision says essentially just exactly that. And this is simply a recognition or affirmation of what the FISA Court of Review has said.

In pointing to the embassy provision, you are exactly right that that is an example where FISA today recognizes and allows for the Executive Branch to take action without a court order to undertake foreign intelligence surveillance. And that is an authority that exists today and that is recognized in the FISA statute.

Chairman SPECTER. So, in totality, Article II power is what it is and it cannot be added to or subtracted by legislation since the Constitution supersedes legislation.

Mr. BRADBURY. The legislation does not change Article II authority. It can add Congress' authority, as Justice Jackson indicated in his concurrence, or it can attempt to leave the Article II authority as it is, or it can attempt to take away from it whatever authority Congress would otherwise provide, and—

Chairman SPECTER. But Congress does not have any authority by statute to change the Constitution.

Mr. BRADBURY. That is correct.

Chairman SPECTER. Including Article II.

Mr. BRADBURY. That is correct.

Chairman SPECTER. Senator Leahy, you have at least 10 minutes, or longer.

Senator LEAHY. Thank you. Of course, we do not amend the statute by—we do not amend the Constitution by statute, but as *Youngstown* pointed out, there are many areas where the President's Article II powers are circumscribed by statute. Is that not correct?

Mr. BRADBURY. Yes. In the exercise of those authorities, but not where those authorities—

Senator LEAHY. Thank you. I was glad to get a simple declaratory judgment—simple declaratory answer from someone from the Justice Department. It has been years. I compliment you, Mr. Bradbury. I compliment you. You will probably get fired for doing that, but I compliment you for doing it.

But the language that Senator Specter quoted was actually never enacted as part of FISA. It was struck from the conference in 1978, as I recall. But there are areas where we can—the Congress under Article I can determine the actions of the President under Article II, and then the President, of course, has—in his oath of office, he says that he will faithfully execute the laws of the United States. Now, of course, if he does not like the laws, he can always veto them.

General Alexander, let's go back to the Terrorist Surveillance Program because we may have been discussing two things in your answers to the earlier questions. Let's say that under this program you establish probable cause that a particular individual you are monitoring is a terrorist and that individual is within the boundaries of the United States. At that point do you go to FISA for a warrant?

General ALEXANDER. Not necessarily, sir. It may be. It may be. It would definitely go to one or the other intel agencies as soon as that is. Our objective would be NSA would not proceed at that point. We would pass it to either the FBI—

Senator LEAHY. If you are going to continue—you have got somebody in the United States. You have established probable cause, and this is putting aside for the moment whether the original program is actually authorized in the law or not. But let us assume you have got probable cause that somebody in Middlesex, Vermont, is a terrorist. I know all the people in Middlesex, Vermont. I do not think there are any.

General ALEXANDER. It would not happen, sir.

Senator LEAHY. But let's say you do. At that point do you have to go to the FISA Court for a warrant if you are going to continue monitoring that person, that individual?

General ALEXANDER. Actually, the procedure—

Senator LEAHY. Does somebody have to go to the FISA Court?

General ALEXANDER. Somebody, potentially, but not necessarily. And the question really gets to where are we in the process of knowing that that is a terrorist. If we know for sure that is a terrorist, it has gone to the FBI, the FBI would take that probably to a FISA and start their own procedures with the lead and investigative information that we gave them.

Generally, you do not have a clear-cut case like that, sir.

Senator LEAHY. I understand. I was trying to make it, for an easier answer, to make it clear-cut.

Let's go to Section 9(k) of the Chairman's bill. This would exempt from criminal liability any FBI agent or intelligence officer who executes a physical search for foreign intelligence information if the search is authorized "under the Constitution." Apparently, that is a reference to the President's claimed inherent authority as Commander-in-Chief. Does this immunize anyone who conducts warrantless searches of American homes and offices without court orders under the say-so of the President?

General ALEXANDER. Steve, do you want to answer that one?

Mr. BRADBURY. Well, I think, Senator, it simply conforms the law to what FISA is trying—

Senator LEAHY. No, no. Now, let's go back. You were so good before answering the question that I began with. Does this immunize somebody who conducted a warrantless search of an American home or office under the say-so of the President? I mean, that should be simple.

Mr. BRADBURY. Well, if intelligence officers have executed surveillance programs that have been duly authorized by the President, this would recognize that those intelligence officers who exercise those authorities should not be subject to a criminal process.

Senator LEAHY. So it immunizes—

Mr. BRADBURY. I would say, Senator, that that is the approach that FISA takes today. The officers and agents of the U.S.—

Senator LEAHY. This is different. This is in Section 9(k), saying if they are authorized by the President—the President. Not FISA but the President. Does that immunize them?

Mr. BRADBURY. Well, the legislation would recognize that there may be instances where there are programs authorized by the President. That is recognized in the legislation, and then there are procedures in place for judicial review. There are also procedures for the Attorney General in temporary circumstances to authorize surveillance without a court order. And so—

Senator LEAHY. Well, has the President authorized warrantless physical searches outside of FISA?

Mr. BRADBURY. I think that the only thing the President has talked about is the Terrorist Surveillance Program. That is the program that is done today without a FISA order. And that has been the subject of the hearings before this Committee, and I think it is an appropriate subject for the legislation that is being proposed.

Senator LEAHY. Can you answer the question whether he has authorized such warrantless searches?

Mr. BRADBURY. I am not going to say he has.

Senator LEAHY. I wanted to make sure you had a chance to respond on that specifically.

You know, I worry that what we are doing is trying to immunize a lot of activity. We had this great battle here conducted in the pages of the press and all on the question of torture. And then after wonderful signing ceremonies at the White House and everything else, the President said, However, there will be areas where we do not have to apply that law, and thus attempted to immunize people.

I worry when we start going into this question of immunization. I am not talking about the President's pardon ability, and we have seen that in Watergate and others where the President has pardoned people afterward, and Iran-contra and so on. I am talking about blanket immunization.

Let me ask both General Alexander and General Hayden this. As I understand FISA, it has always allowed the NSA to use a kind of vacuum cleaner approach to radio communications in the United States, sometimes referred to as the "NSA exemption." So in the Chairman's bill, if you repeal Section 101(f)(2) of FISA, would that

extend the NSA exemption to all electronic communications, both wire and radio?

General HAYDEN. Yes, I think the straightforward answer, Senator, is yes. And just one additional sentence of explanation is that it would allow NSA to target foreign entities—and we in our discussions, I think, have crossed some concepts here. In terms of targeting a foreigner for a foreign intelligence purpose, the Chairman's bill would allow NSA to use all the tools that it has. It would not make a distinction between grabbing a signal out of the air or grabbing a signal some other way.

Senator LEAHY. I understand. So, for example, if you had—this would allow you to seize and record all the calls between the United States and India, just blanket.

General HAYDEN. No, it would not.

Senator LEAHY. I am talking about under the—if you repeal Section 101(f)(2).

General HAYDEN. No, no, not at all.

Senator LEAHY. OK.

General HAYDEN. It would allow you to target a phone number in Central Asia, and it would give you the same ability to cover that target that you now have pulling that signal out of the air or collecting that signal overseas, it would allow you to use all the tools that we have at our disposal in order to get what we have already agreed is coverage of a legitimate foreign intelligence target.

Senator LEAHY. Do we do this kind of vacuum cleaner surveillance of Americans now?

General HAYDEN. You are talking about intercepting the content? Senator, everything that is done is targeted and for a foreign intelligence purpose. No.

Senator LEAHY. On these calls—and I understand, without going into the specifics of the program, you are taking a huge number of calls and e-mails, not specifically on a person. Are those then stored for retrieval and analysis by the NSA?

General HAYDEN. Senator, your premise is incorrect.

Senator LEAHY. OK.

General HAYDEN. Under the President's program, when NSA collects the content of a communication, it has already established a probable cause predicate that one or both communicants is associated with al Qaeda. So we do not vacuum up the contents of communications under the President's program and then use some sort of magic after the intercept to determine which of those we want to listen to, deal with, or report on.

Senator LEAHY. What if something is picked up by mistake? What happens to it?

General HAYDEN. There is a technical term called "inadvertent collection." If NSA collects something inadvertently, standard procedures for the President's program or the standard procedures we have for all inadvertent collection, it is destroyed.

Senator LEAHY. So it is not available to others throughout the Government.

General HAYDEN. Only with one exception. If the inadvertent collection contains evidence of a crime, policy and statute require us to report that. Otherwise, it is destroyed.

Senator LEAHY. Now, in addition to narrowing the definition of "electronic surveillance," as I read Section 9, it would expand the so-called embassy exception in Section 102 of FISA. Am I correct on that, Mr. Bradbury?

Mr. BRADBURY. Yes, Senator. I believe under this new provision, that provision would allow the Attorney General to approve for a period targeted foreign intelligence surveillance that is directed solely at the communications of foreign government operations or non-U.S. persons who are agents of a foreign government. Solely those communications.

Senator LEAHY. If this was passed, for example, if you had a Congressional staffer call the German Embassy to plan a Congressional trip to Berlin, that could be picked up.

General HAYDEN. Senator, across the board, when NSA conducts surveillance against a legitimate foreign intelligence target and that target is in communication with an American—the American is not the target; the foreign entity is the target—we have well-established procedures to protect the privacy of the U.S. communicant.

Senator LEAHY. Well, Section 9 of the Chairman's bill expands the definition of "agent of a foreign power." We expanded that definition a few years ago, the so-called lone-wolf amendment. It also changes the definition of "Attorney General" from being restricted to the Attorney General or Deputy Attorney General to any person or persons designated by the Attorney General. Would that permit the Attorney General to delegate to every FBI agent and intelligence officer in the country the authority to authorize emergency wiretaps of phone calls?

Mr. BRADBURY. No, Senator, that is not the way the Attorney General delegates his authority. So, for example—

Senator LEAHY. But under this change of definition to now include any person or persons designated by the Attorney General—I am not saying whether he would do it, but would he have that power?

Mr. BRADBURY. He would never do that. He would—

Senator LEAHY. Would he have the power?

Mr. BRADBURY. Not under his current—

Senator LEAHY. You buy a car that can go 125 miles an hour. You are going to say, "But, of course, I would never drive over the speed limit." But you could go 125 miles an hour. If this says he can delegate it to anybody, does he have the power to delegate it to anyone?

Mr. BRADBURY. He would delegate pursuant to his existing regulations on delegations, which are limited. And so in this case, for example, you would be talking about the Assistant Attorney General for the National Security Division, in all likelihood.

Senator LEAHY. But we have in the law now it is restricted to the Attorney General or the Deputy Attorney General, as we note a reference to that in Ruth Marcus's column this morning in the paper. But this would permit him to go way beyond that, does it not? I mean, just on the face of it. Aside from what he might or might not do, on the face of it does it allow him to go way beyond that?

Mr. BRADBURY. Well, Senator, let me say this: All authorities of the Attorney General today under statute, unless they are expressly limited against delegation, are subject to delegation by the Attorney General pursuant to his existing regulations in the Department of Justice, and this would simply allow for that. But under those regulations, authorities of the Attorney General are not widely delegated to all individual FBI agents, for example. That is simply not done and it would not be done.

Senator LEAHY. I had such hopes for you earlier when you actually answered a question yes or no. But I will submit the rest of my questions, Mr. Chairman. This is highly technical. Between the House and Senate, I remember we had more than a dozen hearings when we considered reauthorization of the PATRIOT Act. And this bill goes way beyond the PATRIOT Act. So we will require more answers, and I appreciate the extra time.

Chairman SPECTER. Well, Senator Leahy, we are available for more hearings. We have only had five. We will have as many as we need.

General Hayden, thank you for your testimony and thank you for your service.

General HAYDEN. Thank you.

Chairman SPECTER. General Alexander, thank you for your testimony and for your service.

General ALEXANDER. Thank you.

Chairman SPECTER. Mr. Bradbury, thank you for your testimony and your service. It is good to have real professionals come before this Committee and answer the questions.

Mr. BRADBURY. Thank you, Mr. Chairman, and thank you, Senator Leahy.

Chairman SPECTER. We turn now to Panel 2: Mr. Cunningham, Mr. Dempsey, Mr. Schmidt, and Ms. DeRosa.

Our first witness is Mr. Bryan Cunningham, principal in the firm of Morgan & Cunningham; bachelor's degree with distinction from the University of Iowa; law degree from the University of Virginia Law School; worked for the CIA for some 6 years, first as an intelligence analyst and later as executive assistant to the CIA Director; Special Assistant U.S. Attorney in the Department of Justice. His full resume will be made a part of the record.

We appreciate your coming in, Mr. Cunningham, and we are going to go back to 5-minute rounds now.

Senator LEAHY. Mr. Chairman, just before you start, I have just been advised by Ms. Katzman I forgot to put into the record—I had a number of things in my last question, if I might have permission to put that in the record.

Chairman SPECTER. Sure. Without objection, you may put them at your leisure.

[The full resume of Bryan Cunningham appears as a submission for the record.]

Chairman SPECTER. Mr. Cunningham, we are going back to 5-minute rounds and 5-minute openings, and the floor is yours.

STATEMENT OF H. BRYAN CUNNINGHAM, PRINCIPAL, MORGAN & CUNNINGHAM LLC, DENVER, COLORADO

Mr. CUNNINGHAM. Thank you, Mr. Chairman, Ranking Member Leahy, and other members of the Committee, for having me here today. It is a great honor and privilege to testify before you on something that I think is of absolutely vital importance to our Nation today, and that is, how to balance the need of this President and, perhaps more importantly, future Presidents to prevent catastrophic attack against our country with the cherished civil liberties and separation of powers that are the bedrock of our American democracy. As a national security and information security and privacy lawyer for most of my career, serving actually more time under Democratic Presidents than Republican, and participating in the Markle Task Force on National Security, a bipartisan group, I am confident that we can balance these two interests; that we must balance them correctly, or risk far more damage to our civil liberties in the event of a catastrophic attack than we have imagined to date; but only if, in my judgment, the Foreign Intelligence Surveillance Act is reformed and is amended along the lines, Mr. Chairman, of your bill, S. 2453.

In addition to responding to your questions, my testimony today, my statement, which I would ask to be put in the record, addresses essentially three—

Chairman SPECTER. Your full statement will be made a part of the record.

Mr. CUNNINGHAM. Thank you, Mr. Chairman. Essentially three issues.

First, it discusses what I believe to be the proper and appropriate way to analyze the constitutional question here. I understand why both the administration and many Members of Congress and commentators on all sides have addressed this principally as a question of the President's Commander-in-Chief authority under Article II of the Constitution. I believe based on much precedent cited in my testimony and also in a brief that I co-authored with the Washington Legal Foundation in the New York case, which I would also ask be put in the record today, that the best way to look at this issue is under the President's foreign affairs and foreign intelligence authority. And I would submit that that is the way that most courts historically have looked at it and balanced those interests, as you correctly suggested earlier, Mr. Chairman, against the interests of Congress.

I will not go into any detail about those arguments in my opening statement for purposes of time, but I would be happy to take any questions on that.

At the outset, I wanted to say just a brief word about bipartisanship. I am honored to be on this panel with a former Associate Attorney General for the Clinton administration. As I said, I have served in both administrations, and I would also commend to the Committee the work of David Kris, who I know has testified before this Committee, who was a senior FISA expert in the Clinton and the Bush administrations.

Now to the specific provisions, Mr. Chairman, of your legislation. I support the programmatic approval that is called for in that bill, along with a Democratic counterpart recommended in an op-ed

back in February exactly such a program of programmatic approval. I think it is really the only way that we can create a situation where FISA keeps pace with the technological changes since 1978 and the changes in the behavior of our enemies.

I strongly support also the concept of electronic tracking as outlined in the legislation. I think that the ability for the United States to use what I call "machine triage"—that is, sifting of large amounts of content by computers prior to human beings actually looking at the data—is important both for our national security and our civil liberties. And I am happy to see that concept included in your bill.

I would just say a couple of brief words about Section 801. There was a lot of discussion, appropriately, in the first panel about that. The language that would make it clear that the President retains his Article II—in my view, foreign affairs primarily, but Article II constitutional authority to conduct electronic surveillance for foreign intelligence purposes when at least one party is outside the United States or in other circumstances. There has been some discussion about why that is important, and I watched with interest your discussion with the Attorney General the other day, Mr. Chairman, about this issue. I think this is absolutely essential that this language be included in any FISA reform legislation, and I think it is essential for four reasons.

First, I think it is important that the public have a clear understanding and statement of what the law and the Constitution is. I know some of my colleagues on the Markle Task Force, whom I am proud to have served with and proud to be here with today, would agree with the notion that this, whatever our law is, should be made clear to the public. And I think 801 does that. I think it is a statement of the current law.

Second, I think it is important, I think it is necessary to get any President, whether this President or a future President, to agree to reform legislation like this.

And, third, I think it is important because it will help our officers avoid the risk aversion that General Hayden discussed earlier in the context of being criticized for following the law, to have it be clear that the Congress and the administration and the judiciary all agree on this state of the law.

And, finally, I think no President of either party should ever have to be forced in the future into the Hobson's choice of deciding whether to fail to collect information that could protect us against attack or be accused of violating the law.

I look forward to answering your questions. Thank you.

[The prepared statement of Mr. Cunningham appears as a submission for the record.]

Chairman SPECTER. Thank you very much, Mr. Cunningham.

Our next witness is Mr. Jim Dempsey, Policy Director for the Center for Democracy and Technology; bachelor's degree from Yale; law degree from Harvard; clerked for Massachusetts Supreme Court Justice Robert Braucher; served as assistant counsel to the House Judiciary Committee; has a distinguished record in the practice of law, which will be made a part of the record.

Thank you for coming in, Mr. Dempsey, and the floor is yours.

STATEMENT OF JAMES X. DEMPSEY, POLICY DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY, WASHINGTON, D.C.

Mr. DEMPSEY. Mr. Chairman, thank you for the opportunity to testify at this hearing today.

Mr. Chairman, we commend you for your tireless leadership in seeking to ensure judicial review of the President's warrantless surveillance program. From the outset, you have been forthright in your criticism of the administration and their disregard of the express requirements of the FISA statute. And now, through intense negotiation, you have secured the promise of the President to submit his current surveillance program to court review.

With profound respect, Mr. Chairman, we must conclude that the price you paid for that simple concession is far too high. It pains me to say this, Mr. Chairman, but your bill as it stands today is not a 21st century bill. To the contrary, it would turn the clock back to an era of unchecked Presidential power, warrantless domestic surveillance, and constitutional uncertainty.

Your bill as it now stands, Mr. Chairman, has been so far altered from its origins and has become so dangerous to fundamental constitutional precepts that, as one civil libertarian to another, Mr. Chairman, let me say that we would rather see the President's unlawful program continue unchecked than to see your bill enacted into law.

You said the President will not yield to Congressional mandate. True. This President has a radical view of Presidential power. The next President may not have that view. But your bill would endorse the radical concept of the imperial presidency. And once Congress gives up on the concept of checks and balances and gives the President the blank check, it may be decades before the pendulum can swing back to the center.

Let me just focus on two ways in which your legislation would turn back the clock to an era of warrantless surveillance.

Sections 5 and 6 of the Chairman's bill would authorize a program of domestic surveillance far broader than President Bush's program. The Attorney General has said, and General Hayden confirmed today, that the President's program targets only communications with particular suspected members or affiliates of al Qaeda, only on the basis of probable cause, only for short term, and only if one leg of a call is overseas.

Your bill, Mr. Chairman, would authorize seizing the contents of purely domestic calls of American citizens without probable cause, without specific suspicion, where the call has nothing to do with al Qaeda or even with terrorism, and would allow that surveillance to go on long term.

Section 9 of your bill, by redefining "electronic surveillance," would vastly expand the scope of warrantless surveillance, and the changes that you make to Section 102 of FISA would authorize warrantless surveillance of purely domestic calls.

General Hayden offered excellent testimony this morning, Mr. Chairman, and it provides a road map for how to address some of the problems facing the intelligence agencies today. But that road map does not lead to your bill.

On the question of who is the target, General Hayden emphasized the importance of the emergency procedures of FISA and about allowing the Attorney General to delegate his authority to grant emergency orders. I agree with that.

As to where is the target, General Hayden said how important it was—and you noted in your op-ed—when a foreign person is calling a foreign person, that a FISA order should not be required even if the vagaries of technology, the advances in technology put that call into the United States and at the disposal of the intelligence agencies. I don't think that foreign to foreign, accessible in the United States, is currently covered by FISA, and it shouldn't be.

In terms of technology neutrality, again, yes, the statute should be technology neutral. But in which direction? Your bill takes technology neutrality and uses it to expand the scope of warrantless surveillance. I think it is worth looking at using technology neutrality to expand the warrant requirement.

A lot of this boils down to one question: foreign to domestic calls. And one key word lacking from your bill, which we heard time and again from General Hayden and General Alexander, is the word "targeting." When the Government is targeting a known or suspected terrorist reasonably believed to be overseas, whether that call is intercepted in the United States or overseas, a warrant should not be required. And I think it is worth thinking about not turning off the tap when that target happens to call a number in the United States. If it turns out that he repeatedly calls the United States, then maybe you do have to go to a warrant, regardless of geography. But that is a much narrower solution to the problem of foreign to domestic than exists in your bill, and I think we can have a lot more in-depth discussion about how to respond to the global changes in technology without having a one-way downward ratchet so that just because technology is changed, privacy principles have to be abandoned.

Thank you, Mr. Chairman. I look forward to your questions and those of Senator Leahy.

[The prepared statement of Mr. Dempsey appears as a submission for the record.]

Chairman SPECTER. Thank you, Mr. Dempsey.

Our next witness is Mr. John Schmidt, partner of the firm Mayer, Brown, Rowe & Maw; cum laude graduate from Harvard College—magna cum laude from Harvard College, cum laude from the law school, and an editor on the Harvard Law Review; was Ambassador and Chief U.S. Negotiator on the Uruguay Round under the General Agreement on Tariffs and Trade; Associate Attorney General from 1994 to 1997; a visiting scholar at the Northwestern University School of Law.

We appreciate your coming in today, Mr. Schmidt, to testify, and we look forward to your testimony.

STATEMENT OF JOHN SCHMIDT, PARTNER, MAYER, BROWN, ROWE & MAW LLP, CHICAGO, ILLINOIS

Mr. SCHMIDT. Thank you, Mr. Chairman and Senator Leahy. I am happy to be here and give you my thoughts on what Congress should now be doing to improve the Foreign Intelligence Surveil-

lance Act. I have submitted a full statement, and I will summarize it as briefly as I can.

Chairman SPECTER. Your full statement will be made a part of the record.

Mr. SCHMIDT. I think it is important to get away from any talk or even thinking about whether the President or Congress is winning or losing or whether somebody is capitulating or compromising. None of that matters. What matters is whether we end up with an institutional structure that will both protect constitutional rights and achieve effective surveillance of al Qaeda and other terrorist groups.

It seems to me that the bill that you have introduced and that I understand the administration is now supporting would, in fact, be a constructive step to achieve both of those objectives. It would, as has already been discussed, allow the President to submit to the Foreign Intelligence Surveillance Court for a decision on its constitutionality a program of surveillance that does not involve the Court in the individualized approval of warrants specifying individual targets of surveillance.

The NSA program that we know something about is a program of that nature. The President cannot do that under current law. The FISA Court has made very clear it is a court of limited statutory jurisdiction. In fact, there was an effort some years ago to submit a physical search to the FISA Court before the statute allowed that, and the FISA Court said, "We don't do physical searches. We only approve electronic surveillance." The statute was later amended. But it is absolutely clear that the Court would not, could not do that now.

It seems to me that letting that Court determine the constitutionality of the NSA program or other programs that come along in future circumstances is really in everybody's interest. It is in the interest of the President to find out if, in fact, the Court agrees that that program is constitutional. He can make changes if he needs to. It is in the interest of Congress to get off of Congress the burden which some people want to put on you to make constitutional judgments of that nature. It is not that you cannot do it as individuals, but institutionally Congress is not in that business, Congress is not capable of making individualized judgments about a particular program's constitutionality. Oversight should continue. But oversight is not a substitute for a constitutional judgment by a court.

I think it is in the interest of the security professionals at the NSA and elsewhere to allow a court decision. That is something that we really have not talked much about, but, you know, there is no reason to think the current program is the last word on what we should be doing to use the electronic surveillance capacities we have against al Qaeda. If you are at the NSA today and you are thinking working on possible change in that program, if you come up with a new idea to change it, a new program, it has to be chilling, inhibiting to know that those efforts are likely to be the result in hearings of this nature, being able to get a court decision in advance on whether a program is constitutional gives those NSA professionals confidence that what they are doing is not going to be subject to that kind of controversy. And, most of all, it gives the

American people the confidence of knowing that there has been a court decision on the constitutionality of a program. I think courts are the way we make constitutional decisions in this country. It is the process that people have confidence in.

The part of the bill that seems to be the most controversial is the provision that says it recognizes that the President retains Article II surveillance authority outside the provisions of the statute. As has been noted, that is consistent with the judicial authority today, court of appeals decisions that recognize the President's authority and the 2002 Court of Review decision that says flatly Congress cannot encroach upon that authority. So it is not as though Congress is giving up anything which any court has ever said that it has.

But, you know, even if Congress could limit the President to a statutory surveillance process, I don't think Congress should want to do that. The strongest statements on this issue were made by Edward Levi, who was referred to earlier by Senator Kennedy, who played an active role in the development of the FISA statute, worked to pass it. Ed Levi always said that statute cannot be exclusive. He was insistent that there be an acknowledgment in the statute of the President's retained Article II authority. He was asked the question that Senator Leahy was pressing Mr. Bradbury on: What difference does it make if the President has the authority anyway? And Levi's response was it would create a dangerous confusion for Congress to pass a statute which did not acknowledge that the President retained his own constitutional Article II surveillance authority outside the terms of that statute. And if there was ever any doubt about whether Levi was right, it seems to me that the events of 9/11 prove that.

If it were true that the President was, in fact, limited to a statutory surveillance process, it would mean that if on the morning of 9/11 General Hayden had called President Bush and said, "We want to go forward immediately with the interception of calls at airports around this country where we think al Qaeda has people on the ground prepared to carry out further attacks," the President's only lawful response to that would be to say, "Well, we need to get the Attorney General, we need to begin examining whether each of those intercepts complies with the FISA statute, and maybe we will be able to get you authority by this afternoon or tomorrow morning."

That is not the way any American President would construe his constitutional authority when faced with an attack on this country. I do not think it is the way any Member of Congress wants him to construe it. And I can see no negative and it seems to me there is a positive in having the statute acknowledge that there are circumstances—which the statute does not try to define, but that the President retains Article II authority even in the face of any statute that Congress passes.

So I think it would be a good step. I think it would be an effort to rise above the current confrontation and create a mechanism that can avoid controversies like this in the future.

[The prepared statement of Mr. Schmidt appears as a submission for the record.]

Chairman SPECTER. Thank you very much, Mr. Schmidt.

Our final witness on the panel is Ms. Mary DeRosa, Senior Fellow at Johns Hopkins Center for Strategic and International Studies; bachelor's degree from the University of Virginia; law degree from George Washington University Law School; clerked for Second Circuit Judge Cardamone; had been special counsel to the Department of Defense; Special Assistant to the President for the National Security Council.

We thank you for joining us today Ms. DeRosa, and the floor is yours.

STATEMENT OF MARY B. DEROSA, SENIOR FELLOW, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, TECHNOLOGY AND PUBLIC POLICY PROGRAM, WASHINGTON, D.C.

Ms. DEROSA. Thank you, Mr. Chairman, Senator Leahy. Thank you for inviting me to testify today. I did want to just correct my institution. It is not the Johns Hopkins Center for Strategic and International Studies.

As you mentioned, I was a legal adviser at the National Security Council and a lawyer at the Department of Defense, and from that experience, both of those experiences, I developed an understanding of the need to act quickly and flexibly in the national security area and a strong appreciation for Executive authority. I actually thought at one point that I was sort of extreme on the subject of Executive authority, but I now realize that that is not the case.

I come to a discussion of FISA with a respect for the need in the Executive Branch to act nimbly, to adapt to changes in technology and threats, and I believe the law must permit this flexibility. But saying that national security operators need flexibility is not the same as saying that they must be able to take the easiest route in all cases.

Sometimes other priorities will require some different routes, some extra steps, and will make the job perhaps a little bit more difficult. That is not the inquiry, the correct inquiry. The correct inquiry is: Do these extra steps make it so that the operators cannot get what they need to get done done?

When we are talking about something as sensitive and intrusive as interception of private communications of people in the United States, court oversight of Executive Branch action, although it might not be the easiest way to go, is absolutely essential.

Experts in the late 1970s who crafted FISA concluded that the critical mechanism for ensuring public acceptance of national security wiretaps was a process that ensured careful court oversight of surveillance and making that process exclusive for approving surveillance decisions. And I would like to comment on some of the exchange with the last panel about whether the President's Article II powers can be limited in any way.

It is true absolutely that the President has Article II powers and authority to conduct electronic surveillance in the national security area, but that is the beginning of the inquiry. That is not the end of the inquiry. Congress absolutely may regulate and limit the exercise of those authorities. I am sort of uncomfortable as a former White House lawyer saying it, but I believe that that argument sells Congress' own authorities short.

In the Youngstown analysis that has been discussed, Category 3, where there is a conflict between the Congress' exercise and the President's exercise, Justice Jackson said at that point the President's powers—the ability to exercise his powers is at its lowest ebb. It is not unaffected—the Article II powers are not unaffected. That is Category 2. In Category 3, the President's ability to exercise his authority is at its lowest ebb. So Congress can affect and in the case of FISA did intend to affect the exercise of those powers.

Now, does that mean necessarily that those powers are extinguished. In my view, no. There might be something left. It depends on the extent of the Congress' powers. But it is unquestionably something less, something limited. I think in the circumstances of the Hobson's choice that Mr. Cunningham mentioned and the 9/11 circumstance that Mr. Schmidt mentioned, perhaps there would be some authority under those very, very limited, exigent circumstances, limited period of time to do something within the President's power. But it is not an unlimited entire exercise of the Article II authorities.

The drafters of FISA made concessions to the need for flexibility along the way, and the FISA Court is not a regular Federal court. It operates in secret and ex parte. And the requirement for obtaining a warrant is not like a criminal probable cause requirement. It is a much less rigorous standard, the probable cause that the target is an agent of a foreign power. But it is a disciplined process, and it is transparent in that the public understands what is happening and understands the rules.

I see that my time is just about out, and I welcome your questions.

[The prepared statement of Ms. DeRosa appears as a submission for the record.]

Chairman SPECTER. Thank you very much, Ms. DeRosa.

Mr. Dempsey, you testified and you have in your written statement this sentence: "With profound respect, we must conclude that the price the Chairman paid for that simple concession is far too high." That follows the sentence there was the "promise of the President to submit his current program to court review." And you characterize it as a "simple concession."

Have you ever gotten a concession from a President?

Mr. DEMPSEY. It is not hard, Mr. Chairman, and—I mean, it is not easy, excuse me.

[Laughter.]

Chairman SPECTER. Well, wait a minute. Is it hard under the Freudian slip or is it easy? Have you followed what President Bush has done by way of signing statements?

Mr. DEMPSEY. Mr. Chairman, this is a President who has an extreme view of—

Chairman SPECTER. Have you followed—

Mr. DEMPSEY. Yes, I have.

Chairman SPECTER.—what the President has done on signing statements?

Mr. DEMPSEY. Yes, Mr. Chairman.

Chairman SPECTER. Have you followed what he did on refusing to give clearance to the Office of Professional Responsibility to check on the surveillance program?

Mr. DEMPSEY. Yes.

Chairman SPECTER. Have you followed the activities generally of the President's view of Executive authority?

Mr. DEMPSEY. Yes.

Chairman SPECTER. Well, I will not ask you how you can say it is a simple concession, but let me tell you that to get the President's—well, let me rephrase it. Have you ever seen in the past a President agree to legislation that he was generally opposed to through negotiations in advance of the introduction of a bill? Do you know of any precedent for that?

Mr. DEMPSEY. I am sorry, Mr. Chairman. I did not understand that question.

Chairman SPECTER. Well, have you ever seen the President negotiate an agreement to sign a bill that was not originated by the administration?

Mr. DEMPSEY. I cannot cite one, but I don't know that it has not happened.

Chairman SPECTER. Well, I would just suggest to you that given the President's attitude on the surveillance program and his attitude on Executive power generally, it was not a simple concession but really was quite a breakthrough. But I respect your difference of opinion.

Mr. DEMPSEY. May I respond, Mr. Chairman? May I respond?

Chairman SPECTER. Sure.

Mr. DEMPSEY. Call it, then, a major concession. The price is still too high because for this one promise to submit this one program to the FISA Court, your bill would excuse this President from submitting any future program and any future President from submitting any other program to the Court.

Chairman SPECTER. Would excuse him from submitting any program? You say "excuse"?

Mr. DEMPSEY. Yes. It would give him—

Chairman SPECTER. Well, the President has no obligation to submit this program or any program to the Court, as President Bush interprets his Article II power.

Mr. DEMPSEY. And this is where I think that we have a monumental clash, and you have put yourself into the middle of that clash, Mr. Chairman, and you are to be complimented to the highest degree. But there is—

Chairman SPECTER. Well, I did not put myself there. The Senate did by making me Chairman of the Judiciary Committee. But let me move on—

Mr. DEMPSEY. And you accepted, Mr. Chairman, if I—

Chairman SPECTER. Just a minute, Mr. Dempsey. I have heard you on that. I want to ask Ms. DeRosa a question based on your testimony. Ms. DeRosa, do you agree with what Mr. Dempsey has had to say, that he would prefer to see the President's unlawful conduct continue rather than have a structured review by the FISA Court?

Ms. DEROSA. Well, I am not sure that I would characterize it exactly the way you have, but I do—

Chairman SPECTER. No, I did not characterize it that way. Mr. Dempsey said that he would prefer to see the President's unlawful conduct continue.

Ms. DEROSA. I think given the legislation as written, I would prefer no legislation to the legislation that is introduced because I believe that it—although I think judicial review of this program is a high priority, it is not as high as exclusivity and some of the other issues that are raised by—

Chairman SPECTER. Is there exclusivity for FISA today?

Ms. DEROSA. Well, I believe that there is. I believe that it is clear from the language of the statute that that is what was intended. And as a practical matter, is the President complying with the language of the statute? No. But that is what the statute clearly states and would for the future as well.

Chairman SPECTER. My red light went on in the middle of your answer, so I will yield to Senator Leahy.

Senator LEAHY. Thank you.

Mr. Schmidt, good to see you here. I listened to your hypothetical about what the President might do if he was asked to track some of these people on September 10th or 11th. Let's go from the hypothetical to the reality. The reality is that the Bush administration had all the information necessary to stop the attack on September 11th and failed to act upon it. In fact, if you want to go to what happened on September 10th, they were proposing to cut very substantially the counterterrorism funds for investigations in this country. The thing is we can change the laws all the way we want. Sometimes it requires a little competence in using what they have.

Now, Mr. Dempsey, having watched the President's unwillingness to obey the law and follow the law, you are not suggesting that Congress then should simply give up and ignore our own Article I powers that could require the President to follow the law?

Mr. DEMPSEY. No, Senator, and I think there is a bill before the Committee, the Specter-Feinstein bill, that would insist upon Congress' powers under the Constitution and would require the President or be more likely to require the President—he still may disregard it. I think that this is an absolutely momentous debate that we are in, and it may take years for this conflict between the President's vision of Executive power and what I believe to be the constitutionally correct vision of Presidential power, endorsed most recently by the Supreme Court in the *Hamdan* case.

Senator LEAHY. I am going to be getting to that. The Chairman asked Ms. DeRosa whether there is exclusivity today. Of course, the answer is yes. And you and I agree on one thing. The President's program is unlawful.

Now, if we repeal the exclusivity provision, what effect would that have?

Mr. DEMPSEY. Then that would make FISA optional and would cast doubt, constitutional doubt, on surveillance activities. Here we are in the middle of a war against terrorism. We have a FISA statute that has been approved by every court that has reviewed it. Evidence from FISA surveillances has been introduced in hundreds of criminal cases and never been rejected. And here we are proposing to cast that aside and allow the President to carry out wire-

taps outside of that. What if they find a real terrorist? What if the evidence is rejected in court?

It is a very risky approach to cast aside what in my view the Supreme Court has held is appropriate, that is, Congress has war powers, the President has war powers. Congress, in its exercise of its war powers under the necessary and proper clause, under its authority to regulate the armed forces, can adopt legislation that limits the President's inherent power.

Senator LEAHY. In fact, many of the arguments made by the administration about what the powers are showing here is what happened in World War II and on and on, all of that was before FISA was enacted. Then came Justice Jackson's decision in *Youngstown Steel*. That would certainly circumscribe what the President could do.

Do you agree with Attorney General Gonzales that Section 8 of the bill is meaningless and does not change the status quo?

Mr. DEMPSEY. Well, if it is meaningless, then let's not pass it.

Senator LEAHY. OK.

Mr. DEMPSEY. Other than the fact that the Chairman feels that that is what it will take to get the President, that was the quid pro quo for the President submitting this one program—

Senator LEAHY. Of course, I have stated before, you know—and I was not in the negotiations, but basically I worry the President said here, "I will stop breaking the law if you will pass a law saying that I am pardoned from breaking the law and I do not have to follow the law anymore."

The Justice Department White Paper on the so-called—that is sort of "Alice in Wonderland." The Justice Department White People on the so-called Terrorist Surveillance Program assumes that the NSA's activities constitute electronic surveillance as defined by FISA. A reasonable assumption given the current definition of "electronic surveillance," which covers any wire communication to or from a person in the U.S. if the acquisition occurs in the U.S.

The Chairman's bill narrows the definition, in particular, repeals the language I just referred to. As you read the new definition, would the NSA's activities, or at least the activities the President has acknowledged so far, still constitute electronic surveillance? Or would FISA no longer require the Government to get a warrant for those activities?

Mr. DEMPSEY. Well, actually, the President's program, because it is foreign to foreign and they are targeting somebody overseas, I guess it would not require a warrant for the President's program.

Senator LEAHY. OK. And you will have a chance—

Mr. DEMPSEY. Although let me say that General Hayden testified that they have probable cause and specificity for every single one of the surveillances under the President's program, which would fit the FISA definition currently. Also, as I said, General Alexander and Senator Feinstein had sort of an "aha" moment there when General Alexander was explaining that the NSA, our Government, has benefited from a windfall as a result of the changes in technology, such that a large percentage of foreign-to-foreign communications now pass through the United States. So what the NSA used to have to try to acquire overseas, where FISA does not apply, is now available to them in the United States. And everybody

agrees, including from the civil liberties perspective, that foreign to foreign should be exempt from FISA regardless of geography, regardless of where the interception occurs, and regardless of the technology.

General Alexander said, But then once we start in the United States targeting an individual overseas, most of whose conversations are foreign to foreign and, therefore, exempt, and we find a foreign-to-domestic conversation, under current law, if they are in the United States, they have to suspend, and they believe they have to go get a warrant.

Now, that is a problem worth thinking about; that is, where you are targeting an individual overseas, most of his conversations are foreign to foreign. You can get him in the United States even though he is overseas. His communications get routed through this country, an accident of the evolution of technology that was not apparent in 1978.

Now, I think it is worth thinking about, if we are talking about that problem, a much more narrow definition. The Chairman's bill would say that anything that is foreign to foreign, including when you are not targeting a foreigner, or anything that is foreign to domestic, including when you are not targeting a foreigner, would be exempt from the warrant requirements—which, by the way, also makes it exempt from the statutory minimization requirements and casts you only back upon whatever the President decides to adopt on his own.

So I think that there is something there worth thinking about, but it is far narrower, Mr. Chairman, than what is in your bill.

Senator LEAHY. I will submit my other questions for the record.

Chairman SPECTER. Thank you very much, Senator Leahy.

Thank you, Mr. Cunningham, Mr. Dempsey, Mr. Schmidt, and Ms. DeRosa. We very much appreciate your testimony.

[Whereupon, at 12:08 p.m., the Committee was adjourned.]

[Questions and answers and submissions for the record follows.]

QUESTIONS AND ANSWERS

Senator Arlen Specter
FISA for the 21st Century
Wednesday, July 26, 2006
Questions for Lt. General Keith B. Alexander

1. Not only has the FISA Court been able to maintain its secrecy where both the Executive and Legislative branches have allowed leaks, but they are in the best position to weigh and balance the nature of the threat, the scope of the program, how many people are being intercepted, what is being done with the information, what is being done on minimization, how successful the program has been, if any projected terrorist threats have been thwarted, and all factors relating to the specifics on the program. Do you believe that the best solution to the possible problem that the president may lack the authority to conduct warrantless wiretaps is to submit the program to the FISA Court of Review and allow them to determine the constitutionality of the program?

ANSWER: (U) No. The Foreign Intelligence Surveillance Court of Review ("the Court of Review") is an Article III court of limited jurisdiction. The Court of Review does not—and cannot, consistent with the limitations of Article III—issue opinions beyond its statutory authorization. At present, the Court of Review has jurisdiction only with respect to orders of the Foreign Intelligence Surveillance Court *denying* applications by the Government to conduct surveillance pursuant to FISA. *See* 50 U.S.C. § 1803(a), (b). With respect to legislative efforts to change the Court of Review's jurisdiction, S. 3931 would not alter the jurisdiction of the Court of Review in any relevant respect.

2a. Technology has changed tremendously since 1978. What are some of the technological hurdles that make FISA obsolete today?

ANSWER: (U) A full explanation of the technological changes that have impacted the operation of foreign intelligence operations conducted under FISA would require a discussion of highly classified and sensitive information, which is inappropriate for this forum. In short, there has been a radical transformation since 1978 of the means by which the world transmits communications. When FISA was enacted into law in 1978, almost all transoceanic communications into and out of the United States were carried by satellite and those communications were, for the most part, intentionally omitted from the scope of FISA, consistent with FISA's focus upon regulating the collection of foreign intelligence from domestic communications of United States persons. Congress could not have anticipated the revolution in telecommunications technology that would establish global, high-speed, fiber-optic networks that would fundamentally alter how communications are transmitted. Nor could Congress have anticipated the stunning innovations in wireless technology, or the explosion of the volume of communications, that have occurred in recent decades. Unpredicted advances in the development and deployment of new technologies, rather than a considered judgment by Congress, has resulted in the considerable expansion of the reach of FISA to additional technologies and communications beyond the statute's original focus on domestic communications.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00054 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.001

2b. Do you agree with how S. 2453 deals with emerging technological issues?[1]

ANSWER: (U) Yes. FISA should be amended so that it is technology-neutral. This would return it to what we believe was its original purpose of protecting the privacy of persons in the United States. The revolution in telecommunications technology has extended the impact of the FISA regime far beyond what Congress could ever have anticipated in 1978. At present the requirement for a court order depends in part upon both the location at which surveillance is conducted and the particular communications technology employed. S. 2453 would return FISA to what we believe was its original purpose of protecting the privacy of persons in the United States.

2c. Is it feasible for the FISA Court to make the type of determinations and issue the type of program-wide warrants that the bill envisions?

ANSWER: (U) Yes. The judges of the Foreign Intelligence Surveillance Court are highly experienced with the issues implicated by electronic surveillance conducted for the purpose of collecting foreign intelligence. In addition, many of the requirements for approving an electronic surveillance program are very similar to those that FISC judges have been making for years in authorizing electronic surveillance under FISA. Indeed, many of the "necessary findings" set forth in Section 6 of the bills, including S. 2453 and S. 3931, that the FISC would have to make before authorizing programmatic surveillance are similar to those contained in section 105(a) of FISA, 50 U.S.C. § 1805(a).

3. What suggestions do you have to improve my legislation?

ANSWER: (U) All suggestions NSA had for improving the draft legislation have already been provided in the informal Administration process of consultation and providing technical assistance. We look forward to working further with you and Congress as this bill moves through the legislative process. FISA reform is extremely important to the security of the country.

4. Could the Foreign Intelligence Surveillance Court (FISC) authorize a broad collection whereby communications are intercepted when the connection to terrorism is very attenuated or would that potentially violate the Fourth Amendment?

ANSWER: (U) NSA is not in a position to speculate on what actions the FISC might take in a particular case. Of course, all surveillance conducted under FISA must be consistent with the Fourth Amendment's overriding requirement of reasonableness.

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

---

[1] NSA notes that the proposed language of S. 2453 continues to be modified. At present, the Senate's FISA modernization proposal that most closely resembles S. 2453 is S. 3931, the Terrorist Surveillance Act of 2006, as introduced. In most cases, the answers provided herein are responsive to the questions that remain relevant in S. 3931; i.e., where the language in S. 3931 does not substantively change the context of the question. A note has been made to indicate those questions where the significant changes in S. 3931 make the question inapplicable.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00055 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.002

ANSWER: (U) Yes. Although the Department of Justice is better suited to answer constitutional law questions, the general point that legislation cannot override the Constitution is correct. Congress cannot by statute take away from the President authority that the Constitution vests in him.

5a. If that is so, does repealing the so-called exclusivity provision do more than make clear that Congress does not wish to provoke a constitutional clash?

ANSWER: (U) The Department of Justice is better suited to answer this question. Nevertheless, I would say that repealing the so-called "exclusive means" provision would make clear that Congress is not interested in provoking a conflict between the branches.

5b. Aside from the constitutional law, is it good policy to interfere with the President's ability to detect and prevent terrorist plots of a declared enemy?

ANSWER: (U) It is, of course, never good policy to interfere with the Nation's ability to detect and to prevent terrorist plots. Recent events in Britain remind us that, five years after al Qaeda succeeded in launching the single most deadly foreign attack on American soil in history, we continue to confront a determined and deadly enemy that is dedicated to launching further catastrophic attacks against America. We act at our peril if we do not do everything in our power to detect and prevent such plots.

6. In your opinion, would the President continue the Terrorist Surveillance Program if the Foreign Intelligence Surveillance Court or the Court of Review concluded that the program is unconstitutional?

ANSWER: (U) I cannot, of course, speak for the President on what he might do if the FISC or the Court of Review concluded that the Program is unconstitutional. That said, I am confident that the Terrorist Surveillance Program is lawful and that the courts will come to the same conclusion.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00056 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.003

Senator Charles E. Schumer
FISA for the 21st Century
Wednesday, July 26, 2006
Questions for Lt. General Keith B. Alexander

1. On July 13, Senator Specter announced that he had reached a deal with the White House on his legislation to authorize the Terrorist Surveillance Program and re-write much of the Foreign Intelligence Surveillance Act (FISA). This was just two weeks after the Supreme Court's decision in *Hamdan*, which many have characterized as a rebuke of the Administration's legal defense of the President's warrantless surveillance program.

1a. Do you continue to believe that the NSA Surveillance Program is legal and Constitutional and that it would survive any legal challenge in the FISA Court?

ANSWER: (U) NSA believes that the Terrorist Surveillance Program is lawful, and that the Foreign Intelligence Surveillance Court would uphold the legality of the Program. As Assistant Attorney General Moschella explained in his detailed response to your June 30th letter, it is the considered legal judgment of the Executive Branch that the Supreme Court's decision in *Hamdan v. Rumsfeld* does not affect the analysis set forth in the Department's January 19th *Legal Authorities* paper outlining the legal basis for the Terrorist Surveillance Program. As the Moschella letter explains, there are many reasons to support that conclusion, but at bottom, the relevant statutory scheme at issue in *Hamdan* is fundamentally different from the one implicated by the Terrorist Surveillance Program. FISA expressly contemplates that Congress may authorize electronic surveillance through a subsequent statute without amending or repealing FISA. *See* 50 U.S.C. § 1809(a)(1) (prohibiting electronic surveillance "except as authorized by statute"). The primary provision at issue in *Hamdan*, Article 21 of the Uniform Code of Military Justice ("UCMJ"), has no analogous provision. Moreover, the Supreme Court recognized in *Hamdi v. Rumsfeld*, 542 U.S. 519 (2004), that the Authorization for Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (Sept. 18, 2001), satisfies a statute similar to FISA prohibiting detention of U.S. citizens "exception pursuant to an Act of Congress," 18 U.S.C. § 4001(a). Because the Terrorist Surveillance Program implicates a statutory regime analogous to the one at issue in *Hamdi*, we believe that the reasoning of that decision is far more relevant to the Program than *Hamdan*.

1b. If the administration has "the authority, both from the Constitution and the Congress, to undertake this vital program," as President Bush asserted in January, what need is there to legislate on this issue from your perspective?

ANSWER: (U) As stated in the Department of Justice's *Legal Authorities* paper, the Executive Branch has the statutory and the constitutional authority to implement the Terrorist Surveillance Program. Nevertheless, additional legislation could be very helpful by providing additional authority for the Terrorist Surveillance Program and by modernizing FISA to confront the new threats and technologies of the 21st Century.

1c. Would you prefer that Congress not legislate in this area at all?

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00057 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.004

ANSWER: (U) No. As indicated above, the Executive Branch wants to work with Congress on electronic surveillance issues, including legislation addressing the Terrorist Surveillance Program.

1d. Did the Supreme Court's recent ruling in *Hamdan* play any role in the Administration's decision to support Senator Specter's legislation?

ANSWER: (U) No. The Executive Branch supports Senator Specter's bill, S. 2453, because it is a sound proposal to allow the FISC to approve programmatic electronic surveillance and to modernize FISA, while better protecting the privacy of United States persons.

2. Senator Specter has characterized his bill as simply allowing the Court to decide the Constitutionality of the program, including whether the President has the authority to authorize this surveillance. It has been said that if kept in its precise current form, the President will submit the program to the FISA Court. Why doesn't the Administration just submit the program to the FISA Court now, without any legislation?

ANSWER: (U) Traditional FISA procedures do not allow the speed and agility that makes the Terrorist Surveillance Program such an important early-warning system. Legal options, however, are always being evaluated.

3. If the Specter bill is passed in its current form, what signing statement do you anticipate the President issuing in connection with it?

ANSWER: (U) NSA is not in a position to answer this question.

4. If the Specter bill is passed in its current form, and the Administration then voluntarily submitted the program to the FISC, would the Administration argue that the Specter bill authorized the NSA's Terrorist Surveillance Program?

ANSWER: (U) NSA is not in a position to answer this question.

5. Do you believe that the portion of the Specter bill that allows the President to submit the NSA surveillance program to the FISA Court is constitutional? Specifically, do you believe this provision does not run afoul of the constitutional proscription against advisory opinions?

ANSWER: (U) NSA is not in a position to answer this question.

6. The Specter bill provides that any cases pending right now – upon application by the Attorney General – must be transferred to the FISA Court of Review. The bill also provides that the decision of that FISA Court "shall be subject to certiorari review in the United States Supreme Court."

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00058 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.005

6a. Is it your understanding that one who is challenging a FISA Court decision favorable to the government may obtain review before the Supreme Court under the bill?

ANSWER: (U) NSA is not in a position to answer this question.

6b. What are the arguments against allowing the constitutional review in a traditional Federal District Court, with expedited review to the Supreme Court, so long as the court applies the procedures and standards of the Classified Information Procedures Act?

ANSWER: (U) The FISC is better suited than ordinary district courts to deal with this area of law both because of its experience in that area of law and because it has the facilities and experience required to handle highly classified material.

7. During his February appearance before the Committee, Senator Biden asked Attorney General Gonzales what harm had been caused by public disclosure of the warrantless surveillance program. He responded: "You would assume that the enemy is presuming we are engaged in some kind of surveillance. But if they're not reminded about it all the time in the newspapers and in stories, they sometimes forget." When I asked him the same question in July, he deferred to the intelligence community.

7a. Do you have a better answer as to how the disclosure that wiretapping is going on harmed national security?

ANSWER: (U) Disclosure of the Terrorist Surveillance Program puts at risk efforts by the U.S. Government to prevent catastrophic al Qaeda-sponsored attacks within the United States. Even the smallest reduction in the effectiveness of the Program could be catastrophic in an environment in which we cannot afford to miss one plot, one event, one individual, or one movement. These unauthorized disclosures also have a chilling effect on cooperation, affecting both friendly governments and individual clandestine sources. To put it starkly, if we cannot be trusted to keep our own secrets, why should others share sensitive information with us? Finally, foreign intelligence services and non-state terrorist groups capitalize on this public hemorrhage of U.S. secrets, which becomes a "bonus," enriching the unclassified open source collection activities many of our opponents already perform.

7b. To your knowledge have any officials in the intelligence community had direct discussions with Attorney General Gonzales or officials in his Department about how disclosure of the program harmed national security? If so, what was said?

ANSWER: (U) Neither I nor other officials in the Intelligence Community can reveal the internal deliberations of the Executive Branch or the content of our confidential discussions with the Attorney General.

8. Do you have legal or constitutional concerns about the use of warrantless physical searches in the United States?

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00059 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.006

ANSWER: (U) No. NSA is confident that any such activities would be conducted only as consistent with the laws of the United States, including the Constitution. We are not, however, in a position to either confirm or deny any asserted intelligence activities.

9. To your knowledge, has the Administration ever used its commander-in-chief powers or the AUMF to justify warrantless physical searches?

ANSWER: (U) NSA is not in a position to confirm or deny any asserted intelligence activities. Our inability to discuss such asserted programs should not be taken as an indication that such activities exist.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00060 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.007

Senator Dianne Feinstein
FISA for the 21st Century
Wednesday, July 26, 2006
Questions for Lt. General Keith B. Alexander

Background. Several of us in Congress – and especially those of us serving on the Intelligence Committees – were surprised and disappointed that we had to learn of the so-called Terrorist Surveillance Program from the *New York Times*. Since then, we have read reports about other programs as well.

A May 12, 2006 *USA Today* story, reporting on the NSA's apparent collection of millions or even billions of telephone records from major carriers, has been denied by some carriers but not others. Last week, it was revealed that Republican House Intelligence Chairman Hoekstra had sent a letter to the Administration complaining of another program that had not been disclosed to his committee. And in earlier testimony, the Administration has alluded to the possibility, but did not confirm, that other intelligence programs could exist.

- Are there any intelligence programs carried out by your agencies, or otherwise within the intelligence community that you know of, that have not been briefed to the Congressional intelligence committees?

ANSWER: (U) As Director of the National Security Agency, I can only speak for NSA. I assure you that NSA takes its congressional reporting obligations extremely seriously. The National Security Act of 1947 contemplates that the Intelligence Committees of both Houses would be appropriately notified of any such intelligence programs that exist, and the Act specifically contemplates more limited disclosure in the case of exceptionally sensitive matters. Title 50 of the U.S. Code provides that the Director of National Intelligence and the heads of all departments, agencies, and other entities of the Government involved in intelligence activities shall keep the Intelligence Committees fully and currently informed of intelligence activities "[t]o the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters." 50 U.S.C. §§ 413a(a), 413b(b). It has for decades been the practice of both Democratic and Republican administrations to inform only the Chair and Ranking Members of the Intelligence Committees about exceptionally sensitive matters. The Congressional Research Service has acknowledged that the leaders of the Intelligence Committees "over time have accepted the executive branch practice of limiting notification of intelligence activities in some cases to either the Gang of Eight, or to the chairmen and ranking members of the intelligence committees." *See* Alfred Cumming, *Statutory Procedures Under Which Congress is to be Informed of U.S. Intelligence Activities, Including Covert Actions*, Congressional Research Service Memorandum at 10 (Jan. 18, 2006).

- Did anyone in the Administration offer, grant or otherwise provide in any way some sort of promise of immunity or offer of protection against civil or criminal liability to

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00061 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.008

telecommunications or internet service provider or financial entities or any other company for their cooperation in any of the surveillance programs? If yes, under what legal authority?

ANSWER: (U) Operational information about the Terrorist Surveillance Program is highly classified and exceptionally sensitive. Publicly revealing information about the operational details of the Program could compromise its value and facilitate terrorists' attempts to evade it. Accordingly, we cannot confirm or deny operational details of the Program in this setting. As you are aware, the operational details of the Program have been and continue to be reviewed by the full intelligence committees and, in certain circumstances, congressional leadership.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00062 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.009

Senator Edward M. Kennedy
FISA for the 21st Century
Wednesday, July 26, 2006
Questions for Lt. General Keith B. Alexander

1. In a White House press briefing on December 19, 2005, Attorney General Gonzales said that the standard for beginning surveillance on an individual under the NSA warrantless wiretapping program is "a *reasonable basis* to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda." Similarly, in a session with *The San Diego Union-Tribune*, published on February 5, 2006, General Hayden said that the constitutional standard under the Fourth Amendment is "*reasonableness*," ignoring the probable cause provision of the Fourth Amendment.

   However, as General Hayden told the Senate Judiciary Committee on July 26, 2006, "There is a *probable cause* standard, before any communication is intercepted, that one or both communicants is, again, to a probable cause standard, associated with al Qaeda."

1a. Is the standard used by the NSA reasonableness or probable cause, in determining the targets for wiretapping under the NSA's warrantless wiretapping program? Has the standard ever changed from "probable cause" at any time, for any reasonable period, since September 11th?

ANSWER: (U) The Department of Justice is in a better position to discuss the "probable cause" standard. Nevertheless, the Terrorist Surveillance Program is narrowly tailored to target for interception only communications where one party is outside the United States and there are reasonable grounds to believe that at least one party is a member or agent of al Qaeda or an affiliated terrorist organization. The Program has consistently employed this standard. The "reasonable grounds to believe" standard is synonymous with "probable cause." *See, e.g.*, *Maryland v. Pringle*, 540 U.S. 366, 371 (2003) ("We have stated . . . that '[t]he substance of all the definitions of probable cause is a reasonable ground for belief of guilt.'") (internal quotation omitted).

2. The bill negotiated between Senator Specter and the Administration would allow authorization of a spying program targeted not just at members of al Qaeda but at anyone "reasonably believed to have communication with or be associated with" *any* foreign powers or their agents engaged in terrorism preparations. This broad standard could sweep in thousands of innocent Americans who are unaware that someone in the federal government has determined that they are "associated with" a person the government considers to be a terrorist.

Question:

2a. What is the justification for a standard that is even broader than the current standard, which requires probable cause that one person involved in the communication is directly "affiliated with al Qaeda" or "associated with al Qaeda" [The standard most recently

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00063 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.010

articulated by General Hayden at the July 26, 2006, hearing before the Senate Judiciary Committee]?

ANSWER: (U) The United States faces a flexible, secretive, decentralized, and constantly evolving global network of terrorist cells. The need for an agile surveillance system is at a premium because our adversaries in the War on Terror seek to inflict massive casualties through another catastrophic attack on our homeland.

2b. What would be the basis and legal standard to conclude that a U.S. person is "associated with" al Qaeda or an organization determined to be affiliated with al Qaeda under the proposed legislation?

ANSWER: (U) The professional intelligence officers at the National Security Agency, who are experts on al Qaeda and its tactics, including its use of communication systems, with the assistance of other elements of the Intelligence Community and subject to appropriate and vigorous oversight by the NSA Inspector General and General Counsel, among others, would rely upon the best available intelligence information to determine whether there are reasonable grounds to believe that a party to an international communication is affiliated with al Qaeda.

3. In December 2005, at a White House press briefing, General Hayden said that the NSA warrantless wiretapping program targeting communications that involve al Qaeda, with one end inside the United States, had been successful in detecting and preventing terrorist attacks. He also said that the program deals only with international calls with a time period much shorter than is typical under the Foreign Intelligence Surveillance Act.

When asked about the inadequacies of FISA, which led to the creation of the domestic spying program, General Hayden said that the "whole key here is agility… [and] the intrusion into privacy is significantly less. It's only international calls," and the time period for surveillance is shorter than that is generally authorized under the Foreign Intelligence Surveillance Act. Attorney General Gonzales reiterated the statement that the program was limited to those with ties to al Qaeda.

In a session with the *San Diego Union-Tribune*, General Hayden said that the publicly acknowledged program is "limited" and "focused," and has been "effective."

At the Senate Judiciary Committee hearing on July 26, 2006, Mr. Bradbury stated that the program involves "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 affiliate terrorist organization."

The program described in the bill negotiated by the Administration and Senator Specter is significantly broader than the program General Hayden said had been successful in detecting and preventing attacks. The bill would allow authorization of a spying program targeted not just at members of al Qaeda but at anyone

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00064 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.011

"reasonably believed to have communication with or be associated with" *any* foreign powers or their agents engaged in terrorism preparations. This broad standard could sweep in thousands of innocent Americans who are unaware that they are "associated with" a person the government considers to be a terrorist.

General Hayden has also repeatedly stated that the targets for the wiretapping are approved by "shift supervisors," whom he later characterized as "senior executives." Yet, this bill authorizes the Attorney General to delegate his authority to anyone he wishes, instead of limiting the delegation to senior officials.

Questions: Members of the Administration have repeatedly claimed that the publicly announced program has saved an untold number of American lives.

3a. Why did the Administration insist on a bill that would allow the authorization of a program that spies on even more Americans?

ANSWER: (U) The Terrorist Surveillance Program *does not* involve "domestic spying." As the Executive Branch has stated on a number of occasions, the Program targets communications where one party is outside the United States and 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. Under the Program, decisions about what communications to intercept are made by professional intelligence officers at the National Security Agency who are experts on al Qaeda and its tactics, including its use of communication systems. Relying upon the best available intelligence and subject to appropriate and vigorous oversight by the NSA Inspector General and General Counsel, among others, the NSA determines whether one party is outside the United States and whether there are reasonable grounds to believe that at least one of the parties to the communication is a member of al Qaeda or an affiliated terrorist program. Procedures are also in place under the Program to protect U.S. privacy rights, including applicable procedures required by Executive Order 12333 and approved by the Attorney General, which govern acquisition, retention, and dissemination of information relating to United States persons. The NSA takes very seriously the need to protect the privacy of United States persons. S. 2453 provides additional authority to help protect the Nation in a way that also protects privacy interests of Americans.

3b. Is this just another attempt to expand Executive authority even further, or does the Administration have a specific, documented need to spy on far larger numbers of innocent Americans than are at risk under the current program?

ANSWER: (U) The Executive Branch has no need to spy and no interest in spying on any innocent Americans. The NSA supports modernizing FISA to address the threat confronted by the United States and providing additional support for the Terrorist Surveillance Program to protect American lives and to enhance the communications privacy of United States persons. Recent events in Britain remind us that, five years after al Qaeda succeeded in launching the single most deadly foreign attack on American soil in history, we continue to confront a

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00065 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.012

determined and deadly enemy that is dedicated to launching further catastrophic attacks against America. We act at our peril if we do not do everything in our power to detect and prevent such plots. Although FISA remains a vital tool in the War on Terror, the Terrorist Surveillance Program provides an advantage in terms of speed and agility that is critical to successful intelligence collection against a flexible, secretive, diffused, and constantly evolving global network of terrorist cells. The Executive Branch takes very seriously the need to protect Americans from terrorist threats consistent with the protection of civil liberties. To that end, electronic surveillance is conducted in accordance with the law.

3c. What are the Administration's justifications for such a broad program that far exceed the program described publicly by each of you in past statements and in testimony before this Committee?

ANSWER: (U) There is no reason to believe that either S. 2453 or S. 3931 would authorize programs that "far exceed" the Terrorist Surveillance Program in size and scope, since any such program would still have to meet the Fourth Amendment's reasonableness requirement. The Executive Branch takes very seriously the need to protect Americans from terrorist threats consistent with the protection of civil liberties. Electronic surveillance is conducted with Congress's oversight and in accordance with the law.

4. At the July 26, 2006, Senate Judiciary Committee hearing, Mr. Bradbury described the NSA warrantless wiretapping program as "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 affiliate terrorist organization."

Question:

4a. What is the legal definition of an "affiliate terrorist organization"?

ANSWER: (U) Whether a particular group is an "affiliate terrorist organization" of al Qaeda is a factual matter determined by experts in the Intelligence Community.

4b. Who makes the determination that an organization is one that is an "affiliate terrorist organization" to al Qaeda?

ANSWER: (U) Experts in the Intelligence Community, relying upon the best available intelligence information, their expertise, and their judgment, determine which groups are "affiliate terrorist organization[s]" of al Qaeda.

4c. What are the criteria used?

ANSWER: (U) The criteria used to determine whether a group is affiliated with al Qaeda are developed by the Intelligence Community based on the best information available about the characteristics and behavior of terrorist groups.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00066 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.013

4d. How quickly is such a determination made?

ANSWER: (U) The Intelligence Community endeavors to make an accurate decision regarding whether a group is affiliated with al Qaeda as quickly as possible, based upon the best available information.

5. The Intelligence Authorization Act for fiscal year 2000 included a provision requiring a report to Congress from the intelligence community on the legal standards used by agencies in conducting signals intelligence, including electronic surveillance. Congress wisely saw the need to require legal justification from the intelligence community on any program affecting the privacy interests of Americans. The report was submitted before 9/11. In that report, the NSA said, "in order to conduct electronic surveillance against a U.S. person located within the United States, FISA requires the intelligence agency to obtain a court order from the Foreign Intelligence Surveillance Court." We must guarantee the same oversight in any new legislation.

Question:

5a. Will the Administration agree to report on the legal standards being used now? Obviously, the standards provided to Congress in 2000 have become outdated and, perhaps, obsolete.

ANSWER: (U) The Executive Branch has provided the Committee with extensive information regarding the legal standards currently applicable to foreign intelligence surveillance. On January 19, 2006, the Department of Justice released 42-page paper setting forth the legal rationale underlying the Terrorist Surveillance Program and explaining, consistent with the public nature of that document, the standards used in the Program. Since that time, officers of the NSA and the Department of Justice have appeared in numerous public and classified congressional hearings on these legal standards, and have answered hundreds of questions for the record about the Terrorist Surveillance Program. In addition, every member of both of the Intelligence Committees has been authorized to be briefed about the Terrorist Surveillance Program and nearly all have availed themselves of this opportunity.

6. In a White House press briefing on December 19, 2005, General Hayden said that shift supervisors determine individual targets for warrantless wiretapping; in February 2006, General Hayden said that "senior executives" make these decisions.

Questions:

6a. What specific level of government official is making the determination that there is either "reasonableness" or "probable cause" to bring a person into surveillance under this program?

ANSWER: (U) A select group of senior officers at NSA, who are experts on counterterrorism generally and al Qaeda and its communications tactics specifically, are authorized to approve surveillance under the Terrorist Surveillance Program. All authorizations to conduct surveillance under the Program are subject to rigorous oversight by the Office of the Inspector General and

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00067 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.014

the Office of the General Counsel of the NSA, as well as by attorneys from the Department of Justice.

6b. What legal training do these officials have, if any?

ANSWER: (U) Although the NSA personnel making the initial determinations to conduct electronic surveillance do not have formal legal training, the determination itself is premised on the common-sense judgments of reasonable and prudent people. Indeed, the federal Courts have consistently held that the probable cause standard is a practical, nontechnical concept. *See, e.g., Maryland v. Pringle*, 540 U.S. 366, 371 (2003); *Illinois v. Gates*, 462 U.S. 213, 235-36 (1983). Probable cause refers simply to reasonable grounds for a belief that one holds based on the factual and practical considerations of everyday life on which reasonable and prudent persons act. *Pringle*, 540 U.S. at 366.

(U) These officers are an integral part of the rigorous review process NSA has instituted as part of the Terrorist Surveillance Program to protect the privacy of United States persons. Relying upon the best available intelligence and their training and experience regarding counterterrorism, these officers—before ordering the interception of certain international communications—must determine whether there is probable cause ("reasonable grounds") to believe that at least one of the parties to the communication is a member or agent of al Qaeda or an affiliated terrorist organization.

(U) As I have noted previously, the Terrorist Surveillance Program of course is subject to intense legal oversight, within the NSA and by other elements or agencies within the Executive Branch. The oversight process includes review at the National Security Agency (by both the Office of General Counsel and Office of Inspector General) and the Department of Justice.

6c. What are their qualifications to make the decision to target an individual for surveillance on U.S. soil, a decision that is required to be made by a FISA Court judge under existing law?

ANSWER: (U) We disagree with the assertion that "existing law" always requires a judge of the FISC to make the determination whether to authorize foreign intelligence surveillance involving a person within the United States. As set forth in greater detail in the Department of Justice's *Legal Authorities Supporting the Activities of the National Security Agency Described by the President* (Jan. 19, 2006) ("*Legal Authorities*"), the courts have long recognized that the President has inherent authority under the Constitution to conduct electronic surveillance for the purposes of collecting foreign intelligence information without prior judicial approval. Congress has confirmed and supplemented that authority through the September 18, 2001 Authorization for the Use of Military Force ("Force Resolution"). Decisions about what communications to intercept are made by professional intelligence officers who are experts on al Qaeda and its tactics, including its use of communications systems. These experts have years of training and experience in the field of counterterrorism. Relying on the best available intelligence and subject to appropriate and rigorous oversight by the NSA Inspector General and General Counsel, among others, these officers determine whether there is probable cause to believe that one of the parties to a communication is a member or agent of al Qaeda or an affiliated terrorist organization.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00068 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.015

7. At the July 26, 2006, Senate Judiciary Committee hearing, General Hayden said, "[T]he Government looks to four factors in assessing whether or not a court order is required before NSA can lawfully intercept a communication...those factors are: who is the target, where is the target, how do we intercept the communication, and where do we intercept the communication."

Questions:

7a. Who at the NSA assesses each of these four factors? If you are unable to name specific people, what level of government official makes this assessment?

ANSWER: (U) My understanding is that the above-quoted statement from General Hayden's testimony at the July 26 hearing did not in any way concern the Terrorist Surveillance Program. Rather, his statement concerning the 'who, what, where, and how' of intercepting an electronic communication is addressed to the determinations that must be made regarding whether FISA even applies to a particular communication. General Hayden's statement is true generally for all NSA intelligence collection activities, and has been true for the 28 years FISA has been in effect. The four issues must be considered because the manner in which FISA defines the term "electronic surveillance" is in part dependent on factors that those questions address.

(U) While there is no single person whose job it is to assess these factors, the Office of General Counsel provides legal advice to NSA employees, including training specifically concerning the applicability of the FISA, and is available to provide legal advice in a given situation to NSA officials concerning the applicability of the statute. Sometimes it is quite clear to an individual responsible for initiating surveillance that no court order is required under the particular circumstances contemplated, such as when NSA wants to conduct surveillance of a foreign target located overseas using a surveillance technique accomplished entirely overseas. At other times, it is clear that FISA does require a court order, such as when the government seeks to acquire the contents of a wire communication sent by or intended to be received by a particular known U.S. person in the United States by targeting that person.

7b. What legal training do these staff members have, if any?

ANSWER: (U) Please see our responses to questions 6b, 6c, and 7a, above.

7c. What are their qualifications to make this determination?

ANSWER: (U) Please see our responses to questions 6b, 6c, and 7a, above.

8. In response to Senator Specter's question about whether or not it is "impossible or impractical to get an individualized warrant when the caller is outside of the United States, not knowing whether the recipient will be inside the United States," you said, "it would be impractical because we don't know what the foreign to U.S. number could possibly be." However, FISA allows you to begin tapping a source immediately and continuously for up to 72 hours while you pursue a warrant. This can be done entirely at the discretion of the Attorney General, as long as he makes a good-faith effort to "reasonably determine[]" that "an emergency situation

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00069 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.016

exists" and that "the factual basis for the issuance of an order . . . exists." 50 U.S.C. § 1805.

You made the same argument in response to Senator Feinstein's question about obtaining FISA warrants under the current law to execute the NSA surveillance program, arguing that "it would require us to get a FISA on every foreign one in advance because we do not know who they are calling until it has happened," again ignoring the 72-hour grace period under the current law.

Questions:

8a. Given that current law allows for the 72-hour grace period for obtaining a warrant, why would you have to get those warrants "in advance"? Would you clarify your answer to Senator Feinstein's question?

ANSWER: (U) Thank you for the opportunity to correct a common misperception about FISA. The emergency authorization provision in FISA, which allows 72 hours of surveillance without obtaining a court order, does not—as many believe—allow the Government to undertake surveillance immediately. Rather, in order to authorize emergency surveillance under FISA, the Attorney General first must personally "determine[] that . . . the factual basis for issuance of an order under [FISA] to approve such surveillance exists." 50 U.S.C. § 1805(f). For surveillance requested by NSA, that process ordinarily entails review by intelligence officers at the NSA, NSA attorneys, and Department of Justice attorneys, each of whom must be satisfied that the standards have been met before the matter proceeds to the next group for review. In addition, if the Attorney General authorizes emergency surveillance and the FISA court later declines to permit surveillance, the surveillance must cease 72 hours after its initial authorization, and there is a risk that the court would disclose the surveillance publicly. *See id.* § 1806(j). To meet the statutory requirements and to reduce those risks, the Attorney General must ensure that any "emergency" surveillance ultimately will be acceptable to the FISA court, in essence requiring the Attorney General to be certain in advance that the FISC would grant a warrant before even initiating emergency surveillance.

8b. If the problem with the current law is an inability for the NSA to process the required number of FISA petitions within the 72-hour window, why not simply amend the statute to extend the grace period? If the grace period were extended to a month, or three months, the NSA could discard useless information and use the ample extra time to apply for warrants to cover any useful information. Why do we need the Chairman's sweeping overhaul if the actual problem can be solved in a targeted manner?

ANSWER: (U) NSA supports extending the period that surveillance can be conducted before obtaining an order from the FISC, but that alone would not be sufficient to enable the United States to collect foreign intelligence from an agile and flexible enemy. As noted above, modernization of FISA and provisions dealing with programmatic orders are needed to help us detect and to prevent future terrorist attacks by al Qaeda and its affiliates as well as to counter other foreign threats.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00070 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.017

8c. If the concern is about the time that it takes for the Attorney General to approve wiretapping under the emergency 72-hour provision, why does it take longer to meet the requirements of FISA ("reasonably determin[ing] that "an emergency situation exists" and that "the factual basis for the issuance of an order…exists") than the Administration's standard for the warrantless wiretapping program ("a communication we believe to be affiliated with al Qaeda, associated with al Qaeda, one end of which is in the United States, and we believe at least one end we have a probable cause standard is al Qaeda")? Could this problem be solved by delegating this responsibility to specified senior officials with legal proficiency in these matters? Or the allocation of additional resources to the FISA Court or the relevant federal agencies gathering intelligence?

ANSWER: (U) By itself, amending FISA to permit a senior official other than the Attorney General to authorize an emergency wiretap would not make FISA suitable to provide the sort of early warning system necessary. Under such a proposal, it would still be necessary for the official first to personally "determine[] that . . . the factual basis for issuance of an order under [FISA] to approve such surveillance exists." 50 U.S.C. § 1805(f). Because the failure to obtain a court order within 72 hours authorizing the interception would result in the surveillance being stopped and would risk its disclosure, the Executive Branch would still need to follow the existing multi-layered review procedure before any such official would authorize "emergency" surveillance. Under FISA, each statutory requirement must be included in each application to ensure the application is approved. For example, the statute requires that each application contain a statement of facts supporting the application, a certification from a high-ranking official with national security responsibilities, and the signature of the Attorney General. FISA applications are sometimes an inch thick. This proposal would still present the Executive Branch with a bottleneck prior to authorization, and would do nothing to alleviate the bottleneck at the application stage.

(U) For these and other reasons, committing even substantial additional resources within the traditional FISA framework for obtaining orders—while welcome—would not provide the flexibility and agility necessary to allow it to function as an early warning system against attacks by al Qaeda and affiliated terrorist organizations. There are several problems with traditional FISA procedures that cannot be solved simply by allocating additional money to foreign intelligence collection. First, these traditional procedures require individual applications for each target. *See* 50 U.S.C. §§ 1804 & 1805. Second, the tremendous changes in global telecommunications technology since 1978 have resulted in the unintended expansion of the reach of FISA to include international communications that Congress intended to exclude from the scope of the statute. This unintended expansion of FISA's scope requires the Government and the FISC to devote considerable resources to surveillance that Congress intended not to regulate through FISA. Third, section 104 of FISA, 50 U.S.C. § 1804, currently requires certifications from high-level national security officials and personal approval by the Attorney General of all applications to the Foreign Intelligence Surveillance Court, thus creating "bottlenecks" in the application process that cannot be eliminated simply by appropriating additional funds to foreign intelligence surveillance.

9. The procedures required by FISA are often blamed for the Administration's difficulties in predicting and responding to 9/11. However, as has been widely reported, the NSA

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00071 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.018

intercepted statements on September 10th referring to the September 11th attacks, but these warnings were not translated until September 12th—too late to provide any warning of the devastation planned for New York and Washington, DC. In the five years since September 11th, the media has continued to report that intelligence agencies, including the NSA, do not have the ability to keep up with the translation demands of the war on terror. At the Senate Judiciary Committee hearing on July 26, 2006, General Hayden acknowledged the translation backlogs and concerns about allocating resources.

Questions:

9a. What are you and others at the NSA doing to hire more translators of Arabic and other languages that are critical to fighting terrorism?

ANSWER: (U) The Global War on Terror and continuing military campaigns have placed an enormous burden on NSA's population of civilian and military language and intelligence analysts. Supplemental funding has helped to expand the contract linguist population in several low-density crisis languages, increase analytic training across the extended SIGINT enterprise, immediately activate a civilian Cryptologic Reserve Program, and significantly expand the Military Reserve program. The Agency continues to need skilled linguists and analysts, and is aggressively pursuing qualified applicants.

9b. Is there currently a backlog in translating intelligence information? If so, what is the average amount of time between an interception that takes place under surveillance and its translation? Do you have a system in place to prioritize translation of critical information? If so, how do you determine which intelligence is more important than other information?

ANSWER: (U) Depending on the source of the information there could be time lags between when it was intercepted and when it was available for a linguist to review at NSA Headquarters. Given the wide differences in targets and the methods of communicating, we cannot give an estimate of an average time lag.

(U) Although we have made significant progress in addressing the problems identified in 2001, the translation backlog is a systemic issue. Terrorist lead information has proliferated since 2001 and, unfortunately, it is a very labor intensive exercise to sift through large volumes of foreign language data and painstakingly attempt to separate the wheat from the chaff. This dilemma is compounded by the fact that the target set has expanded exponentially since 2001 in terms of geographic reach and languages used. Today's backlog is no longer confined to Arabic and its multiple dialects, but also includes a variety of other less commonly taught languages, where linguists eligible for security clearances are in short supply.

9c. If there is a backlog in translation, how does this affect your ability to protect America from future terrorist attacks?

ANSWER: (U) It is important to bear in mind that SIGINT is only one component of America's defense and, given the vague and fragmentary nature of terrorist communications, it is more likely that a combination of intelligence sources will be necessary to prevent a terrorist attack. What SIGINT can do is work hand-in-glove with other intelligence agencies, the military, and

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00072 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.019

law enforcement to enable key takedowns, so that the details of a plot can be uncovered through interrogation and forensics exploitation. That being said, the translation backlog can prevent the timely delivery of key information to NSA's customers and stall development efforts against new targets.

9d. What resources are required for the NSA to increase its translation efficiency to a level at which translation will not be an impediment to protecting America?

ANSWER: (U) NSA must have a robust hiring and contracting program for GWOT languages, with a particular focus on the identification and recruitment of high-caliber, clearable native speakers, and the agility to adapt to the constantly-changing needs of the terrorist target set. NSA will also need better analytic methods, which we call "Human Language Tools," to help focus efforts on the most lucrative leads, given that it will never be possible to fully exploit all of the material that we have the capacity to collect. Finally, NSA needs a high-quality GWOT language training program to help our current linguists acquire the necessary skills to address this challenging target set.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00073 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.020

Senator Dick Durbin
FISA for the 21st Century
Wednesday, July 26, 2006
Questions for Lt. General Keith B. Alexander

1. It is interesting that 4 ½ pages of your 5-page written statement focus on the Specter bill's change in the definition of electronic surveillance. You clearly believe it is important to make this change in the law to facilitate effective surveillance of terrorists.

   When did you become aware of the problem with current law? Do you know why the administration has not previously asked Congress to change the definition of electronic surveillance?

ANSWER: (U) It has long been known that FISA's existing definition of "electronic surveillance" is obsolete and that changes in technology inadvertently are sweeping within the scope of FISA electronic communications that Congress in 1978 had intended to exclude. It was our judgment, however, that disclosing that fact to explain the need to reform the definition of "electronic surveillance" could disclose sensitive intelligence sources and methods. Such disclosures would have posed a serious risk to national security. Numerous unauthorized and harmful disclosures of intelligence activities, including the public disclosure of the Terrorist Surveillance Program, have reduced the risk of additional damage to national security from seeking to amend FISA to solve the inadvertent expansion in FISA's scope since 1978.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00074 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.021

Senator Russell D. Feingold
FISA for the 21st Century"
Wednesday, July 26, 2006
Questions for Lt. General Keith B. Alexander

Following are questions regarding the July 25, 2006, version (marked "JEN06974") of Senator Specter's bill, which was originally introduced as S. 2453[2]. Please respond to the greatest degree possible in an unclassified setting, and please endeavor to provide any classified answers at a clearance level that will allow at least some cleared Judiciary Committee staff to review the responses.

1. The Specter bill makes a number of changes to the existing FISA statute. In reviewing these changes to the statute, it would of course be helpful to know how the FISA court has interpreted it. Please provide copies of any FISA court decisions containing legal interpretations of provisions of FISA that are amended by the Specter bill.

ANSWER: (U) NSA is not in a position to provide these documents because NSA does not control them. In any event, the orders issued by the Foreign Intelligence Surveillance Court are classified documents that are not publicly available. Consistent with long-standing practice, however, the Executive Branch notifies Congress concerning the classified intelligence activities of the United States through appropriate briefings of the respective Intelligence Committees of the Senate and the House of Representatives. Furthermore, in the only case it has ever heard, the Foreign Intelligence Surveillance Court of Review published a redacted version of its decision that did not reveal intelligence sources and methods. *See In re Sealed Case*, 310 F.3d 717 (For. Intel. Surv. Ct. Rev. 2002).

2. At the hearing, General Hayden stated that Section 9 of the Specter bill originated at the NSA. Please explain with regard to each subsection of the Specter bill, including each subsection of Section 9, the degree to which you or anyone at your agency/department had input on it, and to the extent not addressed in the answers to the questions below, whether you support it.

ANSWER: (U) Because of the interactive and cooperative nature of the legislative process, it is not possible to say definitively on which subsections of the bill NSA had substantive input. In response to requests from several Members, NSA provided technical drafting assistance that Congress was free to accept or reject.

3. The Specter bill creates a new Title VII of FISA. Under this title, the FISA court would be granted the authority to issue program warrants. Under the bill, would the government

[2] As noted previously, *supra* n.1, the proposed language of S. 2453 (marked JEN06974) continues to be modified. At present, the Senate's FISA modernization proposal that most closely resembles S. 2453 is S. 3931, the Terrorist Surveillance Act of 2006, as introduced. In most cases, the answers provided herein are responsive to the questions that remain relevant in S. 3931; i.e., where the language in S. 3931 does not substantively change the context of the question. A note has been made to indicate those questions where the significant changes in S. 3931 make the question inapplicable.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00075 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.022

ever be required by the statute to seek a warrant from the FISA court to engage in an existing or future electronic surveillance program?

ANSWER: (U) S. 2453 has undergone significant changes that affect this question. Nevertheless, Senator Specter's legislation would not require the Executive Branch to submit an electronic surveillance program to the FISC.

4. Please explain your understanding of the interplay in the new Title VII of FISA created by the Specter bill of the section 701 definitions of "electronic communication," "electronic tracking," and "electronic surveillance program." Also explain how those definitions vary from the definition of "electronic surveillance" in existing FISA Title I.

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

5. In the Specter bill, the newly inserted section 701(6) defines "foreign intelligence information" as having the same meaning as the current statute, but also adds "and includes information necessary to protect against international terrorism." Given the definitions already in the FISA statute, isn't this additional language just duplicative?

ANSWER: (U) NSA continues to evaluate these provisions. Because "foreign intelligence information" is broader and encompasses terrorism, the reference to terrorism merely adds emphasis and does no harm.

6. The current FISA statute defines "contents" as "any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication." The Specter bill, in creating the new Title VII, uses the term "substance" rather than "contents." It defines "substance" as "any information concerning the symbols, sounds, words, purport, or meaning of a communication, and does not include dialing, routing, addressing, or signaling." Please discuss whether you believe this alternate definition is necessary and if so, why. Please also discuss how you believe this alternate definition varies from the new definition of "contents" that Section 9 of the Specter bill would create in the existing FISA Title I.

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

7. In the Specter bill's new section 702, the FISA Court is given jurisdiction to issue an order authorizing an electronic surveillance program "to obtain foreign intelligence information or to protect against international terrorism." The Administration has publicly described the NSA program as involving communications where there is a reasonable basis to believe that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda.
    a. Do you agree that the bill authorizes program warrants "to obtain foreign intelligence information" even when there is no connection to al Qaeda, and that this is broader even than what the President has stated he has authorized?

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00076 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.023

ANSWER: (U) Yes. The bill authorizes court orders "to obtain foreign intelligence information" even when there is no connection to al Qaeda. The bill provides flexibility beyond the al Qaeda threat.

b. Do you agree that the bill authorizes program warrants "to obtain foreign intelligence information" even when there is no connection to terrorism, and that this is broader even than what the President has stated he has authorized?

ANSWER: (U) Yes. The bill authorizes court orders "to obtain foreign intelligence information" as that term is defined in FISA.

8. In the Specter bill's new section 702, the FISA Court's initial authorization of an "electronic surveillance program" cannot be for longer than 90 days, but a re-authorization can be for as long as the court determines is "reasonable." What do you believe is the justification, if any, for not limiting reauthorization to 90 days?

ANSWER: (U) An initial authorization of 90 days would be appropriate in order to enable the Foreign Intelligence Surveillance Court to review the actual initial operation of the program, particularly the functioning of its minimization procedures. Mandating further review every 90 days thereafter, however, would be unnecessary and inefficient, and would undermine the flexibility and agility that is necessary to conduct effective foreign intelligence surveillance. After the FISC has had the opportunity to see a program in operation for a period, it may reasonably conclude that the protections in place are sufficient that reauthorization every 90 days is unnecessary. Rather than impose an artificial limit upon reauthorizations, proposed section 702(a)(2) in S. 3931 would grant to the experienced Article III judges of the FISC the authority to reauthorize an electronic surveillance program for a "reasonable" period of time.

9. The Specter bill's new section 702(b) establishes guidelines for mandatory transfers of cases to the FISA Court of Review, and refers to "any case before any court." Do you believe that these mandatory transfer provisions would apply to pending cases?

ANSWER: (U) NSA is not in a position to answer this question. We defer to the answer of the Department of Justice on this question.

10. In the Specter bill's new section 702(b), the mandatory transfer provision applies to any case "challenging the legality of classified communications intelligence activity relating to a foreign threat, including an electronic surveillance program, or in which the legality of any such activity or program is in issue." "Electronic surveillance program" is defined in the bill, but there is no definition in the current FISA statute or in the Specter bill of a "classified communications intelligence activity." What do you read this term to mean, and what types of cases beyond those involving "electronic surveillance programs" do you believe would be covered by this term?

ANSWER: (U) Given the highly classified nature of the intelligence activities of the United States, it would be inappropriate to attempt in this setting to describe specifically those activities

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00077 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.024

that would fall within the scope of the term "classified communications intelligence activities." At a minimum, NSA believes the term "classified communications activity" refers to NSA's activities authorized under Executive Order 12333. The definition of an "electronic surveillance program" in S. 3931 is more limited in scope.

11. In the Specter bill's new section 702(b), the mandatory transfer provision, cases are transferred to the FISA Court of Review "for further proceedings under this subsection." But, there is no subsection defining the procedures for the FISA Court of Review's "further proceedings," as there was in prior versions of the bill.
    a. Did you or anyone at your agency/department request or suggest that the paragraph in earlier versions of the bill entitled "Procedures for Review" be removed? If so, why?

ANSWER: (U) No.

    b. As you read this subsection, what relief would the FISA Court of Review have the authority to grant if it found that the program at issue were illegal?

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

    c. As you read this subsection, what role would the parties challenging the program play in the FISA Court of Review proceedings?

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

12. The Specter bill's new section 702(b)(3) preserves "all litigation privileges" for any case transferred to the FISA Court of Review.
    a. Do you read this as being intended to cover the state secret privilege?
    b. If so, has the state secrets privilege ever before been invoked in the FISA court? Why would it be necessary to invoke the state secrets privilege in a court that operates in a one-sided, secret process?

ANSWER: (U) This section has undergone significant changes in S. 3931. These questions are no longer applicable. Furthermore, NSA is not in a position to answer these questions. We defer to the views of the Department of Justice on these questions.

13. The Specter bill repeals sections 111, 309, and 404 of the FISA statute, which, notwithstanding any other law, give the President the authority to use electronic surveillance, physical searches, or pen registers or trap and trace devices without a court order for up to fifteen days following a declaration of war by Congress. Does the Administration support this repeal of these provisions, which on their face appear to grant additional surveillance options to the executive branch in time of war? If so, why?

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00078 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.025

ANSWER: (U) As explained in the Department of Justice's *Legal Authorities Supporting the Activities of the National Security Agency Described by the President* (*"Legal Authorities"*) at 6-10 (Jan. 19, 2006), section 111 of FISA (and parallel sections 309 and 404) does not specify the manner in which the President must proceed after the expiration of the 15-day period, nor does it address armed conflicts in which there is no formal declaration of war. We believe, however, that Congress understood that subsequent legislation, including legislation such as the Authorization for Use of Military Force, could authorize electronic surveillance outside traditional FISA procedures. *See Legal Authorities at* 2-3, 20 (stating that 50 U.S.C. § 1809(a)(1) contemplates that Congress could authorize electronic surveillance through another statute, such as the AUMF); 50 U.S.C. § 1809(a)(1) (prohibiting any person from intentionally "engage[ing] . . . in electronic surveillance under color of law except as authorized by statute").

14. The Specter bill, in section 8(c)(2)(A)(i), inserts "or under the Constitution" in 50 U.S.C. § 1809(a)(1). What is the effect of this amendment to section 1809?

ANSWER: (U) This section has undergone significant changes in S. 3931, and this specific question is no longer applicable. Nevertheless, the general purpose of inserting such language is to avoid an unnecessary constitutional conflict regarding whether the FISA unconstitutionally interferes with the authority of the President to conduct electronic surveillance without prior judicial approval for the purpose of collecting foreign intelligence information during an ongoing armed conflict. A statute (such as FISA), of course, cannot eliminate the President's constitutional authority to conduct surveillance of a foreign enemy without prior judicial approval. *See, e.g.*, *In re Sealed Case*, 310 F.3d 717, 742 (For. Intel. Surv. Ct. Rev. 2002). Accordingly, revising 50 U.S.C. § 1809(a)(1) to make clear that the conduct of foreign intelligence surveillance pursuant to *either* the FISA *or* the Constitution is not unlawful would clarify that FISA should not be construed to infringe on the constitutional authority of the President to conduct surveillance of a foreign enemy during an armed conflict without prior judicial approval.

15. The Specter bill, in section 8(c)(2)(A)(iii), adds a third category of criminal activity to 50 U.S.C. § 1809(a). This third category is similar to the second category, 1809(a)(2).
    a. Please explain your view of the difference between the language of the new 1809(a)(3), "knowingly discloses or uses information obtained under color of law by electronic surveillance ..."; and the language of the existing 1809(a)(2), "discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance ..."
    b. Second, the new 1809(a)(3) would add the phrase "in a manner or for a purpose" prior to "authorized." Do you agree with this added language, and if so, why?
    c. Third, it ends with the phrase "authorized by law," rather than "authorized by statute" as 1809(a)(2) does, or "authorized by statute or under the Constitution," as the bill would amend 1809(a)(2) to read. Please explain the reason, if any, for not adopting the same phrase as in 1809(a)(2), either in current law or as it would be amended by the bill.

ANSWER: (U) NSA is not in a position to answer this question.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00079 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.026

16. The Specter bill, in section 8(c)(2)(B), increases the penalties of violating 50 U.S.C. 1809's criminal prohibitions, both in amount of maximum fines ($10,000 to $100,000) and maximum prison term (five years to fifteen years). Do you support these changes? If so, why do you believe they are justified?

ANSWER: (U) NSA is not in a position to answer this question.

17. The Specter bill, in section 9(b)(1), inserts an additional category into the current FISA statute's definition of a non-U.S. person "agent of a foreign power" – someone who "possesses or is expected to transmit or receive foreign intelligence information within the United States." Given that section 1801(b)(1)(C) of FISA already includes any non-U.S. person engaged in "activities in preparation" of international terrorism, do you believe this added language is necessary? If so, why?

ANSWER: (U) Yes, we believe the added language is necessary. This change to FISA is not meant to deal only with terrorism, but with a problem that affects NSA's ability to collect foreign intelligence from non-U.S. persons while they are inside the United States for a limited amount of time. Specific examples could be provided in a classified setting, but the problem may be described in general terms as follows. On numerous occasions, non-U.S. persons come to the United States and either have in their possession or are anticipated to access from within the United States foreign intelligence information that is of vital interest to the United States Government. However, if an individual is not currently an "officer or employee" of a foreign power, or a spy, terrorist or saboteur (or someone who aids or abets someone engaging in espionage, terrorism, or sabotage), the FISC does not have jurisdiction to authorize either physical searches or electronic surveillance directed at that individual. It is important to note that the proposal would not allow intelligence agencies to direct searches or surveillances against visitors to the United States at their discretion. It would merely afford them an opportunity to ask the FISC to authorize the surveillance or search of a non-U.S. person within the United States where a certifying official deems the foreign intelligence information to be significant. Currently, because FISC authorization is not available, intelligence agencies can only seek to obtain the foreign intelligence held or available to such individuals while they are outside the United States. Operating outside the United States puts intelligence gatherers at risk of exposure, imprisonment, or execution.

18. The Specter bill [see footnote 2], in section 9(b)(2), modifies section 1801(f) of FISA, defining "electronic surveillance." The opening language of the definition in 1801(f)(1) – "the acquisition by an electronic, mechanical or other surveillance device" – is replaced with "the installation or use of an electronic, mechanical or other surveillance device." Please explain the effect you think this would have on the FISA process, and any reason you see for the change in definitional language.

ANSWER: (U) The current definitions of "electronic surveillance" in FISA are related to two very different things. The first three definitions apply only to the "acquisition" of communications. The fourth definition is broader, encompassing the installation or use of surveillance devices to acquire not only communications (other than those passed by wire or

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00080 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.027

radio) but also any other "monitoring to acquire information." Sometimes, it is only the installation of a surveillance device that may require a court order, while the use does not. For this reason, it was necessary to use "installation or use" from the current fourth definition, rather than "acquisition," which is used in the first three, if the statute is to govern the full spectrum of surveillance activities directed at persons within the United States.

19. The Specter bill [see footnote 2], in section 9(b)(2), modifies section 1801(f) of FISA, defining "electronic surveillance." The new section 1801(f)(1) would cover only the "intentional collection of information." No such limitation exists in the current 1801(f)(1). Please explain what you think would be the effect of this new limitation.

ANSWER: (U) The current definition in section 1801(f)(1) governs only the acquisition of communications through "intentionally targeting that United States person." The use of "intentional collection of information" is designed to replicate this limitation. The current definition in section 1801(f)(1) does not prohibit the incidental acquisition of communications of a United States person within the United States when someone else (e.g. a non-U.S. person outside the United States) is being targeted. Neither should the new definition.

20. The Specter bill [see footnote 2], in section 9(b)(2), modifies section 1801(f) of FISA, defining "electronic surveillance." The current language in 1801(f)(1) refers to a person "who is in the United States" while the new language refers to a person "who is reasonably believed to be in the United States." Please explain what you think would be the effect of this new language.

ANSWER: (U) The proposed change to section 1801(f)(1) would recognize that many of the forms of electronic communication that have come into existence since 1978 are much more portable and present the possibility of targeting someone in an unexpected location. In 1978, NSA reliably could associate a phone number with an area code in a European capital with a telephone physically located in that city. Now, telephone area codes are less reliable indicators of the physical location of their users, with the option to purchase phones with any area code that one desires as well as the growth of roaming agreements that allow portable phones to function around the globe. In addition, even newer services like webmail may be used anywhere in the world that an account user has access to the Internet. In accordance with FISA's overarching purpose of regulating the collection of foreign intelligence information from United States persons within the borders of the United States, we believe that an order permitting electronic surveillance should be required only where the Government reasonably believes a target is physically in the United States. Under the proposed definition, once an intelligence agency has a reasonable belief that a target has entered the United States, the Government would be obligated to seek authorization for electronic surveillance to continue so long as the target is inside the United States.

21. The Specter bill [see footnote 2], in section 9(b)(2), modifies section 1801(f) of FISA, defining "electronic surveillance." It would limit the definition in 1801(f)(1) to "the intentional collection of information concerning a particular known person . . . by intentionally targeting that person . . . ." In contrast, the current language of 1801(f)(1) covers the "acquisition . . . of the contents of any . . . communication sent by or intended to

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00081 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.028

be received by" a particular person who is intentionally targeted. Would this change in the definition mean that if the government targeted an individual to obtain information about someone other than that person, that it would fall outside the definition of "electronic surveillance"? Please explain your view of the effect of this change to the definition.

ANSWER: (U) The first definition of "electronic surveillance" in the current law applies only when the contents of communications are obtained by intentionally targeting someone in the United States. NSA would regard any targeting directed at someone within the United States as constituting intentional targeting of the communications of that person. NSA does not believe that the proposed language would permit it to target someone who was within the United States merely because it could identify an interest in someone else or any other purpose. NSA does not believe that it can nominally "target" foreigners outside the United States without an order from the FISC if the purpose of the collection is to obtain the communications of someone inside the United States with a foreign target.

22. The Specter bill [see footnote 2], in section 9(b)(2), modifies section 1801 of FISA defining "electronic surveillance." It creates a two-part definition of "electronic surveillance," in which the second half of the definition covers "any communication" where "both the sender and all intended recipients are in the United States." In all four parts of the current FISA definition, the phrase "by an electronic, mechanical, or other surveillance device" is used. The second part of the definition in the Specter bill does not use this language. Please explain your view of the legal effect of this omission.

ANSWER: (U) As NSA understands it, the purpose of the definition governing the acquisition of domestic communications was to forestall concerns that because the first definition of surveillance only affected surveillance directed at a particular person within the US, it would allow NSA to target large amounts of domestic communications without targeting any one person and thereby avoid triggering the requirement for an order. NSA does not believe the omission of the phrase "by an electronic, mechanical or other surveillance device" has any negative substantive effect, because it believes that acquisition of domestic communications "under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes" will always be accomplished through the installation or use of some surveillance device. If anything, the absence of this phrase actually acts to broaden the application of the definition, so that acquisition of the information by any means "under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes" would be covered by its terms.

23. The Specter bill [see footnote 2], in section 9(b)(3), modifies section 1801 of FISA defining "Attorney General" to include "a person or persons designated by the Attorney General or Acting Attorney General." What limit would there be on the ability of the Attorney General to designate individuals, including employees of agencies/departments other than the Justice Department, as "Attorney General" for purposes of FISA? To the degree that your answer references regulations, could the Attorney General amend those regulations without congressional approval?

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00082 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.029

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

24. The Specter bill [see footnote 2], in section 9(b)(4)(C), modifies the FISA definition of "minimization procedures" by striking 50 U.S.C. § 1801(h)(4), which requires that any contents of communications to which a U.S. person is a party shall not be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a FISA court order is obtained or the Attorney General determines the information indicates a threat of death or serious bodily harm to any person. Please discuss what you believe are the advantages of entirely eliminating 1801(h)(4) from the current FISA statute.

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

25. The current FISA statute, in section 1801(n), defines the covered "contents" of communication as: "when used with respect to a communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication." The Specter bill [see footnote 2], in section 9(b)(5), replaces the definition of "contents" with the definition contained in 18 U.S.C. § 2510(8) – "when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication."
    a. The new definition does not cover "any information concerning the identity of the parties to such communication." Please discuss what you believe is the effect of this proposed change.
    b. The new definition does not cover "any information concerning…the existence…of that communication." Please discuss what you believe is the effect of this proposed change.

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

26. The Specter bill [see footnote 2], in section 9(c), makes a number of changes to section 1802 of FISA. Section 1802(a)(1) authorizes the President to engage in electronic surveillance without court order for up to one year in certain limited circumstances "under this subchapter." The Specter bill modifies this phrase to "under this title." In your opinion, what effect would this change have?

ANSWER: (U) We believe this provision would have no substantive effect.

27. The Specter bill [see footnote 2], in section 9(c), makes a number of changes to section 1802 of FISA. The current section 1802 requires the Attorney General to certify that "the electronic surveillance is solely directed at" the acquisition of certain covered communications. The Specter bill strikes the "solely directed at" phrase. Given this modification, what showing about the surveillance do you believe the Attorney General would have to make to meet the requirements of this provision? Please explain whether you support this change, and if so, why.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00083 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.030

ANSWER: (U) NSA supports the change but does not believe it is essential. We note that this provision has been modified significantly in S.3931, in a manner that scales back the provision with which you were concerned.

28. The Specter bill [see footnote 2], in section 9(c), makes a number of changes to section 1802 of FISA, which permits electronic surveillance without a court order in certain limited circumstances. The language of 1802(a)(1)(A)(i) currently requires a showing that the communications being pursued are "communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801(a)(1), (2), or (3) of this title." The Specter bill, in contrast, would require only that the communications being pursued were "communications of foreign powers, as defined in section 101(a), an agent of a foreign power as defined in section 101(b)(1)." This is a significant expansion of section 1802's exemption from the usual FISA court order requirement.
    a. Do you support this modified language of section 1802? If so, please discuss the justification for eliminating the limiting language that requires the means of communications be "used exclusively between or among foreign powers."
    b. If you do support the modified language of section 1802, please explain the justification for expanding the "foreign powers" covered by this blanket exemption from those defined in 1801(a)(1)-(3) to all "foreign powers."
    c. If you do support the modified language of section 1802, please explain the justification for adding non-U.S. person agents of foreign powers to this blanket exemption.
    d. In combination with the change to the definition of "agent of foreign power" elsewhere in the bill, wouldn't this mean that the government could wiretap without a warrant the calls of any non-U.S. person in the United States who possessed or was expected to transmit or receive "information with respect to a foreign power or foreign territory that relates to … the conduct of the foreign affairs of the United States"? Wouldn't this be a very broad category covering foreign nationals who have nothing to do with terrorism and no intent to harm the United States in any way?

ANSWER: (U) This section has undergone significant changes in S. 3931. As noted above, these changes have scaled back the scope of the proposed provision. This question is no longer applicable.

29. The Specter bill [see footnote 2], in section 9(c), makes a number of changes to section 1802 of FISA, which permits electronic surveillance without a court order in certain limited circumstances. The Specter bill strikes the requirement of 1802 that the Attorney General certify that "there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party." Please discuss your view of the justification, if any, for repealing this requirement.

ANSWER: (U) The bill would allow the Attorney General to authorize surveillance against these foreign powers as well as non-U.S. persons within the United States without the

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00084 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.031

requirement that the surveillance be limited to communications exclusively used by such individuals. The intent of these changes is to reflect how intelligence agencies currently handle communications to, from, or about U.S. persons when they are acquired by other means, such as when NSA intercepts communications of U.S. persons in contact with foreign powers overseas. Intelligence agencies acting pursuant to Attorney General certification would handle any U.S. person communications in accordance with approved minimization procedures.

30. The Specter bill [see footnote 2], in section 9(c), makes a number of changes to section 1802 of FISA. In creating a new 1802(b), the Specter bill creates a completely new category of Attorney General authority – that as long as the Attorney General certifies that given information, facilities or technical assistance does not fall within the definition "electronic surveillance," the Attorney General can require any electronic communications service, landlord, custodian or other person to furnish such information, facilities, or technical assistance. Please discuss what you consider to be the advantages, if any, of this new provision.

ANSWER: (U) The new provision allows the Intelligence Community, through the Attorney General, to obtain the assistance described. In addition, it provides the service providers with the necessary legal protection from liability claims that may result from the assistance they provide pursuant to lawful Government requests.

31. The Specter bill [see footnote 2], in section 9(c), makes a number of changes to section 1802 of FISA. The Specter bill creates a new 1802(c), which is similar to the language of the current FISA section 1802(a)(4) that permits the Attorney General to order carriers to provide assistance to implement section 1802 and allows them to be compensated.
    a. The current 1802(a)(4) only applies to "electronic surveillance authorized by this subsection." The new 1802(c) would apply to "electronic surveillance or the furnishing of any information, facilities, or technical assistance authorized by this section." Please discuss your view of the effect of the difference between these two formulations.
    b. The current 1802(a)(4) also only applies to a "specified communication common carrier." The new 1802(c) applies to "any electronic communication service, landlord, custodian or other person (including any officer, employee, agent, or other specified person thereof) who has access to electronic communications, either as they are transmitted or while they are stored or equipment that is being or may be used to transmit or store such communications." Do you agree with this change? If so, please discuss why you believe that this wider scope is needed.

ANSWER: (U) This section has undergone significant changes in S. 3931. Nevertheless, the new formulation is necessary to achieve the goal discussed in the answer to the previous question. The change indicated in part b, or something like it, is necessary to update FISA.

32. The Specter bill [see footnote 2], in section 9(c), creates a new section 1802(d), which reads: "Electronic surveillance directed solely at the collection of international radio communications of diplomatically immune persons in the United States may be authorized by an official authorized by the President to engage in electronic surveillance for foreign

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00085 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.032

intelligence purposes in accordance with procedures approved by the Attorney General." Please discuss whether you believe this added authorization is necessary, and if so, why.

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

33. The Specter bill [see footnote 2], in section 9(e), would strike requirements (6), (8), (9) and (11) from the section 1804(a) of FISA, the provision that lays out the required components of FISA applications for electronic surveillance.
    a. Please discuss whether you believe these changes are necessary, and if so, why.
    b. Do you believe that the information required in these paragraphs was not helpful to the FISA court?

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

34. The Specter bill [see footnote 2], in section 9(f)(4), would substantially modify section 1805(e)(1) of FISA, which sets the time limits for a FISA surveillance order. Under current law, FISA surveillance can be authorized for at most ninety days; except that for a non-U.S. person agent of a foreign power, it can be 120 days at most; and for surveillance of certain types of foreign powers, a year at most. The Specter bill replaces these three tiers with a single time limit – a maximum limit of a court order of surveillance for one year – even for U.S. persons.
    a. Please discuss whether you believe this change is necessary, and if so, why.
    b. Please explain your understanding of what is intended by the second sentence of the new 1805(e)(1) that would be created by the Specter bill: "If such emergency employment of electronic surveillance is authorized, the official authorizing the emergency employment of electronic surveillance shall require that the minimization procedures required by this title for the issuance of a judicial order be followed."

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

35. The Specter bill [see footnote 2], in section 9(g), modifies section 1806(i) of FISA, which requires the destruction of certain communications contents that were unintentionally acquired unless the Attorney General determines they indicate a threat of death or serious bodily harm to any person. The amendment would allow the Attorney General to retain any unintentionally acquired communications contents that he determines contains "significant foreign intelligence."
    a. Please discuss whether you believe this change is necessary, and if so, why.
    b. In making this determination, what procedures do you believe the law would require the Attorney General to undertake?

ANSWER: (U) This section would only apply to the inadvertent interception of domestic communications transmitted by any means (not just radio communications, if the statute

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00086 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.033

becomes "technology neutral"). We believe this change is necessary because the current standard is extraordinarily high and could require the destruction of extremely valuable intelligence. As an example, in the course of collecting international communications, NSA might inadvertently intercept a domestic communication in which it is revealed that a spy for a foreign nation has slipped into the United States undetected. Under such circumstances, the statute may require destruction of the information unless the Attorney General determines that this information indicated a "threat of death or serious bodily harm to any person." Requiring that the Attorney General make a specific determination that the information was "significant foreign intelligence" is a reasonable alternative.

36. The Specter bill, in section 9(i), strikes section 1809(a) of the current FISA and replaces it with new language. But the Specter bill, in section 8(c), makes different line-by-line amendments to section 1809(a) of the FISA statute. Do you agree that these two provisions of the proposed legislation are inconsistent and cannot both become law? Of the two provisions, which do you support and why?

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

37. The Specter bill, in section 9(k), modifies section 1827 of FISA by expanding the exception to the criminal prohibition of warrantless physical searches in section 1827(a)(1) to include "except as authorized…under the Constitution." What authority to do warrantless physical searches do you believe is granted "under the Constitution"? Also please discuss whether you believe this change is necessary, and if so, why.

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

38. The Specter bill, in section 9(k), modifies section 1827(a)(2) of FISA by omitting the phrase – "for the purpose of obtaining intelligence information." Please discuss whether you believe this change is necessary, and if so, why.

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00087 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.034

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

September 19, 2007

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

Please find enclosed responses to questions arising from the appearance of Acting Assistant Attorney General Steven G. Bradbury before the Committee on July 26, 2006, at a hearing entitled "FISA for the 21st Century." We apologize for the delay in responding.

The attached responses do not reflect recent changes to the Foreign Intelligence Surveillance Act of 1978 (FISA) resulting from the passage of S.1927, the "Protect America Act of 2007." Based on discussions with your staff we understand the Committee's desire to receive these responses immediately, rather than incurring further delay if the Department were to revise the responses to correspond with recent changes in the law. We look forward to continuing to work with the Committee on this critical issue.

We hope that this information is of assistance to the Committee. Please do not hesitate to call upon us if we may be of additional assistance. The Office of Management and Budget advises us that from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,

Brian A. Benczkowski
Principal Deputy Assistant Attorney General

Enclosures

cc: The Honorable Arlen Specter
Ranking Minority Member

FISA for the 21st Century
Wednesday, July 26, 2006
Questions for Steven G. Bradbury

Questions from Chairman Specter

1. **Can you describe the current process for seeking approval of an application for a warrant? How is this process more flexible from the process of seeking a routine criminal warrant? What are the problems with this process and how does my bill help solve some of them?**

ANSWER: Obtaining an order authorizing electronic surveillance under section 104 of FISA, 50 U.S.C. § 1804, requires the Department of Justice to prepare and to file an application that documents in detail the information justifying surveillance. For example, the statute and practice require that each application contain a lengthy statement of certain facts supporting the application and a certification from a high-ranking Executive Branch official with national security responsibilities who is appointed by the President with the advice and consent of the Senate. Moreover, all applications under section 104 must be approved by the Attorney General, as defined by FISA. Fulfilling these requirements can take substantial time and effort. The process of preparing, reviewing, and approving applications for orders to conduct electronic surveillance can impede the timely collection of foreign intelligence in certain circumstances.

FISA's provisions for emergency surveillance do not entirely ameliorate these problems. The emergency authorization provision in section 105(f) of FISA, 50 U.S.C. § 1805(f), which permits 72 hours of surveillance before obtaining a court order, does not allow the Government to undertake surveillance immediately. Rather, before surveillance can begin, the Attorney General first must personally "determine[] that . . . the factual basis for issuance of an order under [FISA] to approve such surveillance exists." *Id.* § 1805(f)(2). Great care must be exercised in reviewing requests for emergency surveillance, because if the Attorney General authorizes emergency surveillance and the Foreign Intelligence Surveillance Court ("FISC") does not subsequently approve an application for the surveillance, then the surveillance must cease 72 hours after its initial authorization, and there is a presumption that the court would order disclosure of the surveillance to an affected person. *See id.* § 1806(j).

Although FISA does allow innovative approaches (which cannot be described in this unclassified setting), the approval process for electronic surveillance in ordinary criminal cases is in some ways more flexible than the process for obtaining an order authorizing electronic surveillance under FISA. Unlike under FISA, applications under Title III do not require the approval or certification of the Attorney General or another similarly high-level Executive Branch official. Instead, applications under Title III need only have the approval of the Assistant Attorney

43453.036

General for the Criminal Division or a deputy assistant attorney general in that division.

Finally, it is my understanding that the bill to which you refer, S. 2453, which was introduced in the 109th Congress, has undergone substantial revision, and has not been reintroduced in this Congress. Nevertheless, we continue to believe that any amendment to FISA should streamline the application and authorization procedures for obtaining an order authorizing electronic surveillance. More fundamentally, amending the definition of "electronic surveillance," in combination with other amendments to FISA, would help to restore FISA to its original focus on protecting the privacy of U.S. persons in the United States.

2. **Technology has changed tremendously since 1978. What are some of the technological hurdles that make FISA obsolete today? Do you agree with how S. 2453 deals with emerging technological issues? Is it feasible for the FISA Court to make the type of determinations and issue the type of program-wide warrants that the bill envisions?**

ANSWER: A full explanation of the technological changes that have impacted the operation of foreign intelligence collection conducted under FISA would require a discussion of highly classified and sensitive information. In short, since 1978 there has been a fundamental transformation in the means by which we transmit communications. Sheer fortuity in the development and deployment of new communications technologies, rather than a considered judgment of Congress, has resulted in a considerable expansion of the reach of FISA beyond the statute's original focus on the domestic communications of U.S. persons.

S. 2453, which was introduced in the 109th Congress, has undergone substantial revision and has not been reintroduced in this Congress. Nevertheless, we continue to believe that the definition of "electronic surveillance" must be changed to account for the revolution in communications technology since 1978. This critical term can and should be defined in a technologically neutral way that, in combination with other amendments, would return FISA to its original focus on protecting the privacy of U.S. persons in the United States.

3. **Would the President continue the Terrorist Surveillance Program (TSP) if the Foreign Intelligence Surveillance Court (FISC) or the Court of Review concluded that the program is unconstitutional?**

ANSWER: As you are aware, on January 10, 2007, a judge of the FISC issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that at least one of the communicants is a member or an agent of al Qaeda or an affiliated associated terrorist organization. As a result of these orders, any electronic surveillance that may have been occurring as part of the Terrorist Surveillance Program now is subject to the approval of the FISC. Under these

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00090 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.037

circumstances, the President determined not to reauthorize the Terrorist Surveillance Program when the last authorization expired.

4. **Was the Court of Review correct when it said that FISA cannot encroach on the President's constitutional authority?**

ANSWER: The Foreign Intelligence Surveillance Court of Review was correct when, relying upon the decisions of *every* court of appeals that had decided the issue, it took "for granted that the President" has the constitutional authority to conduct electronic surveillance to obtain foreign intelligence without prior judicial approval and that FISA "could not encroach on the President's constitutional power." *In re Sealed Case*, 310 F.3d 717, 742 (For. Intel. Surv. Ct. Rev. 2002). It is well established that the President has the independent constitutional authority to conduct foreign intelligence surveillance without prior judicial approval, even during times of peace. *See United States v. Truong Dinh Hung*, 629 F.2d 908, 913-17 (4th Cir. 1980); *United States v. Butenko*, 494 F.2d 593, 602-06 (3d Cir. 1974) (en banc); *United States v. Brown*, 484 F.2d 418, 425-27 (5th Cir. 1973); *United States v. bin Laden*, 126 F. Supp. 2d. 264, 271-77 (S.D.N.Y. 2000).

a. **If that is so, does repealing the so-called exclusivity provision do more than make clear that Congress does not wish to provoke a constitutional clash?**

ANSWER: Construing FISA to preclude the President from conducting electronic surveillance for the purpose of collecting foreign intelligence against an enemy during an armed conflict would raise a serious constitutional question. *See Legal Authorities Supporting the Activities of the National Security Agency Described by the President* at 20-23 (Jan. 19, 2006) ("*Legal Authorities*"). Repealing the so-called exclusivity provision of FISA, codified at 18 U.S.C. § 2511(2)(f), simply would clarify that Congress does not intend to limit the authority that the President has under the Constitution, thus avoiding the potential for a serious constitutional dispute regarding whether FISA encroaches upon the President's inherent constitutional authority.

b. **Aside from the constitutional law, is it good policy to interfere with the President's ability to detect and prevent terrorist plots of a declared enemy?**

ANSWER: It is, of course, never good policy to interfere with either the Nation's ability to detect and to prevent terrorist plots or to engender a constitutional clash between the Branches. Intelligence indicates that, more than five years after al Qaeda succeeded in launching the single most deadly foreign attack on American soil in history, we continue to confront a determined and deadly enemy that is dedicated to launching additional catastrophic attacks against America.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00091 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.038

5. **Would simply throwing more resources into the current FISA process address the problems that required the President to create the Terrorist Surveillance Program (TSP)?**

   ANSWER: No. Although additional resources are always welcome, committing even substantial additional resources within the current FISA framework would not provide the modernization that FISA needs. Several problems with FISA cannot be solved simply by allocating additional money and other resources to the process. Most importantly, the tremendous changes in global telecommunications technology since 1978 have resulted in the unintended expansion of the reach of FISA to include communications that Congress intended to exclude from the scope of the statute. Redefining "electronic surveillance," in combination with other amendments to FISA, would provide the Intelligence Community with much needed speed and agility and, at the same time, would have the effect of restoring FISA's original focus on protecting the privacy of U.S. persons in the United States.

6. **Could the new FISA title be used merely to collect evidence for criminal prosecutions?**

   ANSWER: The proposed new title of FISA referenced in this question was part of S. 2453, which was introduced in the 109th Congress. S. 2453 has undergone substantial revision and has not been reintroduced in this Congress. We are not aware of any current legislative proposal that includes the proposed new title of FISA.

Questions from Senator Leahy

Questions regarding the "White House-Specter Compromise" refer to the substitute amendment to S.2453 marked "Discussion Draft" and attached hereto.

7. **The Justice Department White Paper on the Terrorist Surveillance Program assumes that the NSA's activities constitute "electronic surveillance" as defined by the Foreign Intelligence Surveillance Act ("FISA"). That is a reasonable assumption given the current definition of "electronic surveillance," which covers "any wire communication to or from a person in the United States ... if the acquisition occurs in the United States." But section 9 of the Chairman's bill narrows the definition of "electronic surveillance" and, in particular, repeals the language quoted above. Under the new definition, would the NSA's activities under the Terrorist Surveillance Program constitute "electronic surveillance"?**

   ANSWER: We cannot comment here as to whether certain activities would or would not constitute "electronic surveillance" under any potential new definition of that term in FISA or under the current definition. To do so would require disclosing highly classified and exceptionally sensitive information. In any event, as you are aware, on January 10, 2007, a judge of the FISC issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that at least one of the

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00092 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.039

communicants is a member or an agent of al Qaeda or an affiliated terrorist organization. As a result of these orders, any electronic surveillance that may have been occurring as part of the Terrorist Surveillance Program now is subject to the approval of the FISC. Under these circumstances, the President determined not to reauthorize the Terrorist Surveillance Program when the last authorization expired.

8. **The former presiding judge of the FISA court, Judge Royce Lamberth, said on May 8, 2006, that he believed government lawyers had not used evidence obtained by the NSA under the Terrorist Surveillance Program in FISA applications. Is Judge Lamberth correct on this point? Has the government used this information in its FISA warrant applications and, if not, why not?**

   ANSWER: As a general matter, a judge of the FISC would be familiar with the factual basis for an application by the Government to authorize surveillance pursuant to FISA. As we previously have made clear, we cannot comment on the Department's communications with the FISC or on the operational details of the Terrorist Surveillance Program.

9. **Has the government used information obtained from the Terrorist Surveillance Program in criminal cases?**

   ANSWER: We cannot discuss operational aspects of the Terrorist Surveillance Program, as noted in my answers to Questions 7 and 8. We note, however, that because the Program served a "special need, beyond the normal need for law enforcement," the warrant requirement of the Fourth Amendment did not apply to the Terrorist Surveillance Program. *See, e.g.*, *Vernonia Sch. Dist. v. Acton*, 515 U.S. 646, 653 (1995). And, in view of the narrowly targeted nature of the Program, the essential government interest it served, the appropriate minimization techniques that were employed, and the careful and frequent review by high-level Executive Branch officials, the Program met the Fourth Amendment's reasonableness requirement. Therefore, there would appear to be no constitutional barrier to introducing evidence obtained through the Terrorist Surveillance Program in a criminal prosecution.

   Nevertheless, several considerations would weigh against the use of such evidence in a criminal prosecution. The purpose of the Program was not to bring criminals to justice. Rather, it was a critical intelligence program that was part of an ongoing military operation that provided the United States with an early warning system to protect the Nation from foreign attack by a declared enemy of the United States—al Qaeda. Moreover, the use of such information would carry a substantial risk of disclosing classified information and impairing critical intelligence sources and methods.

10. **Suppose that someone in Pakistan is calling or e-mailing someone in Afghanistan. The call or e-mail is routed through a switch or a wire in the United States, where the government picks it up. Would the current FISA**

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00093 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.040

statute require a warrant in that situation? If yes, please point me to specific language in FISA that you believe would require a warrant in this circumstance.

ANSWER: We cannot comment on this hypothetical in an unclassified forum, because that would require a discussion of highly classified and exceptionally sensitive technical and operational information.

11. **You testified, in response to a question from Senator Specter, that "statutes can reasonably regulate exercises of the President's constitutional authority" but cannot "eliminate it or snuff it out." How does FISA as currently written -- by requiring the President to obtain a warrant for certain categories of domestic surveillance -- "eliminate" or "snuff out" the President's constitutional authority?**

ANSWER: As I stated in my answer to Question 4, it is well established that the President has constitutional authority to conduct electronic surveillance without prior judicial approval for the purpose of collecting foreign intelligence. *See In re Sealed Case*, 310 F.3d 717, 742 (For. Intel. Surv. Ct. Rev. 2002); *United States v. Truong Dinh Hung*, 629 F.2d 908, 913-17 (4th Cir. 1980); *United States v. Butenko*, 494 F.2d 593, 602-06 (3d Cir. 1974) (en banc); *United States v. Brown*, 484 F.2d 418, 425-27 (5th Cir. 1973); *United States v. bin Laden*, 126 F. Supp. 2d. 264, 271-77 (S.D.N.Y. 2000). Some have argued, however, that FISA precludes the President from conducting any electronic surveillance for the purpose of collecting foreign intelligence without obtaining an order from the FISC. If FISA were interpreted to require such an order in all circumstances—including during an armed conflict against an enemy who already has successfully attacked the United States and who repeatedly has avowed its intention to do so again—then it would eliminate the President's constitutional authority. Such a construction would raise a serious constitutional question. *See Legal Authorities Supporting the Activities of the National Security Agency Described by the President* at 20-23 (Jan. 19, 2006) ("*Legal Authorities*").

White House-Specter Compromise

12. **You testified at the hearing that "the President has pledged to the Chairman that he will submit his Terrorist Surveillance Program to the FISA court for approval, if the Chairman's legislation were enacted in its current form, or with further amendments sought by the Administration." Chairman Specter has said that the President objected to memorializing this "pledge" in legislation, *e.g.*, by having the bill *require* the President to submit the program to the FISA court, because the President does not want to bind future Presidents and make an institutional change in the powers of the presidency. Couldn't this objection be met by sunsetting the bill (or, alternatively, sunsetting only that portion of the bill that required the President to submit the program to the FISA court) on the last day of the President's term of office?**

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00094 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.041

ANSWER: S. 2453 is no longer pending before Congress. In addition, as you are aware, on January 10, 2007, a judge of the FISC issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that at least one of the communicants is a member or an agent of al Qaeda or an affiliated terrorist organization. As a result of these orders, any electronic surveillance that may have been occurring as part of the Terrorist Surveillance Program now is subject to the approval of the FISC. Under these circumstances, the President determined not to reauthorize the Terrorist Surveillance Program when the last authorization expired.

13. **Let's say the Administration changes one aspect of the current Terrorist Surveillance Program, as for example by extending it to terrorists who are not affiliated with al Qaeda, or by lowering the self-imposed burden of establishing probable cause. Would the President's "pledge" to submit the program for judicial approval extend to the revised program?**

    ANSWER: Please see my answer to Question 12.

14. **Please identify any provisions in the current version of the bill that the Administration (A) believes may be unconstitutional; (B) claims the authority to disregard, intends to disregard or will decline to enforce; (C) interprets in a manner inconsistent with the clear intent of Congress or consistent with its so-called "unitary executive" theory.**

    ANSWER: S. 2453, which was introduced in the 109th Congress, has undergone substantial revision, and has not been reintroduced in this Congress. The Administration has put forward a comprehensive proposal to modernize FISA as Title IV of its proposed FY 2008 Intelligence Authorization Act, which we believe is constitutional. We would be pleased to work with Congress on ways to streamline and modernize FISA.

Section 3 of White House-Specter Compromise (proposing addition of new section 701 to FISA)

15. **The definition of "electronic tracking" proposed in the new section 701(4) is limited to the substance of a person's electronic communication where that person "has a reasonable expectation of privacy." This phrase appears in FISA and is repeated at several other points in the bill. When would a person talking on the telephone or sending an email to another person not have a reasonable expectation of privacy from government surveillance?**

    ANSWER: As a general matter, an individual talking on the phone or sending an email to another individual would have a reasonable expectation of privacy. For example, the Senate committee report on FISA noted generally that two individuals "talking in a public park, far from any stranger, would not reasonably anticipate that their conversations could be overheard from afar through a directional microphone,

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00095 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.042

and so would retain their right of privacy." S. Rep. No. 95-701, 95th Cong., 2d Sess. (1978) at 37, *reprinted in* 1978 U.S.C.C.A.N. 3973, 4006. The committee report also noted that an individual would not have a reasonable expectation of privacy "where a participant could reasonably anticipate that his activities might be observed." *Id.* Hence, for example, an individual talking on a speaker phone in a public place likely would not have a reasonable expectation of privacy. And prisoners communicating on prison telephones are generally considered not to have a reasonable expectation of privacy in their communications.

It is difficult, however, to identify in the abstract all of the many possible circumstances in which an expectation of privacy would be unreasonable. As you note, the phrase "reasonable expectation of privacy" already appears in FISA, although it is not defined there. *See, e.g.*, 50 U.S.C. § 1801(f). The Fourth Amendment jurisprudence regarding whether a person has a "reasonable expectation of privacy" provides guidance in interpreting the scope of the phrase under FISA. *See, e.g.*, *Kyllo v. United States*, 533 U.S. 27 (2001); *California v. Ciraolo*, 476 U.S. 207 (1986). Under the Fourth Amendment, aside from the well established expectation of privacy a person has in his home, *see Kyllo*, 533 U.S. at 33-34, 40, determining whether a person has a "reasonable expectation of privacy" is a fact-intensive issue, the resolution of which turns upon several inquiries regarding the scope of a search, the subjective expectations of the person, and the objective reasonableness of that expectation, *see Ciraolo*, 476 U.S. at 212-13; *Smith v. Maryland*, 442 U.S. 735, 741-43 (1979). Therefore, rather than attempt to identify in general terms all of the possible circumstances in which a person would not have a reasonable expectation of privacy, it is best to rely upon the case-by-case interpretation of the term in particular circumstances.

16. The term "electronic surveillance program" proposed in the new section 701(5) is defined as including situations "where it is not technically feasible to name every person or address every location to be subjected to electronic tracking." What does "technically feasible" mean? Is it different from, or does it include, "not feasible given the large number of persons or locations to be subjected to electronic tracking"?

ANSWER: These questions refer to the definition of "electronic surveillance program" in proposed section 701(5) of FISA. This provision appears in S. 2453, which was introduced in the 109th Congress. S. 2453 has undergone substantial revision, and it has not been reintroduced in this Congress. We are not aware of any current legislative proposal incorporating this definition of "electronic surveillance program."

17. In the same definition of "electronic surveillance program," what constitutes "an extended period of electronic surveillance"? Does this mean that something of shorter duration can be undertaken with no approvals?

ANSWER: Please see my answer to Question 16.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00096 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.043

18. The term "intercept" is defined in the new section 701(9) as acquisition "by a person" of a communication, "through the use of any electronic, mechanical, or other device." Would the meaning of this change if you removed "by a person?" If the acquisition is accomplished entirely by automation, with no person involved, would it not be an "intercept" and, therefore, not be governed by these rules?

ANSWER: These questions refer to the definition of "intercept" in proposed section 701(9) of FISA. This provision appears in S. 2453, which was introduced in the 109th Congress. S. 2453 has undergone substantial revision, and it has not been reintroduced in this Congress. We are not aware of any current legislative proposal that includes this definition of "intercept."

19. Separate from the Chairman's bill, does the Administration have a legal position on whether automatic searching of the contents of communications is a search or seizure for Fourth Amendment purposes?

ANSWER: As an initial matter, it is important to be clear that the Terrorist Surveillance Program did not involve any such activity. The Program targeted for collection only international communications into or out of the United States where there was probable cause to believe that at least one of the communicants was a member or agent of al Qaeda or an associated terrorist organization. As General Hayden correctly stated, the Terrorist Surveillance Program was *not* a "data-mining" program; it was not a "drift net out there where we're soaking up everyone's communications." Rather, under the Program, NSA targeted for interception "very specific communications" for which, in NSA's professional judgment, there was probable cause to believe that one of the parties to the communication was a member or an agent of al Qaeda or an affiliated terrorist organization—people "who want to kill Americans." Remarks by General Michael V. Hayden to the National Press Club, *available at* http://www.dni.gov/release_letter_012306.html.

In any event, the Department of Justice has not announced a legal position regarding whether automatic searching of the contents of communications is either a search or a seizure under the Fourth Amendment to the Constitution of the United States.

<u>Section 4 of White House-Specter Compromise (proposing addition of new section 702 to FISA)</u>

20. Under the new section 702(a)(2), reauthorization of an electronic surveillance program can be "for a period of time not longer than [the Foreign Intelligence Surveillance Court] determines to be reasonable." Under this provision, a single judge could authorize a program for 5 or 10 years, or longer. Is there any way for a future judge to re-examine that decision? Does it seem appropriate not to

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00097 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.044

give the judges any guidance on what Congress believes might be an outside limit on reasonableness?

ANSWER: These questions refer to proposed section 702(a) of FISA. This provision appears in S. 2453, which was introduced in the 109th Congress. S. 2453 has undergone substantial revision, and it has not been reintroduced in this Congress. We are not aware of any current legislative proposal that incorporates proposed section 702(a).

21. **As I read the new section 702(a), a single FISA Court judge can issue and indefinitely renew an order for an "electronic surveillance program," with no possibility of review by another judge or panel of judges at any time. Is that correct?**

ANSWER: Please see my answer to Question 20.

22. **In your exchange with Senator Feinstein, you sought to reassure her that a program warrant under this bill would be kept in check because "It could only be approved for 90 days" and then the government "would have to come back in" to the FISA court for careful judicial review and reauthorization. Is it the Administration's position that, once a program warrant is sought and authorized under the bill, the government *must* submit to periodic review and reauthorization, or could the President simply continue the program past the initial 90-day period of authorization pursuant to his inherent authority under Article II?**

ANSWER: These questions refer to provisions in S. 2453, which was introduced in the 109th Congress, that would have authorized the FISC to issue an order approving an "electronic surveillance program." S. 2453 has not been reintroduced in this Congress, and we are not aware of any current legislative proposal that incorporates these "electronic surveillance program" provisions.

23. **Regarding mandatory transfer for review, wouldn't it be more reasonable to transfer cases to the Foreign Intelligence Surveillance Court of Review only after a regular District Court judge found that proceeding in the regular courts would violate the state secrets privilege? FISA was created to handle mainly ex parte proceedings. (Even in the one case that went to the Court of Review, only the government was a party, and others were limited to an amicus role.) Aren't the regular courts the best place for adversarial proceedings? Haven't regular courts for many years been making these kinds of decisions about the need to protect national security information, either in applying the state secrets privilege or the Classified Information Procedures Act?**

ANSWER: These questions refer to provisions in S. 2453 concerning the transfer of cases to the Foreign Intelligence Surveillance Court of Review. S. 2453, which was introduced in the 109th Congress, has not been reintroduced in this Congress. We are

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00098 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.045

aware of no current legislative proposal to transfer cases to the Court of Review. The Administration has proposed similar amendments that would authorize the transfer of cases involving classified communications intelligence activities to the Foreign Intelligence Surveillance Court ("FISC") as part of its proposed FY 2008 Intelligence Authorization Act. We would be pleased to work with Congress on ways to streamline and modernize FISA and to help protect critical national security information from disclosure.

We believe that transferring litigation concerning classified communications intelligence activities to the FISC (which we believe is better situated than the Court of Review to conduct discovery if necessary) from regular federal district courts would both help to protect national security and facilitate resolution of those cases by Article III judges with expertise in the statutory and constitutional issues raised by foreign intelligence surveillance.

24. If we adopt the mandatory transfer provisions as proposed, would the Administration agree to waive the state secrets privilege in litigation before the Foreign Intelligence Surveillance Court of Review and, if not, why not? Is the Administration seeking both the protection of the more secretive proceedings of the FISA court and full scope of the state secrets privilege?

ANSWER: These questions refer to provisions in S. 2453 concerning the transfer of cases to the Foreign Intelligence Surveillance Court of Review. S. 2453, which was introduced in the 109th Congress, has not been reintroduced in this Congress. We are aware of no current legislative proposal to transfer cases to the Court of Review. The Administration has proposed similar amendments that would authorize the transfer of cases involving classified communications intelligence activities to the FISC as part of its proposed FY 2008 Intelligence Authorization Act.

The Department of Justice would not—and should not—commit in advance to waive potential assertions of the state-secrets privilege in any litigation. The "well established" state-secrets privilege serves the essential function of allowing the Government to protect against the discovery of information in litigation, the disclosure of which could be harmful to national security. *See United States v. Reynolds*, 345 U.S. 1, 7-8 (1953); *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C. Cir. 1983). Accordingly, rather than agree to a universal waiver of the state-secrets privilege, the Department of Justice, as it has always done, would decide in each case whether to assert the privilege.

25. The bill would require transfer to the Foreign Intelligence Surveillance Court of Review of any case challenging the legality of "classified communications intelligence activity relating to a foreign threat, including an electronic surveillance program, or in which the legality of such activity or program is in issue." What sorts of cases would this language cover, besides cases challenging the legality of the so-called Terrorist Surveillance Program? Why shouldn't we

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00099 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.046

narrow this language to apply only to the program that the President has acknowledged?

ANSWER: These questions refer to provisions in S. 2453 concerning the transfer of cases to the Foreign Intelligence Surveillance Court of Review. S. 2453, which was introduced in the 109th Congress, has not been reintroduced in this Congress. We are aware of no current legislative proposal to transfer cases to the Court of Review. The Administration has proposed similar amendments that would authorize the transfer of cases involving classified communications intelligence activities to the FISC as part of its proposed FY 2008 Intelligence Authorization Act.

The proposed narrowing language in this question would pose several disadvantages. First, the Government is currently litigating cases in various courts in which there are a variety of allegations that do not coincide with the Terrorist Surveillance Program. Such suits, even if baseless, can cause serious harm to national security because the Government is placed in the position of having to choose between asserting the state-secrets privilege and denying specific allegations (which itself discloses information). Second, plaintiffs likely would attempt to plead carefully to avoid such a narrow transfer provision—defeating its very purpose.

26. How would litigation in transferred cases before the Foreign Intelligence Surveillance Court of Review be conducted? What rules and procedures would apply?

ANSWER: These questions refer to provisions in S. 2453 concerning the transfer of cases to the Foreign Intelligence Surveillance Court of Review. S. 2453, which was introduced in the 109th Congress, has not been reintroduced in this Congress. We are aware of no current legislative proposal to transfer cases to the Court of Review. Any attempt to answer this question would be speculative at this time.

27. The proposed paragraph on dismissal of transferred cases (the new section 702(b)(5)) states that "a challenge to the legality of an electronic surveillance program [may be dismissed] for any reason provided for under law." What purpose does this paragraph serve, if any? What would change if this language were dropped?

ANSWER: This question concerns an aspect of the transfer provisions of S. 2453, which was introduced in the 109th Congress. The Administration has proposed a similar amendment in the 110th Congress as part of its proposed FY 2008 Intelligence Authorization Act. Such language would make clear that both the FISC and the court in which litigation was instituted would have authority to dismiss a case at any time "for any reason provided for under law." In a transferred case, the FISC should not be limited to dismissing the case upon grounds related to national security, such as the state-secrets privilege. Rather, in the interest of judicial economy, the FISC should be free to dismiss a case for any reason warranted under law such as, for example, lack of standing or failure to state a claim upon which relief may be granted

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00100 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.047

pursuant to Federal Rule of Civil Procedure 12(b)(6). Likewise, with regard to a case that has not yet been transferred to the FISC, the originating court should have authority to dismiss the case, for example, on the grounds of the state-secrets privilege. Finally, if the FISC were to transfer a case back to the originating court, the originating court should still have the authority to dismiss the case as provided for by law.

Section 8 of White House-Specter Compromise

28. Senator Specter has said that the "Executive Authority" provision of his bill does not grant the President any new authority, it simply recognizes any existing authority he may have. (A) Do you agree? (B) If so, could we accomplish this more clearly by amending the "Executive Authority" provision to read as follows: "Nothing in this Act shall be construed to limit the constitutional authority of the President to collect intelligence with respect to foreign powers and agents of foreign powers, to the extent that he retains any such authority despite the "exclusive means" clause of section 2511(2)(f) of title 18, United States Code"? Isn't that the way to ensure that Congress is not granting new authority to the President, but only acknowledging the possibility that he may have some residual authority?

ANSWER: We agree with Senator Specter's conclusion. Although S. 2453 has not been reintroduced in this Congress, it would have created a new section 801 of FISA, which would have provided: "Nothing in this Act shall be construed to limit the constitutional authority of the President to collect intelligence with respect to foreign powers and agents of foreign powers." The plain terms of section 801 could not be read to grant the President any new authority. That interpretation of proposed section 801 is strongly supported by the Supreme Court's decision in *United States v. United States District Court* ("*Keith*"), 407 U.S. 297 (1972), which construed a similar provision then codified at 18 U.S.C. § 2511(3). Section 2511(3) stated that "[n]othing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect [against specified dangers]." The Court wrote:

> At most, this is an implicit recognition that the President does have certain powers in the specified areas. Few would doubt this, as the section refers—among other things—to protection 'against actual or potential attack or other hostile acts of a foreign power.' But so far as the use of the President's electronic surveillance power is concerned, *the language is essentially neutral.*
>
> *Section 2511(3) certainly confers no power*, as the language is wholly inappropriate for such a purpose. It merely provides that the Act shall not be interpreted to limit or disturb such power as the President may have under the Constitution. *In short, Congress simply left presidential powers where it found them.*

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00101 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.048

Keith, 407 U.S. at 307 (emphases added). As the Supreme Court concluded, wording like that found in section 801 is particularly well-suited to making clear that Congress did not intend to create a constitutional clash between the Branches.

Moreover, the alternative language suggested by the question is not preferable to the language in proposed section 801. By its plain terms, proposed section 801 is a simple, clear statement that FISA should be interpreted to avoid a serious constitutional question that would arise if the statute were read to interfere with the President's well recognized constitutional authority to conduct electronic surveillance for foreign intelligence purposes even during times of peace, let alone during an armed conflict. Your proposed alternative language would perpetuate the difficult constitutional issue regarding the President's constitutional authority by suggesting that FISA did purport to extinguish the constitutional authority of the President.

29. The conforming amendments proposed in section 8(c) of the bill would prospectively immunize U.S. personnel from criminal liability for conducting warrantless electronic surveillance outside of FISA and Title III, if authorized by the President. Do you agree that this amendment has no retroactive effect?

ANSWER: This question concerns section 8(c) of S. 2453, which was introduced in the 109th Congress. S. 2453 has not been reintroduced in this Congress, and we are aware of no current legislative proposal that incorporates the provisions of section 8(c) of S. 2453.

30. Has the Department of Justice initiated any criminal investigations into possible violations of section 109 of FISA [18 U.S.C. 1809], which currently prohibits intentional wiretapping under color of law except as authorized "by statute." If not, why not?

ANSWER: To my knowledge, the Department of Justice has not initiated any criminal investigations into possible violations of section 109 of FISA, 50 U.S.C. § 1809. With respect to the Terrorist Surveillance Program addressed in the Department's *Legal Authorities* paper, even assuming that Program involved any "electronic surveillance," as defined by FISA, as we explained in *Legal Authorities*, section 109 of FISA expressly contemplates that Congress may authorize electronic surveillance through a subsequent statute without amending or referencing FISA. *See id.* at 20-23; 50 U.S.C. § 1809(a)(1). Indeed, historical practice makes clear that section 109 of FISA incorporates electronic surveillance authority outside FISA and Title III. The Authorization for Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (Sept. 18, 2001) ("Force Resolution"), is best understood as another congressional source of electronic surveillance authority (specific to the armed conflict with al Qaeda and its affiliates), and surveillance conducted pursuant to the Force Resolution therefore is consistent with FISA. *See Legal Authorities* at 23-28. The Force Resolution is a statute authorizing, among other well recognized incidents

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00102 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.049

of the use of military force, the use of signals intelligence to learn the intentions of and to protect against al Qaeda and its affiliated terrorist organizations. *See id.*

Section 9 of White House-Specter Compromise

31. Section 9(b)(1) of the bill broadens yet again the definition of an "agent of a foreign power." It would now include any non-U.S. person who has, or is even expected to receive, information that relates to the ability of the United States to protect against a potential attack or sabotage. (A) What individuals who are not currently covered by FISA would be covered by this new definition? (B) Given the potential usefulness of vast categories of privately held information -- including credit card information, travel information, and other personal information of U.S. citizens -- in potentially helping the government to protect against an attack, does this make anyone who holds any of this information -- assuming they are not a U.S. person, but even if they work for a U.S. company -- an agent of a foreign power? (C) In this context, the term "person" includes a corporation. What is to keep this provision from being applied to foreign-owned banks, airlines, and communications service providers operating in the United States?

ANSWER: This question concerns section 9(b)(1) of S. 2453, which was introduced in the 109th Congress. The Administration has proposed a similar amendment in the 110th Congress as part of its proposed FY 2008 Intelligence Authorization Act. We continue to believe that FISA must be modernized. For that reason, we propose amending the definition of "agent of a foreign power" to include non-U.S. persons who possess or receive *significant* "foreign intelligence information," as defined by FISA, while in the United States. This amendment would allow the United States to acquire valuable intelligence from a non-U.S. person in the United States under circumstances in which the non-U.S. person's relationship to a foreign power is unclear.

32. Section 9(b)(2) amends and significantly narrows the definition of "electronic surveillance." What specific categories of surveillance activity would no longer require a warrant if this amendment were adopted?

ANSWER: This question concerns section 9(b)(2) of S. 2453, which was introduced in the 109th Congress. The Administration has proposed similar amendments in the 110th Congress as part of its proposed FY 2008 Intelligence Authorization Act. We continue to believe that FISA must be modernized, and we would be pleased to work with Congress to accomplish this goal. In this unclassified setting we cannot describe specific surveillance activities that would no longer constitute "electronic surveillance." We can state that, in combination with other amendments to FISA, the revisions to the definition of "electronic surveillance" would have the effect of returning FISA to its original focus on protecting the privacy of U.S. persons in the United States. For further information, please see my answer to Question 2.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00103 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.050

33. Under what specific circumstances would the bill permit warrantless surveillance of domestic targets where current law requires a court order?

ANSWER: S. 2453, the bill referenced in this question, has not been reintroduced in this Congress. The Administration supports similar but more modest amendments to FISA, which are set forth in its proposed FY 2008 Intelligence Authorization Act. Although in this unclassified setting we cannot provide detail on the specific circumstances in which that proposal would permit foreign intelligence activities without an order from the FISC, the Administration's proposals would have the effect of returning FISA to its original focus on protecting the privacy of U.S. persons in the United States.

34. Section 9(b)(3) changes the definition of Attorney General from being restricted to the Attorney General himself or his Deputy, to now include any person "or persons" designated by the Attorney General. (A) Would this permit the Attorney General to delegate his authority to someone outside of the Department of Justice, *e.g.*, to someone in the NSA, CIA, or Defense Department? (B) Does the President's promise to sign this bill only if it is not amended include not placing limits on how many people can be the "Attorney General" at one time, or how far down the chain of command or in how many agencies the Attorney General can delegate his authority?

ANSWER: This question concerns section 9(b)(3) of S. 2453, which was introduced in the 109th Congress. S. 2453 has not been reintroduced in this Congress, and we are aware of no current legislative proposal that incorporates the provisions of section 9(b)(3) of S. 2453.

35. Section 9(b)(5) narrows the definition of "contents," when used with respect to a communication, to exclude information concerning the identity of the parties to the communication and information concerning the existence of the communication. Why is this change needed? What practical effect would it have? What specific categories of surveillance activity would no longer require a warrant if it were adopted?

ANSWER: Revising the definition of "contents" in FISA to include only "information concerning the substance, purport, or meaning of . . . communications," 18 U.S.C. § 2510(8), would harmonize FISA's definition of "contents" with the definition used in federal laws regulating electronic surveillance conducted for domestic law enforcement purposes. It also would make clear that the acquisition of information in which persons have no reasonable expectation of privacy is not subject to the very high standard of full-content interceptions under Title I of FISA.

36. Section 9(c) expands the so-called "embassy exception" to FISA. Why is this change needed? What practical effect would it have? What specific categories of surveillance activity would no longer require a warrant if it were adopted?

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00104 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.051

ANSWER: This question concerns section 9(c) of S. 2453, which was introduced in the 109th Congress. The Administration has proposed similar but more modest amendments in the 110th Congress as part of its proposed FY 2008 Intelligence Authorization Act. Attorney General authorization under current section 102 of FISA requires, among other things, circumstances in which the "communications [are] transmitted exclusively by means of communications used exclusively between or among foreign powers." In this unclassified setting we cannot describe specific categories of surveillance activities that would be affected by the proposal. We can state that the Administration's proposal would modernize FISA to account for changes in the means of communications among foreign powers that have seriously eroded the usefulness of the current version of section 102 of FISA. The focus of section 102 of FISA under the Administration's proposed revision would remain on the communications of traditional foreign powers.

37. Currently, FISA's "embassy exception" requires the Attorney General to certify, among other things, that "there is no substantial likelihood that the surveillance will acquire the contents of any communications to which a United States person is a party." The White House-Specter compromise, in section 9(c), would delete this requirement. Why is this change needed? What practical effect would it have? Would it make it easier to collect and retain information about U.S. citizens?

ANSWER: This question concerns section 9(c) of S. 2453, which was introduced in the 109th Congress. The Administration has proposed similar but more modest amendments in the 110th Congress as part of its proposed FY 2008 Intelligence Authorization Act. The current "no substantial likelihood" requirement in section 102 of FISA, coupled with changes in communications technology since FISA was enacted, reduces dramatically the usefulness of this provision. The Administration's proposal would help modernize FISA by allowing this provision to fulfill the role Congress envisioned in 1978. The focus of the provision would remain on communications of traditional foreign powers. And any surveillance conducted under the amended provision still would require that the Attorney General implement the "minimization procedures" required by section 101(h) of FISA. *See* FY 2008 Intelligence Authorization Act § 402(a) ("An electronic surveillance authorized under this section may be conducted only in accordance with the Attorney General's certification and the minimization procedures."); 18 U.S.C. § 1801(h) (defining minimization requirements).

38. Section 9(e) of the bill, entitled "Applications for Court Orders," deletes the current requirement to provide "a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance." Why?

ANSWER: This question concerns section 9(e) of S. 2453, which was introduced in the 109th Congress. The Administration has proposed similar changes in the 110th Congress as part of its proposed FY 2008 Intelligence Authorization Act. This

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00105 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.052

provision would help streamline FISA by reducing the burden involved in providing the FISC with information that is not necessary to protect the privacy of U.S. persons in the United States.

39. Section 9(e) also deletes the requirement that certifications be made by Senate-confirmed officers, providing instead that they may be made by "an[y] executive branch officer authorized by the President to conduct electronic surveillance for foreign intelligence purposes." (A) Who besides Senate-confirmed officers would this language include? (B) Please state your objection, if any, to the limitation in current law.

ANSWER: This question concerns section 9(e) of S. 2453, which was introduced in the 109th Congress. The Administration has proposed a similar amendment in the 110th Congress as part of its proposed FY 2008 Intelligence Authorization Act. The Administration's proposal would authorize an official "designated by the President to authorize electronic surveillance for foreign intelligence purposes" to make the certification required in a FISA application. This change would help to reduce a current bottleneck in the FISA process caused by the fact that very few officials currently can certify FISA applications. The provision would require a presidential designation, thus maintaining accountability.

40. Section 9(e) also deletes the current requirement to reveal all previous applications to other judges involving the people or places targeted by the application and the action taken on those applications. Absent this requirement, if a previous application was denied by another FISA judge, could the FBI take the application to another FISA judge and never have to reveal that it had previously been denied?

ANSWER: This question concerns section 9(e) of S. 2453, which was introduced in the 109th Congress. The Administration has proposed similar amendments as part of its proposed FY 2008 Intelligence Authorization Act that would streamline FISA's application process. The Administration's proposal would not delete this requirement, but instead would require a summary of previous applications in lieu of the detailed statement of all previous applications currently required. This provision would help streamline FISA, and it would not permit the Government to present a previously denied application to a different judge. *See* 50 U.S.C. § 1803(a) (prohibiting this).

41. Section 106(i) of FISA currently requires that information obtained from communications that are accidentally intercepted without appropriate approval, where a warrant would have been required under law, shall be destroyed "unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person." This bill (in section 9(g)) amends that section of FISA to allow the Attorney General (which, under section 9(b)(3), could now mean anyone the Attorney General has designated) to decide to keep such information if he or she decides that it contains "significant foreign

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00106 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.053

intelligence." Would that change apply to U.S. citizen phone calls and to information about U.S. citizens?

ANSWER: This question concerns section 9(g) of S. 2453, which was introduced in the 109th Congress. The Administration has proposed a similar amendment in the 110th Congress as part of its proposed FY 2008 Intelligence Authorization Act. The provision you reference, section 106(i) of FISA, currently applies only to certain radio communications. The Administration's proposed amendment to section 106(i) would help make FISA technologically neutral with respect to incidentally acquired information. This amendment also would ensure that the Government, upon the Attorney General's determination, can retain and act upon valuable foreign intelligence information that is collected *incidentally*, rather than being required to destroy information that could be critical to the national security.

42. Section 9(i) of the bill would amend FISA's criminal penalty provision [50 U.S.C. 1809(a)], which is already amended by section 8(c)(2) of the bill. Current law excepts from criminal liability those who engage in electronic surveillance "as authorized by statute." Section 8(c)(2) extends that exception to those who act "as authorized by statute *or under the Constitution*." Under section 9(i), the exception would cover those who act "as authorized by law." As between the amendments proposed in section 8(c)(2) and section 9(i), which does the Administration prefer and why?

ANSWER: This question concerns section 9(i) of S. 2453, which was introduced in the 109th Congress. S. 2453 has not been reintroduced in this Congress, and we are aware of no current legislative proposal that incorporates the provisions of section 9(i) of S. 2453. This amendment would simply acknowledge the President's constitutional authority and thus avoid a potential constitutional issue.

43. Section 9(j) of the bill repeals section 111 of FISA [50 U.S.C. 1811], which permits the Attorney General to authorize warrantless electronic surveillance to acquire foreign intelligence information for up to 15 days following a declaration of war by Congress. Why is this change needed? What practical effect would it have?

ANSWER: This question concerns section 9(j) of S. 2453, which was introduced in the 109th Congress. S. 2453 has not been reintroduced in this Congress, and we are aware of no current legislative proposal that incorporates the provisions of section 9(j) of S. 2453. The amendment would help modernize FISA. The United States has fought only five declared wars in its history, and the last ended more than 60 years ago.

44. Section 9(k) of the bill changes the definition of "physical search" in title III of FISA. Why is this change needed? What practical effect would it have?

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00107 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.054

ANSWER: This question concerns section 9(k) of S. 2453, which was introduced in the 109th Congress. S. 2453 has not been reintroduced in this Congress, and we are aware of no current legislative proposal that incorporates the provisions of section 9(k) of S. 2453.

Questions from Sen. Kennedy

45. In December 2005, at a White House press briefing, General Hayden said that the NSA warrantless wiretapping program targeting communications that involve al Qaeda, with one end inside the United States, had been successful in detecting and preventing terrorist attacks. He also said that the program deals only with international calls with a time period much shorter than is typical under the Foreign Intelligence Surveillance Act.

When asked about the inadequacies of FISA, which led to the creation of the domestic spying program, General Hayden said that the "whole key here is agility... [and] the intrusion into privacy is significantly less. It's only international calls," and the time period for surveillance is shorter than that is generally authorized under the Foreign Intelligence Surveillance Act. Attorney General Gonzales reiterated the statement that the program was limited to those with ties to al Qaeda.

In a session with the *San Diego Union-Tribune*, General Hayden said that the publicly acknowledged program is "limited" and "focused," and has been "effective."

At the Senate Judiciary Committee hearing on July 26, 2006, Mr. Bradbury stated that the program involves "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 affiliate terrorist organization."

The program described in the bill negotiated by the Administration and Senator Specter is significantly broader than the program General Hayden said had been successful in detecting and preventing attacks. The bill would allow authorization of a spying program targeted not just at members of al Qaeda but at anyone "reasonably believed to have communication with or be associated with" *any* foreign powers or their agents engaged in terrorism preparations. This broad standard could sweep in thousands of innocent Americans who are unaware that they are "associated with" a person the government considers to be a terrorist.

General Hayden has also repeatedly stated that the targets for the wiretapping are approved by "shift supervisors," whom he later characterized as "senior executives." Yet, this bill authorizes the Attorney

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00108 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.055

General to delegate his authority to anyone he wishes, instead of limiting the delegation to senior officials.

Questions: Members of the Administration have repeatedly claimed that the publicly announced program has saved an untold number of American lives.

- **Why did the Administration insist on a bill that would allow the authorization of a program that spies on even more Americans?**
- **Is this just another attempt to expand Executive authority even further, or does the Administration have a specific, documented need to spy on far larger numbers of innocent Americans than are at risk under the current program?**
- **What are the Administration's justifications for such a broad program that far exceed[s] the program described publicly by each of you in past statements and in testimony before this Committee?**

ANSWER: These questions concern S. 2453, which was introduced in the 109th Congress. S. 2453 has not been reintroduced in this Congress, and we are not aware of any current legislative proposal that includes the new title of FISA that was proposed in S. 2453, which would have provided for FISC approval of an "electronic surveillance program," as defined in S. 2453. The "electronic surveillance program" title proposed in S. 2453 was intended to be flexible, to enable the United States in the future to conduct programs of electronic surveillance to help protect the Nation from another attack by international terrorists, and to do so with the approval of the FISC in a manner consistent with the need for effective intelligence capabilities in an era of pervasive global communications. The proposed title was not intended to be limited to the Terrorist Surveillance Program that was publicly acknowledged by the President. Nor was it intended to "spy" on large numbers of Americans. As the Attorney General announced on January 10, 2007, a judge of the FISC approved FISA orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that at least one of the communicants is a member or agent of al Qaeda or an affiliated terrorist organization. As a result of these orders, any electronic surveillance that may have been occurring as part of the Terrorist Surveillance Program is now subject to the approval of the FISC, and under the circumstances the President determined not to reauthorize the Terrorist Surveillance Program when it last expired.

46. **At the July 26, 2006, Senate Judiciary Committee hearing, Mr. Bradbury described the NSA warrantless wiretapping program as "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 affiliate terrorist organization."**

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00109 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.056

Question:

- **What is the legal definition of an "affiliate terrorist organization"? Who makes the determination that an organization is one that is an "affiliate terrorist organization" to al Qaeda? What are the criteria used? How quickly is such a determination made?**

ANSWER: We cannot describe operational details of the Terrorist Surveillance Program. However, on January 10, 2007, a judge of the FISC issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that at least one of the communicants is a member or an agent of al Qaeda or an affiliated terrorist organization. As a result of these orders, any electronic surveillance that may have been occurring as part of the Terrorist Surveillance Program now is subject to the approval of the FISC. The judge of the FISC had to determine that all statutory requirements of FISA were satisfied.

47. The Intelligence Authorization Act for fiscal year 2000 included a provision requiring a report to Congress from the intelligence community on the legal standards used by agencies in conducting signals intelligence, including electronic surveillance. Congress wisely saw the need to require legal justification from the intelligence community on any program affecting the privacy interests of Americans. The report was submitted before 9/11. In that report, the NSA said, "in order to conduct electronic surveillance against a U.S. person located within the United States, FISA requires the intelligence agency to obtain a court order from the Foreign Intelligence Surveillance Court." We must guarantee the same oversight in any new legislation.

Question:

- **Will the Administration agree to report on the legal standards being used now? Obviously, the standards provided to Congress in 2000 have become outdated and, perhaps, obsolete.**

ANSWER: This question may assume the continued operation of the Terrorist Surveillance Program. On January 10, 2007, a judge of the FISC issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that at least one of the communicants is a member or an agent of al Qaeda or an affiliated terrorist organization. As a result of these orders, any electronic surveillance that may have been occurring as part of the Terrorist Surveillance Program now is subject to the approval of the FISC, and the President determined not to reauthorize the Program at that time. Prior to that time, the Intelligence Committees had been briefed on the operational details of the Program in accordance with the National Security Act and longstanding practice.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00110 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.057

48. At the June 26, 2006, Senate Judiciary Committee hearing, you agreed with Senator Cornyn's statement that "there have been at least three courts that have expressly acknowledged the President's inherent power under the Constitution to collect foreign intelligence during a time of war." You later said, "The only decisions from courts are that the President generally has authority under Article II to protect the country through foreign intelligence surveillance."

Questions:

- **You relied on the holdings of three federal courts, including the Second and Fourth Circuits, to support your contentions about executive authority. Why, then, do you support a bill that would strip those same courts of jurisdiction over all cases having anything to do with the NSA warrantless wiretapping program?**

ANSWER: Nothing in S. 2453 would have "stripp[ed]" any federal courts of appeals of jurisdiction in cases "having anything to do with" the Terrorist Surveillance Program. S. 2453 would have permitted the United States to transfer court cases challenging classified communications intelligence activities of the United States to the Court of Review from other courts. Consolidating litigation concerning highly classified communications intelligence activities before a single expert court would ensure uniformity in this critically important area of law and would help to protect critical national security information. Notably, the analysis of the courts of appeals opinions referenced in the question supports the conclusion that federal judges ordinarily lack the expertise called for in such cases.

For those reasons, the Administration supports amendments to FISA that would permit the transfer of cases challenging the legality of classified communications intelligence activities to the FISC and has proposed such amendments as part of its proposed FY 2008 Intelligence Authorization Act. As an initial matter, cases transferred from a district court should be transferred to the FISC, which is akin to a trial court for foreign intelligence surveillance matters, rather than to the Court of Review, which is an appellate court.

- **Which specific holdings of these cases do you rely on to support your view that "the President generally has authority under Article II to protect the country through foreign intelligence surveillance"?**

ANSWER: Every court of appeals to reach the question has concluded that the President possesses constitutional authority to conduct surveillance for foreign intelligence purposes without prior court approval, even during times of peace. *See In re Sealed Case*, 310 F.3d 717, 742 (For. Intel. Surv. Ct. of Rev. 2002); *United States v. Truong Dinh Hung*, 629 F.2d 908, 913-17 (4th Cir. 1980); *United States v. Butenko*, 494 F.2d 593, 602-06 (3d Cir. 1974) (en banc); *United States v. Brown*, 484 F.2d 418, 425-27 (5th Cir. 1973); *see also United States v. bin Laden*, 126 F. Supp. 2d 264, 271-77 (S.D.N.Y. 2000). This conclusion is stronger still in the midst of a congressionally authorized armed conflict undertaken to prevent further

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00111 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.058

attacks on the United States—the core of the President's authority under Article II of the Constitution. As the Supreme Court has long noted, "the President alone" is "constitutionally invested with the entire charge of hostile operations." *Hamilton v. Dillin*, 88 U.S. (21 Wall.) 73, 87 (1874). Included within this constitutional responsibility is the authority to gather foreign intelligence. *See, e.g.*, *Chicago & S. Air Lines v. Waterman S.S. Corp.*, 333 U.S. 103, 111 (1948) ("The President, both as Commander-in-Chief and as the Nation's organ for foreign affairs, has available intelligence services whose reports are not and ought not to be published to the world."); *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 319 (1936) ("[The President] has his confidential sources of information. He has his agents in the form of diplomatic, consular and other officials."); *Totten v. United States*, 92 U.S. 105, 106 (1876) (explaining that the President "was undoubtedly authorized during the war, as commander-in-chief, . . . to employ secret agents to enter the rebel lines and obtain information respecting the strength, resources, and movements of the enemy"); *see also United States v. Marchetti*, 466 F.2d 1309, 1315 (4th Cir. 1972) ("Gathering intelligence information and the other activities of the [CIA], including clandestine affairs against other nations, are all within the President's constitutional responsibility for the security of the Nation as the Chief Executive and as Commander in Chief of our Armed Forces.").

49. Section 8 of the Specter bill indicates that "nothing in [FISA] shall be construed to limit the constitutional authority of the President to collect intelligence with respect to foreign powers and agents of foreign powers." The Attorney General has argued that the clause "does not change the status quo." At the hearing, you agreed with Senator Cornyn's suggestion that this language is nothing more than "a ratification . . . by Congress that the President has that authority".

However, when discussing this provision with Senator Specter, you acknowledged that "statutes can reasonably regulate exercises of the President's constitutional authority." When Senator Leahy asked you whether or not the President's Article II powers can be circumscribed by statute, you answered, "yes."

While your first set of answers is out of line with mainstream constitutional thought, your second set of answers is much more accurate. As the Supreme Court ruled in *Youngstown v. Ohio*, "[w]hen the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum," but "[w]hen the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb."

We still do not know the full contours of the warrantless surveillance program. Based on how the program has been described, it appears to ignore the specific requirements of FISA that bar domestic surveillance without a warrant. If this language is added to the bill, Congress would be expressly endorsing the President's interpretation of his authority over NSA wiretapping.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00112 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.059

Questions:

- **Senator Specter claimed "that line was in the FISA Act of 1978". You responded with "it was," but then clarified your comments to indicate that the bill "was amended to take it out at a later point." Wasn't this provision dropped just before FISA was passed?**

ANSWER: It is my understanding that such a provision was under consideration at some point, but that Congress ultimately did not enact a provision explicitly recognizing the President's inherent right under the Constitution to conduct foreign intelligence surveillance.

- **Doesn't the fact that this line wasn't included in the original legislation but rather was specifically removed from the original legislation suggest that the drafters wanted to make it clear that FISA would be the "exclusive means" under the *Youngstown* framework by which the President could conduct electronic surveillance?**

ANSWER: Whatever the intent of Congress in 1978, an act of Congress cannot strip the President of authority granted to him by the Constitution. *See, e.g.*, *Hamdan v. Rumsfeld*, 126 S. Ct. 2749, 2773 (2006) ("Congress [cannot intrude] upon the proper authority of the President . . . . Congress cannot direct the conduct of campaigns . . . .") (quoting *Ex parte Milligan*, 71 U.S. (4 Wall.) 2, 139-40 (1866) (Chase, C.J., concurring in judgment)); *Morrison v. Olson*, 487 U.S. 654, 691 (1988) (explaining that Congress may not use its legislative authority to "impede the President's ability to perform his constitutional duty"); *Milligan*, 71 U.S. (4 Wall.) at 139 (Chase, C.J., concurring in judgment) (Congress many not "*interfere*[] *with the command of forces and the conduct of campaigns.* That power and duty belong to the President as commander-in-chief.") (emphasis added). As we have stated, it is well established that the President has constitutional authority to conduct electronic surveillance without prior judicial approval for the purpose of collecting foreign intelligence. *See In re Sealed Case*, 310 F.3d 717, 742 (For. Intel. Surv. Ct. Rev. 2002); *United States v. Truong Dinh Hung*, 629 F.2d 908, 913-17 (4th Cir. 1980); *United States v. Butenko*, 494 F.2d 593, 602-06 (3d Cir. 1974) (en banc); *United States v. Brown*, 484 F.2d 418, 425-27 (5th Cir. 1973); *United States v. bin Laden*, 126 F. Supp. 2d. 264, 271-77 (S.D.N.Y. 2000). FISA cannot eliminate the President's constitutional authority to conduct foreign intelligence surveillance without prior judicial approval against a hostile foreign power. *See In re Sealed Case*, 310 F.3d at 742. Accordingly, the proffered interpretation of the "exclusive means" provision of FISA risks a constitutional clash between the Executive Branch and Congress. *See Legal Authorities Supporting the Activities of the National Security Agency Described by the President* at 19-23 (Jan. 19, 2006) ("*Legal Authorities*"). We believe that FISA must be interpreted, if "fairly possible," to avoid raising these serious constitutional concerns. *See INS v. St. Cyr*, 533 U.S. 289, 299-300 (2001) (citations omitted); *Ashwander v. TVA*, 297 U.S. 288, 345-48 (1936) (Brandeis, J., concurring). This canon of constitutional avoidance has particular importance in the realm of national security, where the President's constitutional

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00113 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.060

authority is at its highest. *See Department of Navy v. Egan*, 484 U.S. 518, 527, 530 (1988); William N. Eskridge, Jr., *Dynamic Statutory Interpretation* 325 (1994) (describing "[s]uper-strong rule against congressional interference with the President's authority over foreign affairs and national security").

- **Do you agree that the inclusion of this language in the FISA statute will increase the likelihood that a Court will find the warrantless wiretapping program to be constitutional?**

ANSWER: We believe that the Terrorist Surveillance Program was constitutional. Amending FISA to include a provision stating that "[n]othing in [the] Act shall be construed to limit the constitutional authority of the President to collect intelligence with respect to foreign powers and agents of foreign powers" should not affect the constitutional analysis of the Terrorist Surveillance Program. As the Attorney General stated, the inclusion of such a statement in the legislation would simply recognize that FISA is not intended to affect those presidential authorities that Congress cannot constitutionally take away.

Such a reading is strongly supported by the Supreme Court's decision in *United States v. United States District Court* ("*Keith*"), 407 U.S. 297 (1972), which construed a similar provision then codified at 18 U.S.C. § 2511(3), involving the issuance of wiretap orders in criminal cases, which stated that "[n]othing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect [against specified dangers]." The Court wrote:

> At most, this is an implicit recognition that the President does have certain powers in the specified areas. Few would doubt this, as the section refers—among other things—to protection 'against actual or potential attack or other hostile acts of a foreign power.' But so far as the use of the President's electronic surveillance power is concerned, *the language is essentially neutral.*
>
> *Section 2511(3) certainly confers no power*, as the language is wholly inappropriate for such a purpose. It merely provides that the Act shall not be interpreted to limit or disturb such power as the President may have under the Constitution. *In short, Congress simply left presidential powers where it found them.*

Keith, 407 U.S. at 307 (emphases added). Therefore, we do not believe that proposed section 801 of FISA would have affected the analysis under the three-part framework established by Justice Jackson's concurring opinion in *Youngstown Steel*.

- **Given the established *Youngstown* framework for establishing the constitutionality of a presidential action, is the Attorney General's assertion that this clause "does not change the status quo" correct?**

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00114 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.061

ANSWER: Yes. A statute, such as FISA, cannot eliminate the President's constitutional authority to conduct electronic surveillance without prior judicial approval of a foreign enemy, especially a hostile foreign power that has already struck within the United States. *See In re Sealed Case*, 310 F.3d 717, 742 (For. Intel. Surv. Ct. Rev. 2002). Proposed section 801 of FISA simply would have clarified that Congress did not intend to limit the authority the President has under the Constitution to collect foreign intelligence, thus avoiding a serious constitutional dispute regarding whether FISA encroaches upon the President's inherent authority under the Constitution.

50. In *Hamdan*, the Supreme Court explained that even if the President has "independent power, absent congressional authorization, to convene military commissions," he still "may not disregard limitations that Congress has, in the proper exercise of its own war powers, placed on his powers." 126 S. Ct. 2774 n.23. In a letter to Congress, thirteen of the nation's leading constitutional scholars indicate that, absent future congressional action, this language "strongly supports the conclusion that the President's NSA surveillance program is illegal."

Even ardent defenders of the program's legality, such as legal scholar Cass Sunstein, have acknowledged that, "after *Hamdan*, the NSA surveillance program, while still not entirely indefensible, seems to be on very shaky ground, and it would not be easy to argue on its behalf in light of the analysis in *Hamdan*."

Questions:

- **Do you disagree with the assessment of these leading constitutional scholars on the constitutionality of the NSA wiretapping program under the status quo? If so, please explain why. In your answer, please cite specific authorities supporting your legal position.**

ANSWER: Yes. As we have stated repeatedly, we believe that the Supreme Court's decision in *Hamdan v. Rumsfeld* does not undermine the analysis set forth in the Department's *Legal Authorities* paper outlining the legal basis for the Terrorist Surveillance Program, assuming that the Program involved "electronic surveillance." First, the relevant statutory scheme at issue in *Hamdan* is fundamentally different from the one potentially implicated by the Terrorist Surveillance Program. FISA expressly contemplates that Congress may authorize electronic surveillance through a subsequent statute without amending FISA. *See* 50 U.S.C. § 1809(a)(1) (prohibiting electronic surveillance "except as authorized by statute"). The primary provision at issue in *Hamdan*, Article 21 of the Uniform Code of Military Justice ("UCMJ"), has no analogous provision. Moreover, the Supreme Court recognized in *Hamdi v. Rumsfeld*, 542 U.S. 519 (2004), that the Force Resolution satisfies a statute similar to FISA prohibiting detention of U.S. citizens "except pursuant to an Act of Congress." 18 U.S.C. § 4001(a). Because the Terrorist Surveillance Program

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00115 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.062

implicated a statutory regime analogous to the one at issue in *Hamdi*, we believe that the reasoning of that decision is more relevant to the Program than *Hamdan*.

Second, the UCMJ expressly deals with the Armed Forces and armed conflicts and wars. By contrast, Congress left open the question of what rules should apply to electronic surveillance during wartime. *See Legal Authorities* at 25-27 (explaining that the underlying purpose behind FISA's declaration of war provision, 50 U.S.C. § 1811, was to allow the President to conduct electronic surveillance outside FISA procedures while Congress and the Executive Branch would work out rules applicable to the war). It therefore is more natural to read the Force Resolution to supply the additional electronic surveillance authority contemplated by section 1811 specifically for the armed conflict with al Qaeda than it is to read the Force Resolution as augmenting the authority of the UCMJ, which, as noted, is intended to continue to apply for the duration of any armed conflict or war. Indeed, there is a long tradition of interpreting force resolutions to confirm and supplement the President's constitutional authority in the particular context of surveillance of international communications. *See Legal Authorities* at 16-17 (describing examples of Presidents Wilson and Roosevelt); *cf. id.* at 14-17 (describing long history of warrantless intelligence collection during armed conflicts).

Third, Congress's legislative authority is clearer with respect to the issues in *Hamdan* than is the case here. Under the Constitution, both the Executive Branch and Congress have authority with respect to national security and armed conflict. Congress has express constitutional authority to "define and punish . . . Offenses against the Law of Nations," U.S. Const. Art. I, § 8, cl. 10, and to "make Rules for the Government and Regulation of the land and naval forces," *id.* cl. 14. Because of these explicit textual grants, Congress's authority is at a maximum in these areas, which have obvious applicability to the military commissions at issue in *Hamdan*. But there is no similarly clear expression in the Constitution of congressional power to regulate the President's authority to collect foreign intelligence necessary to protect the Nation, particularly during times of armed conflict. *See Legal Authorities* at 30-34. Indeed, in *Hamdan*, the Court expressly recognized the President's *exclusive* authority to direct military campaigns. *See* 126 S. Ct. at 2773 (quoting *Ex parte Milligan*, 71 U.S. (4 Wall.) 2, 139 (1866) ("Congress cannot direct the conduct of campaigns.") (Chase, C.J., concurring in judgment)). Quoting Chief Justice Chase, the Court affirmed that each power vested in the President "'includes all authorities essential to its due exercise.'" *Id.* As explained in detail in our *Legal Authorities* paper, foreign intelligence collection is a fundamental and traditional component of conducting military campaigns. Therefore, under the reasoning adopted by *Hamdan*, the Terrorist Surveillance Program—which the President determined was essential to protecting the Nation and to conducting the campaign against al Qaeda—fell squarely within the President's constitutional authority. Moreover, nothing in *Hamdan* calls into question the uniform conclusion of *every* federal appellate court to have decided the issue that the President has constitutional authority to collect foreign intelligence information within the United States, consistent with the Fourth Amendment. *See, e.g.*, *In re Sealed Case*, 310 F.3d 717, 742 (For. Intel. Surv. Ct. Rev. 2002) ("[A]ll the

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00116 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.063

other courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information.").

Fourth, the Government did not argue in *Hamdan*, and the Court did not decide in that case, that the UCMJ would be unconstitutional as applied if it were interpreted to prohibit Hamdan's military commission from proceeding. *See* 126 S. Ct. at 2774 n.23. In order to sustain this argument, the Court would have had to conclude that the UCMJ, so interpreted, unduly interfered with "the President's ability to perform his constitutional duty." *Morrison v. Olson*, 487 U.S. 654, 691 (1988); *see also id.* at 696-97. Such a showing would be considerably easier in the context of the Terrorist Surveillance Program, where speed and agility are so essential to the defense of the Nation.

Finally, the Government did not contend in *Hamdan* that the UCMJ must be interpreted, if "fairly possible," to avoid raising serious constitutional concerns. *INS v. St. Cyr*, 533 U.S. 289, 299-300 (2001) (citations omitted); *Ashwander v. TVA*, 297 U.S. 288, 345-48 (1936) (Brandeis, J., concurring). This canon of constitutional avoidance has particular importance in the realm of national security, where the President's constitutional authority is at its highest. *See Department of Navy v. Egan*, 484 U.S. 518, 527, 530 (1988); William N. Eskridge, Jr., *Dynamic Statutory Interpretation* 325 (1994) (describing "[s]uper-strong rule against congressional interference with the President's authority over foreign affairs and national security"). Although we believe that FISA is best interpreted to allow statutes such as the Force Resolution to authorize electronic surveillance outside traditional FISA procedures, this interpretation is at least "fairly possible," and, in view of the very serious constitutional questions that otherwise would be presented, therefore must be accepted under the canon of constitutional avoidance. *See Legal Authorities* at 28-36.

- **Without this enabling legislation, do you agree with program supporters like Professor Sunstein who believe the program is likely to be adjudicated unconstitutional?**

ANSWER: No. As explained above, we continue to believe that the Terrorist Surveillance Program was constitutional.

51. During his questioning of you, Senator Specter claimed that "no statute, including the one I have proposed, can expand or contract the President's Article II powers." This is clearly incorrect, since a statute that represents a lawful exercise of Congress' powers can circumscribe the President's powers. You acknowledged this when you told Senator Specter that "statutes can reasonably regulate exercises of the President's constitutional authority," and again in a response to Senator Leahy on this same issue.

Questions:

- **Please provide us with any additional information you can on the**

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00117 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.064

circumstances under which the President's Article II powers can be or have been circumscribed by statute.

- **In cases where there is a direct conflict between Congress' constitutional exercise of its power and the Executive's constitutional exercise of its power, what is the test that is used to determine which action prevails?**
- **Should courts be called upon to resolve these sorts of inter-branch conflicts? If the Supreme Court is not allowed to be the final arbiter of constitutionality in these cases, what check does Congress have on an Executive Branch that can simply ignore the laws that Congress passes?**

ANSWER: These questions raise complex issues that depend heavily upon the context and constitutional provisions involved. As Justice Jackson noted, these issues are difficult to evaluate in the abstract. *See Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635 (1952) (Jackson, J., concurring) ("The actual art of governing under our Constitution does not and cannot conform to judicial definitions of power of any of its branches based on isolated clauses or even single Articles torn from context."). Generally speaking, however, Congress may not use its legislative authority to usurp "Executive Branch functions," *Bowsher v. Synar*, 478 U.S. 714, 727 (1986); nor may it "impede the President's ability to perform his constitutional duty," *Morrison v. Olson*, 487 U.S. 654, 691 (1988).

Among the President's most basic constitutional duties is his duty to protect the Nation from armed attack. The Constitution gives him all necessary authority to fulfill that responsibility. Hence, the courts have long acknowledged the President's inherent authority to take action to protect the Nation from attack, *see, e.g.*, *The Prize Cases*, 67 U.S. (2 Black) 635, 668 (1863), and to protect Americans abroad, *see, e.g.*, *Durand v. Hollins*, 8 F. Cas. 111, 112 (C.C.S.D.N.Y. 1860) (No. 4186). *See generally Ex parte Quirin*, 317 U.S. 1, 28 (1942) (recognizing that the President has authority under the Constitution "to direct the performance of those functions which may constitutionally be performed by the military arm of the nation in time of war," including "important incident[s] to the conduct of war," such as "the adoption of measures by the military command . . . to repel and defeat the enemy"). As the Supreme Court emphasized in the *Prize Cases*, if the Nation is invaded, the President is "bound to resist force by force"; "[h]e must determine what degree of force the crisis demands" and need not await congressional sanction to do so. 67 U.S. at 670; *see also Campbell v. Clinton*, 203 F.3d 19, 27 (D.C. Cir. 2000) (Silberman, J., concurring) ("[T]he *Prize Cases* . . . stand for the proposition that the President has independent authority to repel aggressive acts by third parties even without specific congressional authorization, and courts may not review the level of force selected."); *id.* at 40 (Tatel, J., concurring) ("[T]he President, as commander in chief, possesses emergency authority to use military force to defend the nation from attack without obtaining prior congressional approval."). The President's authority is at its zenith in defending the Nation from attack and in conducting campaigns during time of armed conflict, and, accordingly, Congress's ability to regulate such efforts is sharply circumscribed. As then-Attorney General Robert H. Jackson observed, "in virtue of

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00118 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.065

his rank as head of the forces, [the President] has certain powers and duties with which Congress cannot interfere." *Training of British Flying Students in the United States*, 40 Op. Att'y Gen. 58, 61 (1941) (internal quotation marks omitted); *accord Hamdan v. Rumsfeld*, 126 S. Ct. 2749, 2773 (2006) ("'Congress [cannot intrude] upon the proper authority of the President . . . . Congress cannot direct the conduct of campaigns'") (quoting *Ex parte Milligan*, 71 U.S. (4 Wall.) 2, 139-40 (1866) (Chase, C.J., concurring in judgment)).

Wherever possible, a statute purporting to regulate the Executive's constitutional authority must be construed to avoid a serious constitutional question. *See INS v. St. Cyr*, 533 U.S. 289, 299-300 (2001) ("[I]f an otherwise acceptable construction of a statute would raise serious constitutional problems, and where an alternative interpretation of the statute is 'fairly possible,' we are obligated to construe the statute to avoid such problems.") (citations omitted). This canon of constitutional avoidance has particular importance in the realm of national security, where the President's constitutional authority is at its highest. *See Department of the Navy v. Egan*, 484 U.S. 518, 527, 530 (1988); William N. Eskridge, Jr., *Dynamic Statutory Interpretation* 325 (1994) (describing "[s]uper-strong rule against congressional interference with the President's authority over foreign affairs and national security").

Where a direct conflict does occur in the context of a case or controversy, it may be appropriate for the courts to resolve the dispute. *See, e.g.*, *Youngstown*, 343 U.S. at 584. There are several judicial doctrines, however, that may, depending on the circumstances, prevent the courts from intervening in some such disputes, such as the political question doctrine. *See, e.g.*, *Baker v. Carr*, 369 U.S. 186, 208-37 (1962) (discussing political question doctrine); *Chicago & S. Air Lines, Inc. v. Waterman S.S. Corp.*, 333 U.S. 103, 111 (1948) ("[T]he very nature of executive decisions as to foreign policy is political, not judicial . . . . They are decisions of a kind for which the Judiciary has neither aptitude, facilities nor responsibility and which has long been held to belong in the domain of political power not subject to judicial intrusion or inquiry."). Moreover, under the doctrine of state-secrets privilege, courts must decline to entertain certain cases concerning sensitive national security secrets, the disclosure of which could be harmful to national security. *See United States v. Reynolds*, 345 U.S. 1, 7-8 (1953); *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C. Cir. 1983).

Even when judicial review is not appropriate, Congress has other avenues available that can serve as a check on executive action. Under no circumstances, however, has this Administration "simply ignore[d]" laws enacted by Congress.

52. You have argued that one benefit of this legislation is that it provides "a very good mechanism" for reviewing the constitutionality of the warrantless wiretapping program. However, as you acknowledged, dozens of cases pending around the country "have challenged various versions of what has been alleged in the media." At the hearing, you said that you "do not think those disparate

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00119 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.066

matters in litigation in various district courts around the country [are] an effective or appropriate way for any of these determinations to be made."

The federal civil justice system is the primary mechanism through which almost all constitutional challenges to legislation are adjudicated. Established procedures exist for handling classified information in a civil law context.

Questions:

- **What is ineffective about allowing the normal federal court system to handle these cases?**
- **What is inappropriate about allowing the normal federal court system to handle these cases?**
- **If judicial review of the program is supported by the administration, and the civil courts are ill-equipped to address these cases, will the Administration endorse a stand-alone statute that transfers jurisdiction over these cases to the FISA Court of Review? If not, why not?**

ANSWER: As you are aware, on January 10, 2007, a judge of the FISC issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that at least one of the communicants is a member or an agent of al Qaeda or an affiliated terrorist organization. As a result of these orders, any electronic surveillance that may have been occurring as part of the Terrorist Surveillance Program is now subject to the approval of the FISC.

Permitting litigation concerning classified communications intelligence activities in the federal district courts around the country raises significant national security concerns. A single court decision concerning a classified communications intelligence activity may have immediate, nationwide ramifications. For example, a decision that holds an intelligence activity illegal could, either temporarily or permanently, end that activity. Intelligence programs that are essential to national security should not be subject to a variety of potentially inconsistent decisions from federal district courts across the country. Consolidating litigation concerning highly classified communications intelligence activities before a single expert court would ensure uniformity in this critically important area of law.

Also, cases concerning intelligence activities often involve very sensitive classified information and highly technical issues. Recognizing those facts, Congress established the FISC and the Court of Review as specialized courts to address these complex issues and to do so with the appropriate facilities and expertise for handling such information. Unlike regular district courts, the FISC has specialized security procedures and secure facilities that are optimized for considering questions regarding highly sensitive intelligence issues. *Cf. Alfred A. Knopf, Inc. v. Colby*, 509 F.2d 1362, 1369 (4th Cir. 1975) ("It is not to slight judges, lawyers or anyone else to suggest that any such disclosure carries with it serious risk that highly sensitive

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00120 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.067

information may be compromised. In our own chambers, we are ill equipped to provide the kind of security highly sensitive information should have."). At the same time, the judges of the FISC are Article III judges, who have the same experience handling adversary proceedings that every other federal judge has, but who also have experience deciding legal issues relating to intelligence collection and handling classified information. In addition, even if all federal district court judges had the necessary facilities and experience (which they do not), litigating such issues in dozens of courts across the country obviously increases the risks of inadvertent disclosures. For all of these reasons, the Administration supports amendments to FISA that would permit the transfer of cases challenging the legality of classified communications intelligence activities to the FISC and has proposed such amendments as part of its proposed FY 2008 Intelligence Authorization Act.

53. In the report of the American Bar Association Task Force on Domestic Surveillance, the ABA urged Congress to conduct a thorough, comprehensive investigation to determine:

a) the nature and extent of electronic surveillance of U.S. persons conducted by any U.S. government agency for foreign intelligence purposes that does not comply with FISA;
b) what basis or bases were advanced (at the time it was initiated and subsequently) for the legality of such surveillance;
c) whether the Congress was properly informed of and consulted as to the surveillance; and
d) the nature of the information obtained as a result of the surveillance and whether it was retained or shared with other agencies.

Questions:

- **What is your response to the recommendations and conclusions of the ABA Taskforce on Domestic Surveillance?**
- **Why can't such an inquiry be conducted, so that legislation is well-informed and tailored to address any deficiencies in current law?**

ANSWER: As you are aware, on January 10, 2007, a judge of the FISC issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that at least one of the communicants is a member or an agent of al Qaeda or an affiliated terrorist organization. As a result of these orders, any electronic surveillance that may have been occurring as part of the Terrorist Surveillance Program now is subject to the approval of the FISC. Under these circumstances, the President determined not to reauthorize the Terrorist Surveillance Program when the last authorization expired. The Attorney General informed both the House Committee on the Judiciary and the Senate Judiciary Committee of these developments by letter on January 17, 2007.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00121 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.088

Furthermore, the Department of Justice and the Intelligence Community have provided extensive information to Congress about the Terrorist Surveillance Program. Every member of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence was briefed on the Program. Under the National Security Act and longstanding practice, these are the appropriate Committees to address such issues.

Moreover, in the past year, the Attorney General, attorneys from the Department of Justice, the Director of the CIA General Hayden, the Director of the NSA General Alexander, and other officials have participated in numerous congressional hearings, briefings, and discussions, written more than a dozen letters to Congress about the Program, and answered hundreds of questions for the record. In addition, in January 2006, the Department of Justice released the *Legal Authorities* paper presenting a detailed analysis of the legal basis for the Program, even assuming that it involved electronic surveillance as defined by FISA. For these reasons, we believe that Congress has ample information to make informed decisions regarding legislation that would streamline and modernize FISA. As always, we are willing to meet with appropriate Members and staff to provide additional assistance.

Questions from Sen. Feinstein

54. Background. In the 95th Congress back in 1978, language was eliminated from the 1968 Title III wiretap statute that expressly recognized the constitutional power of the President. It was replaced it with the current requirement that FISA "shall be the exclusive means" for conducting such surveillance.

In considering FISA in 1978, Congress also refused to enact language proposed by the Ford Administration that "[n]othing contained in this chapter shall limit the constitutional power of the President."

However, the Specter-White House bill now before us states, "Nothing in this Act shall be construed to limit the constitutional authority of the President to collect intelligence with respect to foreign powers and agents of foreign powers." The bill also contains other references authorizing unspecified actions "under the Constitution."

- ***In your opinion, what is the impact of having this language in the bill?***

ANSWER: Please see my answers to Questions 28 and 49.

55. Background. In the 1952 *Youngstown* case, Justice Jackson divided Presidential action into three areas:

1. **When the President acts consistent with the will of Congress;**
2. **When the President acts in an area in which Congress has not expressed itself; and**

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00122 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.069

3. When the President acts in contravention of the will of Congress.

In the first circumstance, Presidential power is at it greatest, in the third, Presidential power is at its lowest. Justice Jackson wrote that:

"When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter."

- ***In your opinion, how will the new Specter bill be analyzed in a Youngstown analysis given the deletion of the "exclusivity" language in FISA and with the addition of new language about the President's ability to act under the constitution?***

ANSWER: Please see my answer to Question 49.

- ***What legal limits, if any, would exist on the President's ability to conduct electronic surveillance for foreign intelligence without following FISA if we pass the new Specter bill?* Please answer according to what are the legal restrictions that the Specter bill places on the President, not what DOJ or the President may or may not do.**

ANSWER: This question concerns S. 2453, which was introduced in the 109th Congress. S. 2453 has not been introduced in this Congress. We are not aware of any legislation currently under consideration in this Congress, including the Administration's proposed FY 2008 Intelligence Authorization Act, that contains amendments to FISA similar to the provisions in S. 2453 to which you refer in this Question and in Question 54.

56. Background. Sen. Specter's new FISA bill eliminates the 15-day window on surveillance outside of FISA after a declaration of war. This could be interpreted to mean that after a declaration of war the President may unilaterally wiretap whomever he chooses until the end of the war without limitation.

While wars do not have specific end dates, usually there is some identifying action that signals the end – such as surrender of one party, annexation of a territory under dispute, a peace treaty, when one party unilaterally withdraws, etc. However, in the "war on terror" it is highly unlikely that there would be a similar triggering event that would signify the end.

- ***If the new Specter bill were to pass, how long would the President's authority last under the "war on terror"? Could it last decades? When would that authority end?***

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00123 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.070

ANSWER: This question concerns certain provisions of S. 2453, which was introduced in the 109th Congress. S. 2453 has not been reintroduced in this Congress, and we are aware of no current legislative proposal that incorporates these provisions of S. 2453.

We note, however, that we have never suggested that the President's authority to conduct foreign intelligence surveillance is without limit, as this question implies. The Terrorist Surveillance Program, for example, was narrowly focused, targeting for collection only international communications into or out of the United States where there was probable cause to believe that at least one of the communicants was a member or agent of al Qaeda or an affiliated terrorist organization.

57. Background. Under the new Specter-Administration bill, a new blanket exception would be created to the FISA warrant requirement, allowing surveillance of anyone who is inside the United States but is not a U.S. person. Under the bill, such individuals could be wiretapped for up to a year upon a declaration by the Attorney General that they possess foreign intelligence information.

- ***Does "foreign intelligence" include economic trends overseas? What else does it include? Trade policies between the U.S. and another country? The strength of the dollar in another country? Currency valuations? Foreign stock prices and market fluctuations?***

ANSWER: FISA defines "foreign intelligence information" to include information relating to "grave hostile acts," "sabotage or international terrorism," or "clandestine intelligence activities" directed against the United States by a foreign power or one of its agents, or information concerning "national defense or . . . security" or the "conduct of foreign affairs." *See* 50 U.S.C. § 1801(e). Although the need to protect sensitive intelligence sources and methods prohibits a full discussion of the precise scope of these terms in this setting, these terms are well-defined in practice. Moreover, with regard to a United States person, such information is "foreign intelligence information" only if it is "necessary to protect against" such acts (sabotage, terrorism, or clandestine activities) or is "necessary to" national defense or security or the conduct of foreign affairs. *Id.*

58. It appears that this new Specter bill would authorize wiretapping of almost any individual in the United States who is not a U.S. person so long as this certification is made by the Attorney General.

- ***Is that correct? What are the limitations to such a broad authority?***

- ***How would this section affect foreign workers – including skilled workers on H-1-B visas – that U.S. companies routinely bring into the United States every day? If the Attorney General certified that a skilled worker possessed foreign intelligence, would this bill allow the Government to wiretap that worker while***

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00124 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.071

he is here in the U.S.? Would this include all of his calls or emails with other U.S. corporate executives or other persons – without a FISA warrant or other court oversight?

ANSWER: This is not correct. The authority you reference emphatically would not have applied to "almost any individual in the United States who is not a U.S. person." In any event, this question concerns certain provisions of S. 2453, which was introduced in the 109th Congress. S. 2453 has not been reintroduced in this Congress, and we are not aware of any current legislative proposal incorporating this specific provision of S. 2453. The Administration supports modernization of FISA, including section 102 of FISA and has offered specific amendments to that end in its proposed FY 2008 Intelligence Authorization Act. We would be happy to answer the Committee's questions about the provisions in the Administration's new Intelligence Authorization proposal.

59. **Background. Several of us in Congress – and especially those of us serving on the Intelligence Committees – were surprised and disappointed that we had to learn of the so-called Terrorist Surveillance Program from the *New York Times*. Since then, we have read reports about other programs as well.**

A May 12, 2006 *USA Today* story, reporting on the NSA's apparent collection of millions or even billions of telephone records from major carriers, has been denied by some carriers but not others. Last week, it was revealed that Republican House Intelligence Chairman Hoekstra had sent a letter to the Administration complaining of another program that had not been disclosed to his committee. And in earlier testimony, the Administration has alluded to the possibility, but did not confirm, that other intelligence programs could exist.

- ***Are there any intelligence programs carried out by your agencies, or otherwise within the intelligence community that you know of, that have not been briefed to the Congressional intelligence committees?***

- ***Did anyone in the Administration offer, grant or otherwise provide in any way some sort of promise of immunity or offer of protection against civil or criminal liability to telecommunications or internet service provider or financial entities or any other company for their cooperation in any of the surveillance programs? If yes, under what legal authority?***

ANSWER: We can neither confirm nor deny in this setting any asserted intelligence activities or any aspects of such activities. Our inability to discuss such asserted programs in this setting should not be taken as an indication that any such programs exist. Consistent with the reporting requirements of the National Security Act and long-standing practice, the Executive Branch notifies Congress of the classified intelligence activities of the United States through appropriate briefings.

Questions from Sen. Feingold

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00125 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.072

Following are questions regarding the July 25, 2006, version (marked "JEN06974") of Senator Specter's bill, which was originally introduced as S. 2453. Please respond to the greatest degree possible in an unclassified setting, and please endeavor to provide any classified answers at a clearance level that will allow at least some cleared Judiciary Committee staff to review the responses.

60. The Specter bill makes a number of changes to the existing FISA statute. In reviewing these changes to the statute, it would of course be helpful to know how the FISA court has interpreted it. Please provide copies of any FISA court decisions containing legal interpretations of provisions of FISA that are amended by the Specter bill.

ANSWER: As you are aware, on January 10, 2007, a judge of the FISC issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that at least one of the communicants is a member or agent of al Qaeda or an affiliated terrorist organization. Pursuant to an agreement with the House and the Senate, the Department agreed to provide limited access to the orders of the FISC and related documents to certain Members of the House and the Senate and to certain staff members. As we noted at the time, this arrangement is extraordinary, providing Congress with unprecedented access to FISC documents.

61. At the hearing, General Hayden stated that Section 9 of the Specter bill originated at the NSA. Please explain with regard to each subsection of the Specter bill, including each subsection of Section 9, the degree to which you or anyone at your agency/department had input on it, and to the extent not addressed in the answers to the questions below, whether you support it.

ANSWER: The Department of Justice reviewed and provided technical assistance for several bills designed to modernize FISA, including S. 2453. We continue to believe that FISA must be modernized. For this reason, the Administration has suggested specific, critical amendments to FISA in its proposed FY 2008 Intelligence Authorization Act, which has been introduced in this Congress.

62. The Specter bill creates a new Title VII of FISA. Under this title, the FISA court would be granted the authority to issue program warrants. Under the bill, would the government ever be <u>required</u> by the statute to seek a warrant from the FISA court to engage in an existing or future electronic surveillance program?

ANSWER: This question concerns certain provisions of S. 2453, which was introduced in the 109th Congress. S. 2453 has not been reintroduced in this Congress, and we are not aware of any current legislative proposal incorporating these provisions of S. 2453.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00126 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.073

63. Please explain your understanding of the interplay in the new Title VII of FISA created by the Specter bill of the section 701 definitions of "electronic communication," "electronic tracking," and "electronic surveillance program." Also explain how those definitions vary from the definition of "electronic surveillance" in existing FISA Title I.

ANSWER: This question concerns certain provisions of S. 2453, which was introduced in the 109th Congress. S. 2453 has not been reintroduced in this Congress, and we are not aware of any current legislative proposal incorporating these provisions of S. 2453.

64. In the Specter bill, the newly inserted section 701(6) defines "foreign intelligence information" as having the same meaning as the current statute, but also adds "and includes information necessary to protect against international terrorism." Given the definitions already in the FISA statute, isn't this additional language just duplicative?

ANSWER: This question concerns proposed section 701(6) of FISA, which was introduced as part of S. 2453 in the 109th Congress. S. 2453 has not been reintroduced in this Congress, and we are not aware of any current legislative proposal incorporating these provisions of S. 2453.

65. The current FISA statute defines "contents" as "any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication." The Specter bill, in creating the new Title VII, uses the term "substance" rather than "contents." It defines "substance" as "any information concerning the symbols, sounds, words, purport, or meaning of a communication, and does not include dialing, routing, addressing, or signaling." Please discuss whether you believe this alternate definition is necessary and if so, why. Please also discuss how you believe this alternate definition varies from the new definition of "contents" that Section 9 of the Specter bill would create in the existing FISA Title I.

ANSWER: Part of this question concerns certain provisions of S. 2453, which was introduced in the 109th Congress, creating a new Title VII of FISA. S. 2453 has not been reintroduced in this Congress, and we are not aware of any current legislative proposal incorporating these provisions of S. 2453. With regard to the proposed revision to the definition of "contents" in Title I of FISA, please see my answer to Question 35.

66. In the Specter bill's new section 702, the FISA Court is given jurisdiction to issue an order authorizing an electronic surveillance program "to obtain foreign intelligence information or to protect against international terrorism." The Administration has publicly described the NSA program as involving communications where there is a reasonable basis to believe that one party to the

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00127 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.074

communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda.

a. Do you agree that the bill authorizes program warrants "to obtain foreign intelligence information" even when there is no connection to al Qaeda, and that this is broader even than what the President has stated he has authorized?

b. Do you agree that the bill authorizes program warrants "to obtain foreign intelligence information" even when there is no connection to terrorism, and that this is broader even than what the President has stated he has authorized?

ANSWER: These questions concern certain provisions of S. 2453, which was introduced in the 109th Congress, creating a new Title VII of FISA. S. 2453 has not been reintroduced in this Congress, and we are not aware of any current legislative proposal incorporating these provisions of S. 2453.

67. In the Specter bill's new section 702, the FISA Court's initial authorization of an "electronic surveillance program" cannot be for longer than 90 days, but a re-authorization can be for as long as the court determines is "reasonable." What do you believe is the justification, if any, for not limiting reauthorization to 90 days?

ANSWER: These questions concern certain provisions of S. 2453, which was introduced in the 109th Congress, creating a new Title VII of FISA. S. 2453 has not been reintroduced in this Congress, and we are not aware of any current legislative proposal incorporating these provisions of S. 2453.

68. The Specter bill's new section 702(b) establishes guidelines for mandatory transfers of cases to the FISA Court of Review, and refers to "any case before any court." Do you believe that these mandatory transfer provisions would apply to pending cases?

ANSWER: These questions concern certain provisions of S. 2453, which was introduced in the 109th Congress, creating a new Title VII of FISA. S. 2453 has not been reintroduced in this Congress, and we are not aware of any current legislative proposal incorporating these provisions of S. 2453.

69. In the Specter bill's new section 702(b), the mandatory transfer provision applies to any case "challenging the legality of classified communications intelligence activity relating to a foreign threat, including an electronic surveillance program, or in which the legality of any such activity or program is in issue." "Electronic surveillance program" is defined in the bill, but there is no definition in the current FISA statute or in the Specter bill of a "classified communications intelligence activity." What do you read this term to mean, and what types of cases beyond those involving "electronic surveillance programs" do you believe would be covered by this term?

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00128 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.075

ANSWER: We believe that the term "classified communications intelligence activities" has a clear and limited meaning. We cannot, however, give examples of such activities in this setting, because providing such examples could reveal highly classified and exceptionally sensitive information concerning intelligence sources and methods. We would be willing to provide further information concerning the scope of the term to Members of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence in an appropriate classified setting.

70. In the Specter bill's new section 702(b), the mandatory transfer provision, cases are transferred to the FISA Court of Review "for further proceedings under this subsection." But, there is no subsection defining the procedures for the FISA Court of Review's "further proceedings," as there was in prior versions of the bill.

a. Did you or anyone at your agency/department request or suggest that the paragraph in earlier versions of the bill entitled "Procedures for Review" be removed? If so, why?

b. As you read this subsection, what relief would the FISA Court of Review have the authority to grant if it found that the program at issue were illegal?

c. As you read this subsection, what role would the parties challenging the program play in the FISA Court of Review proceedings?

ANSWER: These questions concern the transfer provisions of S. 2453. S. 2453 was introduced in the 109th Congress, and has not been reintroduced in this Congress. We are not aware of any current legislative proposal that would transfer cases to the Foreign Intelligence Surveillance Court of Review.

71. The Specter bill's new section 702(b)(3) preserves "all litigation privileges" for any case transferred to the FISA Court of Review.

a. Do you read this as being intended to cover the state secret privilege?

b. If so, has the state secrets privilege ever before been invoked in the FISA court? Why would it be necessary to invoke the state secrets privilege in a court that operates in a one-sided, secret process?

ANSWER: Although S. 2453 is no longer pending before Congress, the Administration has proposed a similar amendment in the 110th Congress as part of its proposed FY 2008 Intelligence Authorization Act. The Administration's Intelligence Authorization proposal would preserve "all litigation privileges" in any case transferred to the FISC, as well as in any appeal to the Court of Review from a judgment of the FISC in a transferred case.

We would interpret the preservation of "all litigation privileges" to include the state-secrets privilege. The "well established" state-secrets privilege serves the essential function of allowing the Government to protect against the discovery of information in litigation, the disclosure of which could be harmful to national

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00129 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.076

security. *See United States v. Reynolds*, 345 U.S. 1, 7-8 (1953); *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C. Cir. 1983). To date, there has been no need to invoke the privilege in the FISC, due to its limited jurisdiction and the nature of proceedings before it. In the event that adversary litigation were transferred to the FISC or the Foreign Intelligence Surveillance Court of Review from the federal district courts, it might be necessary for the Government to assert the state-secrets privilege. Notwithstanding the FISC's special procedures and secure facilities, it is possible that in adversary proceedings other parties could disclose classified information if they were to obtain access to it. Moreover, the privilege protects more than the disclosure of information to other litigants. In appropriate cases, the privilege operates to prevent disclosure even to the court.

72. The Specter bill repeals sections 111, 309, and 404 of the FISA statute, which, notwithstanding any other law, give the President the authority to use electronic surveillance, physical searches, or pen registers or trap and trace devices without a court order for up to fifteen days following a declaration of war by Congress. Does the Administration support this repeal of these provisions, which on their face appear to grant additional surveillance options to the executive branch in time of war? If so, why?

ANSWER: These questions concern certain provisions of S. 2453, which was introduced in the 109th Congress. S. 2453 has not been reintroduced in this Congress, and we are not aware of any current legislative proposal containing these provisions.

73. The Specter bill, in section 8(c)(2)(A)(i), inserts "or under the Constitution" in 50 U.S.C. § 1809(a)(1). What is the effect of this amendment to section 1809?

ANSWER: Again, this question relates to provisions of S. 2453 that are not included in any legislation pending before Congress of which we are aware. Nevertheless, such an amendment to 50 U.S.C. § 1809(a)(1) would avoid a serious constitutional issue that would arise if FISA were interpreted to preclude the President from exercising his constitutional authority to collect foreign intelligence. It is well established that the President possesses constitutional authority to conduct foreign intelligence surveillance without prior judicial approval for the purpose of gathering foreign intelligence. *See In re Sealed Case*, 310 F.3d 717, 742 (For. Intel. Surv. Ct. Rev. 2002); *United States v. Truong Dinh Hung*, 629 F.2d 908, 913-17 (4th Cir. 1980); *United States v. Butenko*, 494 F.2d 593, 602-06 (3d Cir. 1974) (en banc); *United States v. Brown*, 484 F.2d 418, 425-27 (5th Cir. 1973); *United States v. bin Laden*, 126 F. Supp. 2d. 264, 271-77 (S.D.N.Y. 2000). A statute, such as FISA, cannot eliminate that constitutional authority. *See In re Sealed Case*, 310 F.3d at 742. Accordingly, revising 50 U.S.C. § 1809(a)(1) would clarify that the conduct of electronic surveillance for the purpose of collecting foreign intelligence pursuant to *either* the President's constitutional authority or a statute is lawful and that FISA should not be construed to infringe upon the constitutional authority of the President.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00130 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.077

74. The Specter bill, in section 8(c)(2)(A)(iii), adds a third category of criminal activity to 50 U.S.C. § 1809(a). This third category is similar to the second category, 1809(a)(2).

a. Please explain your view of the difference between the language of the new 1809(a)(3), "knowingly discloses or uses information obtained under color of law by electronic surveillance ..."; and the language of the existing 1809(a)(2), "discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance ..."

b. Second, the new 1809(a)(3) would add the phrase "in a manner or for a purpose" prior to "authorized." Do you agree with this added language, and if so, why?

c. Third, it ends with the phrase "authorized by law," rather than "authorized by statute" as 1809(a)(2) does, or "authorized by statute or under the Constitution," as the bill would amend 1809(a)(2) to read. Please explain the reason, if any, for not adopting the same phrase as in 1809(a)(2), either in current law or as it would be amended by the bill.

ANSWER: These questions concern provisions of S. 2453, which was introduced in the 109th Congress. S. 2453 has not been reintroduced in this Congress, and we are not aware of any current legislative proposal containing these provisions.

75. The Specter bill, in section 8(c)(2)(B), increases the penalties of violating 50 U.S.C. 1809's criminal prohibitions, both in amount of maximum fines ($10,000 to $100,000) and maximum prison term (five years to fifteen years). Do you support these changes? If so, why do you believe they are justified?

ANSWER: These questions concern provisions of S. 2453, which was introduced in the 109th Congress. S. 2453 has not been reintroduced in this Congress, and we are not aware of any current legislative proposal containing these provisions.

76. The Specter bill, in section 9(b)(1), inserts an additional category into the current FISA statute's definition of a non-U.S. person "agent of a foreign power" – someone who "possesses or is expected to transmit or receive foreign intelligence information within the United States." Given that section 1801(b)(1)(C) of FISA already includes any non-U.S. person engaged in "activities in preparation" of international terrorism, do you believe this added language is necessary? If so, why?

ANSWER: The proposed amendment to the definition of "agent of a foreign power" would improve the Intelligence Community's ability to protect the national security of the United States in circumstances where it is difficult to establish the precise connection of a non-U.S. person to a specific foreign power. That is why the Administration supported this amendment in the 109th Congress and has proposed a similar amendment to FISA in this Congress as part of its proposed FY 2008 Intelligence Authorization Act.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00131 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.078

77. The Specter bill, in section 9(b)(2), modifies section 1801(f) of FISA, defining "electronic surveillance." The opening language of the definition in 1801(f)(1) – "the acquisition by an electronic, mechanical or other surveillance device" – is replaced with "the installation or use of an electronic, mechanical or other surveillance device." Please explain the effect you think this would have on the FISA process, and any reason you see for the change in definitional language.

ANSWER: The proposed changes would modernize the definition of "electronic surveillance" to address changes in telecommunications technology and would make the definition technologically neutral. The redefinition of "electronic surveillance," in combination with other amendments to FISA, would help restore FISA's focus on protecting the privacy of U.S. persons in the United States. The applicability of FISA should not depend on the precise means by which a communication is transmitted or on where or how the communication is intercepted. The redefinition, in combination with other amendments to FISA, would enable the FISC and the Government to focus its limited resources on those applications to conduct electronic surveillance that most directly implicate the privacy of U.S. persons in the United States. The Administration continues to believe that FISA must be modernized and supports nearly identical revisions to section 101(f)(1) of FISA as part of its proposed FY 2008 Intelligence Authorization Act.

78. The Specter bill, in section 9(b)(2), modifies section 1801(f) of FISA, defining "electronic surveillance." The new section 1801(f)(1) would cover only the "intentional collection of information." No such limitation exists in the current 1801(f)(1). Please explain what you think would be the effect of this new limitation.

ANSWER: We disagree with the suggestion that "[n]o [intent] limitation exists in current section 1801(f)(1)." Section 1801(f)(1) explicitly limits that component of the definition of "electronic surveillance" to acquisition of "the contents [of communications that] are acquired by *intentionally* targeting [a] particular, known United States person." (Emphasis added.) In any event, a revised definition of "electronic surveillance" could help to achieve FISA's original purpose, as discussed above. We believe that such a redefinition, in combination with other amendments to FISA, would protect the national security better, and also would have the effect of increasing privacy protections for U.S. persons in the United States. The Administration continues to believe that FISA must be modernized and has proposed similar revisions to the definition of "electronic surveillance" as part of its proposed FY 2008 Intelligence Authorization Act.

79. The Specter bill, in section 9(b)(2), modifies section 1801(f) of FISA, defining "electronic surveillance." The current language in 1801(f)(1) refers to a person "who is in the United States" while the new language refers to a person "who is reasonably believed to be in the United States." Please explain what you think would be the effect of this new language.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00132 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.079

ANSWER: Due to the nature of modern telecommunications, the location of parties to a communication is not always clear. The Intelligence Community ought to be able to rely on reasonable conclusions about the location of particular individuals. Currently, in such circumstances, the Intelligence Community would not be able to use information that had been collected based on a reasonable assessment that the target was outside the United States when subsequent information calls that conclusion into doubt. The Administration continues to believe that FISA must be modernized and has proposed the same revision to the definition of "electronic surveillance" as part of its proposed FY 2008 Intelligence Authorization Act.

80. The Specter bill, in section 9(b)(2), modifies section 1801(f) of FISA, defining "electronic surveillance." It would limit the definition in 1801(f)(1) to "the intentional collection of information concerning a particular known person ... by intentionally targeting that person..." In contrast, the current language of 1801(f)(1) covers the "acquisition ... of the contents of any ... communication sent by or intended to be received by" a particular person who is intentionally targeted. Would this change in the definition mean that if the government targeted an individual to obtain information about someone other than that person, that it would fall outside the definition of "electronic surveillance"? Please explain your view of the effect of this change to the definition.

ANSWER: This question concerns a provision of S. 2453, which was introduced in the 109th Congress. The Administration has proposed a similar amendment in the 110th Congress as part of its proposed FY 2008 Intelligence Authorization Act. We continue to believe that FISA must be modernized. To that end, we believe that it is crucial to establish a technologically neutral definition of "electronic surveillance" that does depend on the fortuities of how or where the communication is intercepted or the information is acquired. In combination with other amendments to FISA, this change would enable the FISC and the Government to focus resources on surveillance activities that most directly implicate the privacy of U.S. persons in the United States.

81. The Specter bill, in section 9(b)(2), modifies section 1801 of FISA defining "electronic surveillance." It creates a two-part definition of "electronic surveillance," in which the second half of the definition covers "any communication" where "both the sender and all intended recipients are in the United States." In all four parts of the current FISA definition, the phrase "by an electronic, mechanical, or other surveillance device" is used. The second part of the definition in the Specter bill does not use this language. Please explain your view of the legal effect of this omission.

ANSWER: Section 9(b)(2) of S. 2453 would have amended the definition of "electronic surveillance" in 50 U.S.C. § 1801(f). In combination with other amendments to FISA, a revised definition of "electronic surveillance" would have the effect of restoring FISA to its original focus on protecting the privacy of U.S. persons in the United States. There is no need to specify the type of device in the second

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00133 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.080

definition, which would cover certain communications no matter how the Government acquires them. The Administration's proposed FY 2008 Intelligence Authorization Act follows the same course.

82. The Specter bill, in section 9(b)(3), modifies section 1801 of FISA defining "Attorney General" to include "a person or persons designated by the Attorney General or Acting Attorney General." What limit would there be on the ability of the Attorney General to designate individuals, including employees of agencies/departments other than the Justice Department, as "Attorney General" for purposes of FISA? To the degree that your answer references regulations, could the Attorney General amend those regulations without congressional approval?

ANSWER: These questions concern a provision of S. 2453, which was introduced in the 109th Congress. S. 2453 has not been reintroduced in this Congress, and we are not aware of any current legislative proposal incorporating this provision.

83. The Specter bill, in section 9(b)(4)(C), modifies the FISA definition of "minimization procedures" by striking 50 U.S.C. § 1801(h)(4), which requires that any contents of communications to which a U.S. person is a party shall not be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a FISA court order is obtained or the Attorney General determines the information indicates a threat of death or serious bodily harm to any person. Please discuss what you believe are the advantages of entirely eliminating 1801(h)(4) from the current FISA statute.

ANSWER: Striking 50 U.S.C. § 1801(h)(4) would be a conforming amendment that would be necessary in light of proposed amendments to 50 U.S.C. § 1802(a), which is addressed in my answers to Questions 36, 37, and 86. The Administration supports a similar amendment to section 1801(h)(4) as part of its proposed FY 2008 Intelligence Authorization Act.

84. The current FISA statute, in section 1801(n), defines the covered "contents" of communication as: "when used with respect to a communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication." The Specter bill, in section 9(b)(5), replaces the definition of "contents" with the definition contained in 18 U.S.C. § 2510(8) – "when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication."

a. The new definition does not cover "any information concerning the identity of the parties to such communication." Please discuss what you believe is the effect of this proposed change.

b. The new definition does not cover "any information concerning...the existence...of that communication." Please discuss what you believe is the effect of this proposed change.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00134 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.081

ANSWER: Please see my answer to Question 35.

85. The Specter bill, in section 9(c), makes a number of changes to section 1802 of FISA. Section 1802(a)(1) authorizes the President to engage in electronic surveillance without court order for up to one year in certain limited circumstances "under this subchapter." The Specter bill modifies this phrase to "under this title." In your opinion, what effect would this change have?

ANSWER: This change would have no material effect upon the meaning of 50 U.S.C. § 1802(a)(1).

86. The Specter bill, in section 9(c), makes a number of changes to section 1802 of FISA. The current section 1802 requires the Attorney General to certify that "the electronic surveillance is solely directed at" the acquisition of certain covered communications. The Specter bill strikes the "solely directed at" phrase. Given this modification, what showing about the surveillance do you believe the Attorney General would have to make to meet the requirements of this provision? Please explain whether you support this change, and if so, why.

ANSWER: This question concerns section 9(c) of S. 2453, which was introduced in the 109th Congress. The Administration has proposed similar but more modest amendments to section 102 of FISA in the 110th Congress as part of its proposed FY 2008 Intelligence Authorization Act. As noted in my answers to Questions 36 and 37, this change would help modernize FISA by allowing this provision to fulfill the role Congress envisioned in 1978. Section 102 of FISA requires, among other things, circumstances in which the "communications [are] transmitted exclusively by means of communications used exclusively between or among foreign powers." The change would modernize FISA to account for technological changes in the means by which the communications at issue actually are transmitted today. The focus of the provision should remain on the communications of traditional foreign powers, and any surveillance conducted under the amended provision still would require that the Attorney General implement the "minimization procedures" required by section 101(h) of FISA. *See* FY 2008 Intelligence Authorization Act § 402(a) ("An electronic surveillance authorized under this section may be conducted only in accordance with the Attorney General's certification and the minimization procedures."); 18 U.S.C. § 1801(h) (defining minimization requirements).

87. The Specter bill, in section 9(c), makes a number of changes to section 1802 of FISA, which permits electronic surveillance without a court order in certain limited circumstances. The language of 1802(a)(1)(A)(i) currently requires a showing that the communications being pursued are "communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801(a)(1), (2), or (3) of this title." The Specter bill, in contrast, would require only that the communications being pursued were "communications of foreign powers, as defined in section 101(a),

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00135 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.082

an agent of a foreign power as defined in section 101(b)(1)." This is a significant expansion of section 1802's exemption from the usual FISA court order requirement.

- **a. Do you support this modified language of section 1802? If so, please discuss the justification for eliminating the limiting language that requires the means of communications be "used exclusively between or among foreign powers."**
- **b. If you do support the modified language of section 1802, please explain the justification for expanding the "foreign powers" covered by this blanket exemption from those defined in 1801(a)(1)-(3) to all "foreign powers."**
- **c. If you do support the modified language of section 1802, please explain the justification for adding non-U.S. person agents of foreign powers to this blanket exemption.**
- **d. In combination with the change to the definition of "agent of foreign power" elsewhere in the bill, wouldn't this mean that the government could wiretap without a warrant the calls of any non-U.S. person in the United States who possessed or was expected to transmit or receive "information with respect to a foreign power or foreign territory that relates to ... the conduct of the foreign affairs of the United States"? Wouldn't this be a very broad category covering foreign nationals who have nothing to do with terrorism and no intent to harm the United States in any way?**

ANSWER: This question concerns provisions in section 9(c) of S. 2453, which was introduced in the 109th Congress. As explained above in answers to Questions 36, 37, and 86, we do support amending section 102 of FISA. That is why the Administration has proposed similar but more modest amendments to section 102 as part of its proposed FY 2008 Intelligence Authorization Act. The Administration's proposal to eliminate the requirement that the means of communication be used "exclusively" among foreign powers would modernize FISA to account for technological changes in the means of communications among foreign powers that have seriously eroded the usefulness of the current version of section 102. At the same time, unlike section 9(c) of S. 2453, the Administration's proposal would not expand section 102 to apply to all foreign powers, nor would it expand section 102 to apply to agents of a foreign power. We believe that these amendments would modernize FISA in ways that better protect the Nation while also increasing protection of civil liberties.

88. The Specter bill, in section 9(c), makes a number of changes to section 1802 of FISA, which permits electronic surveillance without a court order in certain limited circumstances. The Specter bill strikes the requirement of 1802 that the Attorney General certify that "there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party." Please discuss your view of the justification, if any, for repealing this requirement.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00136 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.083

ANSWER: Please see my answer to Question 37.

89. The Specter bill, in section 9(c), makes a number of changes to section 1802 of FISA. In creating a new 1802(b), the Specter bill creates a completely new category of Attorney General authority – that as long as the Attorney General certifies that given information, facilities or technical assistance does not fall within the definition "electronic surveillance," the Attorney General can require any electronic communications service, landlord, custodian or other person to furnish such information, facilities, or technical assistance. Please discuss what you consider to be the advantages, if any, of this new provision.

ANSWER: Since the enactment of FISA, it always has been the case that certain types of communications intelligence activities fell outside the scope of "electronic surveillance" under 50 U.S.C. § 1801(f). It is, however, advantageous to be able to enlist private parties to assist the Government even when the surveillance at issue does not fall within the definition of "electronic surveillance." The proposed amendment would have supplied this authority and would have permitted third parties, such as Internet service providers and landlords, to challenge an order by the Attorney General compelling their compliance. The Administration has proposed a similar amendment in the 110th Congress as part of its proposed FY 2008 Intelligence Authorization Act. We continue to believe that this change is critical.

90. The Specter bill, in section 9(c), makes a number of changes to section 1802 of FISA. The Specter bill creates a new 1802(c), which is similar to the language of the current FISA section 1802(a)(4) that permits the Attorney General to order carriers to provide assistance to implement section 1802 and allows them to be compensated.

a. The current 1802(a)(4) only applies to "electronic surveillance authorized by this subsection." The new 1802(c) would apply to "electronic surveillance or the furnishing of any information, facilities, or technical assistance authorized by this section." Please discuss your view of the effect of the difference between these two formulations.

b. The current 1802(a)(4) also only applies to a "specified communication common carrier." The new 1802(c) applies to "any electronic communication service, landlord, custodian or other person (including any officer, employee, agent, or other specified person thereof) who has access to electronic communications, either as they are transmitted or while they are stored or equipment that is being or may be used to transmit or store such communications." Do you agree with this change? If so, please discuss why you believe that this wider scope is needed.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00137 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.084

ANSWER: As discussed in my answer to Question 89, some communications intelligence activities do not constitute "electronic surveillance" under 50 U.S.C. § 1801(f) as defined currently or under the proposed redefinition that was included in S. 2453. It is essential that the Government be able to compel third parties to assist the Government, while allowing these parties to challenge such an order in court. To that end, the Administration has proposed such amendments to FISA in the 110th Congress as part of its proposed FY 2008 Intelligence Authorization Act.

91. The Specter bill, in section 9(c), creates a new section 1802(d), which reads: "Electronic surveillance directed solely at the collection of international radio communications of diplomatically immune persons in the United States may be authorized by an official authorized by the President to engage in electronic surveillance for foreign intelligence purposes in accordance with procedures approved by the Attorney General." Please discuss whether you believe this added authorization is necessary, and if so, why.

ANSWER: These questions concern a provision in section 9(c) of S. 2453, which was introduced in the 109th Congress. S. 2453 has not been reintroduced in this Congress, and we are not aware of any current legislative proposal containing this provision.

92. The Specter bill, in section 9(e), would strike requirements (6), (8), (9) and (11) from the section 1804(a) of FISA, the provision that lays out the required components of FISA applications for electronic surveillance.

a. Please discuss whether you believe these changes are necessary, and if so, why.

b. Do you believe that the information required in these paragraphs was not helpful to the FISA court?

ANSWER: These questions concern several provisions of S. 2453, which was introduced in the 109th Congress. We continue to support streamlining the required statements in section 104(a) of FISA to reduce the administrative burden involved in the FISA process and because these requirements are not necessary to protect the privacy interests of U.S. persons in the United States. The Administration, however, does not propose eliminating current paragraphs (6), (8), and (9) from section 104(a), but rather has proposed streamlining these aspects of the application process as part of its proposed FY 2008 Intelligence Authorization Act. The Administration continues to believe that paragraph (11) of section 104(a), which requires that where "more than one electronic, mechanical or other surveillance device is to be used with respect to a particular proposed electronic surveillance, the coverage of the devices involved and what minimization procedures apply to information acquired by each device," is unnecessary. These amendments would improve the administrative efficiency of the Department of Justice and the Intelligence Community in preparing applications to submit to the FISC and would allow the Government and the FISC to concentrate on the information needed to protect the privacy of persons in the United States.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00138 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.085

93. The Specter bill, in section 9(f)(4), would substantially modify section 1805(e)(1) of FISA, which sets the time limits for a FISA surveillance order. Under current law, FISA surveillance can be authorized for at most ninety days; except that for a non-U.S. person agent of a foreign power, it can be 120 days at most; and for surveillance of certain types of foreign powers, a year at most. The Specter bill replaces these three tiers with a single time limit – a maximum limit of a court order of surveillance for one year – even for U.S. persons.

a. Please discuss whether you believe this change is necessary, and if so, why.

b. Please explain your understanding of what is intended by the second sentence of the new 1805(e)(1) that would be created by the Specter bill: "If such emergency employment of electronic surveillance is authorized, the official authorizing the emergency employment of electronic surveillance shall require that the minimization procedures required by this title for the issuance of a judicial order be followed."

ANSWER: These questions concern provisions of section 9(f)(4) of S. 2453, which was introduced in the 109th Congress. The Administration's FY 2008 Intelligence Authorization Act proposes similar but more modest changes to FISA. The Administration's proposal would establish a revised section 105(d)(1) of FISA that would extend the maximum initial term of authorization for electronic surveillance *of a non-U.S. person* who is an agent of a foreign power to one year from the current 120 days. This amendment would not affect the initial duration of an order authorizing electronic surveillance of U.S. persons, which would remain at 90 days. This revision would have the benefit of reducing the time spent preparing applications for renewals relating to non-U.S. persons, thereby allowing more resources to be devoted to cases involving U.S. persons.

The proposed FY 2008 Intelligence Authorization Act also would extend the maximum term of authorization to conduct electronic surveillance upon renewal of an order authorizing electronic surveillance of any person to up to one year. Because the FISC already has approved the surveillance for an initial period, and because it also has an opportunity to monitor the surveillance through the initial term of the order, a longer renewal period may be warranted. Again, a longer duration of a renewed order would allow more resources to be devoted to other foreign intelligence activities. Of course, under the Administration's proposal, the Government would not seek longer periods—nor would we expect the FISC to grant longer periods—where that would not be reasonable.

With regard to subpart (b) of this question, the Administration's proposed FY 2008 Intelligence Authorization Act would include a provision similar to the quoted sentence in a revised section 105(e)(4) of FISA. That revised section would provide that if the Attorney General authorizes emergency electronic surveillance, then he "shall require that the minimization procedures required by this title for the issuance of a judicial order be followed." The meaning of this provision is self-evident: Any

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00139 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.086

emergency surveillance must follow the minimization procedures required by revised section 101(h) of FISA.

94. The Specter bill, in section 9(g), modifies section 1806(i) of FISA, which requires the destruction of certain communications contents that were unintentionally acquired unless the Attorney General determines they indicate a threat of death or serious bodily harm to any person. The amendment would allow the Attorney General to retain any unintentionally acquired communications contents that he determines contains "significant foreign intelligence."

a. Please discuss whether you believe this change is necessary, and if so, why.

b. In making this determination, what procedures do you believe the law would require the Attorney General to undertake?

ANSWER: The Administration supports a virtually identical amendment as part of its proposed FY 2008 Intelligence Authorization Act. We continue to believe that FISA must be modernized, and this change would help make the statute technologically neutral. With regard to the first part of this question, please see my answer to Question 41. With regard to the second part of this question, the Attorney General, in consultation with appropriate officers and personnel from the Intelligence Community, including the Director of National Intelligence, would determine whether the "foreign intelligence information," as defined by 50 U.S.C. § 1801(e), was "significant."

95. The Specter bill, in section 9(i), strikes section 1809(a) of the current FISA and replaces it with new language. But the Specter bill, in section 8(c), makes different line-by-line amendments to section 1809(a) of the FISA statute. Do you agree that these two provisions of the proposed legislation are inconsistent and cannot both become law? Of the two provisions, which do you support and why?

ANSWER: These questions concern an alleged drafting discrepancy between sections 8(c) and 9(i) of S. 2453, which was introduced in the 109th Congress. S. 2453 has not been reintroduced in this Congress, and we are not aware of any current legislative proposal that contains this apparent discrepancy.

96. The Specter bill, in section 9(k), modifies section 1827 of FISA by expanding the exception to the criminal prohibition of warrantless physical searches in section 1827(a)(1) to include "except as authorized...under the Constitution." What authority to do warrantless physical searches do you believe is granted "under the Constitution"? Also please discuss whether you believe this change is necessary, and if so, why.

ANSWER: Please see my answer to Question 44.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00140 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.087

97. The Specter bill, in section 9(k), modifies section 1827(a)(2) of FISA by omitting the phrase – "for the purpose of obtaining intelligence information." Please discuss whether you believe this change is necessary, and if so, why.

ANSWER: Please see my answer to Question 44.

Questions from Sen. Schumer

98. On July 13, Senator Specter announced that he had reached a deal with the White House on his legislation to authorize the Terrorist Surveillance Program and re-write much of the Foreign Intelligence Surveillance Act (FISA). This was just two weeks after the Supreme Court's decision in *Hamdan*, which many have characterized as a rebuke of the Administration's legal defense of the President's warrantless surveillance program.

- **Do you continue to believe that the NSA Surveillance Program is legal and Constitutional and that it would survive any legal challenge in the FISA Court?**

ANSWER: Yes.

- **If the administration has "the authority, both from the Constitution and the Congress, to undertake this vital program," as President Bush asserted in January, what need is there to legislate on this issue from your perspective?**

ANSWER: Although the President had ample constitutional and statutory authority to implement the Terrorist Surveillance Program, that Program has not been reauthorized, and any electronic surveillance that may have been occurring as part of the Program is now subject to the approval of the FISC, as noted in my answer to Question 3.

FISA still provides a vital framework for the Intelligence Community, but it is now imperative that Congress and the Executive Branch shift their focus away from former intelligence programs and cooperate to close critical gaps in our intelligence capabilities under FISA while ensuring proper protections for the civil liberties of U.S. persons. FISA has been and continues to serve as the foundation for conducting electronic surveillance of foreign powers and agents of foreign powers in the United States. Nevertheless, FISA can and must be improved. The most serious problems with the statute stem from the fact that FISA presently defines the term "electronic surveillance" in a way that depends upon communications technology and practices as they existed in 1978. This technology-dependent approach has had dramatic but unintended consequences, sweeping within the scope of FISA a wide range of communications intelligence activities that Congress intended to exclude from the scope of FISA. This unintended expansion of FISA's scope has hampered our intelligence capabilities and has caused the Intelligence Community, the Department

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00141 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.088

of Justice, and the FISC to expend precious resources obtaining court approval to conduct intelligence activities directed at foreign persons overseas.

To rectify these problems, the Administration has proposed comprehensive amendments to modernize FISA that would make the statute technology neutral, enhance the Government's authority to secure assistance from private entities in conducting lawful foreign intelligence activities, and streamline the application and approval process before the FISC. By modernizing FISA, we can both provide the Intelligence Community with an enduring, agile, and efficient means of collecting foreign intelligence information and strengthen the privacy protections for U.S. persons in the United States. For further explanation of the importance of these amendments to FISA, please see my answers to Questions 1, 2, 89, 90, and 92.

- **Would you prefer that Congress not legislate in this area at all?**

ANSWER: No. Congress can and should play a critical role in protecting the Nation by modernizing and streamlining FISA. Please see my answers to Questions 1 and 2.

- **Did the Supreme Court's recent ruling in *Hamdan* play any role in the Administration's decision to support Senator Specter's legislation?**

ANSWER: No.

99. Senator Specter has characterized his bill as simply allowing the Court to decide the Constitutionality of the program, including whether the President has the authority to authorize this surveillance. It has been said that if kept in its precise current form, the President will submit the program to the FISA Court. Why doesn't the Administration just submit the program to the FISA Court now, without any legislation?

ANSWER: As you are aware, on January 10, 2007, a judge of the FISC issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that at least one of the communicants is a member or an agent of al Qaeda or an affiliated terrorist organization. As a result of these orders, any electronic surveillance that may have been occurring as part of the Terrorist Surveillance Program now is subject to the approval of the FISC.

100. If the Specter bill is passed in its current form, what signing statement do you anticipate the President issuing in connection with it?

ANSWER: This question concerns S. 2453, which was introduced in the 109th Congress. S. 2453 has not been reintroduced in this Congress.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00142 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.089

101. If the Specter bill is passed in its current form, and the Administration then voluntarily submitted the program to the FISC, would the Administration argue that the Specter bill authorized the NSA's Terrorist Surveillance Program?

ANSWER: This question concerns S. 2453, which was introduced in the 109th Congress. S. 2453 has not been reintroduced in this Congress. In addition, as you are aware, on January 10, 2007, a judge of the FISC issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that at least one of the communicants is a member or agent of al Qaeda or an affiliated terrorist organization. As a result of these orders, any electronic surveillance that may have been occurring as part of the Terrorist Surveillance Program now is subject to the approval of the FISC.

102. Do you believe that the portion of the Specter bill that allows the President to submit the NSA surveillance program to the FISA Court is constitutional? Specifically, do you believe this provision does not run afoul of the constitutional proscription against advisory opinions?

ANSWER: These questions concern certain provisions of S. 2453 relating to "electronic surveillance programs," a term defined in S. 2453. S. 2453, which was introduced in the 109th Congress, has not been reintroduced in this Congress. We are not aware of any current legislative proposal that incorporates these provisions of S. 2453.

103. The Specter bill provides that any cases pending right now – upon application by the Attorney General – must be transferred to the FISA Court of Review. The bill also provides that the decision of that FISA Court "shall be subject to certiorari review in the United States Supreme Court."

- **Is it your understanding that one who is challenging a FISA Court decision favorable to the government may obtain review before the Supreme Court under the bill?**
- **What are the arguments against allowing the constitutional review in a traditional Federal District Court, with expedited review to the Supreme Court, so long as the court applies the procedures and standards of the Classified Information Procedures Act?**

ANSWER: These questions refer to provisions of S. 2453 concerning the transfer of cases to the Foreign Intelligence Surveillance Court of Review. S. 2453, which was introduced in the 109th Congress, has not been reintroduced in this Congress. We are not aware of any current legislative proposal that would transfer cases to the Court of Review. The Administration has proposed similar amendments that would authorize the transfer of cases involving classified communications intelligence activities to the FISC as part of its proposed FY 2008 Intelligence Authorization Act.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00143 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.090

With respect to conducting litigation on sensitive foreign intelligence matters in federal district courts, please see my answer to Question 52. We believe that permitting litigation concerning classified communications intelligence activities in the federal district courts raises significant national security concerns. A single court decision concerning a classified communications intelligence activity could have immediate, nationwide ramifications. Intelligence programs that are essential to national security should not be subject to a variety of potentially inconsistent decisions from federal district courts across the country.

Moreover, federal district courts, unlike the FISC, do not have specialized security procedures and secure facilities that are optimized for adjudicating cases regarding highly sensitive intelligence issues. *Cf. Alfred A. Knopf, Inc. v. Colby*, 509 F.2d 1362, 1369 (4th Cir. 1975) ("It is not to slight judges, lawyers or anyone else to suggest that any such disclosure carries with it serious risk that highly sensitive information may be compromised. In our own chambers, we are ill equipped to provide the kind of security highly sensitive information should have."). Nor do federal district courts have expertise in addressing the complex legal, factual, and technical issues concerning foreign intelligence surveillance activities. Consolidating litigation involving classified communications intelligence activities before the FISC would capitalize upon the unique advantages of that court while retaining all of the advantages—and none of the potential disadvantages—of litigating in a regular federal district court.

104. During his February appearance before the Committee, Senator Biden asked Attorney General Gonzales what harm had been caused by public disclosure of the warrantless surveillance program. He responded: "You would assume that the enemy is presuming we are engaged in some kind of surveillance. But if they're not reminded about it all the time in the newspapers and in stories, they sometimes forget." When I asked him the same question in July, he deferred to the intelligence community.

- **Do you have a better answer as to how the disclosure that wiretapping is going on harmed national security?**
- **To your knowledge have any officials in the intelligence community had direct discussions with Attorney General Gonzales or officials in his Department about how disclosure of the program harmed national security? If so, what was said?**

ANSWER: As you know, foreign intelligence collection activities are highly classified and extremely sensitive. It therefore would be inappropriate for me to discuss in this setting the specific way in which the disclosure of the Terrorist Surveillance Program harmed national security. As a general matter, however, I believe we all recognize that the more details our enemies know about our intelligence activities, the more likely it is they will evade detection.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00144 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.091

105. Do you have legal or constitutional concerns about the use of warrantless physical searches in the United States?

ANSWER: I assume that this question does not concern warrantless physical searches where consent has been given. Consent searches are a valid exception to the warrant provisions of the Fourth Amendment to the Constitution. *See Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973). I also assume that this question does not concern warrantless physical searches that occur during law enforcement operations pursuant to one of the many well recognized exceptions to the warrant requirement of the Fourth Amendment, such as a search incident to a lawful arrest, *Maryland v. Buie*, 494 U.S. 325, 334 (1990), exigent circumstances, *Mincey v. Arizona*, 437 U.S. 385, 392 (1978), "hot pursuit," *United States v. Santana*, 427 U.S. 38, 42-43 (1976), or the plain view doctrine, *Coolidge v. New Hampshire*, 403 U.S. 443 (1971) (plurality opinion). Nor do I understand this question to involve the warrantless searching of materials or vessels entering or leaving the United States pursuant to the well recognized border search exception to the Fourth Amendment. *See, e.g., United States v. Ramsey*, 431 U.S. 606, 616 (1977).

A warrantless physical search that does not fall within the scope of any of these doctrines would raise a constitutional issue under the Fourth Amendment if the search were unreasonable. The legality of any physical search ultimately depends upon its reasonableness. *See United States v. Knights*, 534 U.S. 112, 118-19 (2001). The Supreme Court has made clear that warrantless physical searches may be reasonable in situations involving "special needs" that go beyond a routine interest in law enforcement. *See Vernonia Sch. Dist. v. Acton*, 515 U.S. 646, 653 (1995); *see also Illinois v. McArthur*, 531 U.S. 326, 330 (2001) ("When faced with special law enforcement needs, diminished expectations or privacy, minimal intrusions, or the like, the Court has found that certain general, or individual, circumstances may render a warrantless search or seizure reasonable."). We do not think it is appropriate, however, for us to opine on this complex question in the abstract.

106. To your knowledge, has the Administration ever used its commander-in-chief powers or the AUMF to justify warrantless physical searches?

ANSWER: To my knowledge, the Administration has not invoked either the President's constitutional authority as Commander in Chief or the statutory authorities granted by the AUMF to authorize physical searches in the United States without prior judicial approval.

Questions from Sen. Durbin

107. You testified:

The United States, the most advanced Nation on earth, confronts the threat of al Qaeda with a legal regime designed for the last century and geared

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00145 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.092

more toward traditional case-by-case investigations. ... Chairman Specter's legislation includes several important reforms to update FISA for the 21st century. ... Changes contained in the Chairman's bill would correct the most significant anachronisms in FISA."

If we have a legal regime that is "designed for the last century" and FISA includes "significant anachronisms," why, almost five years after 9/11 and after we enacted and reauthorized the PATRIOT Act, has the Administration not previously requested changes in the law that would bring FISA into the 21st Century?

ANSWER: We have sought specific changes to FISA since September 11, 2001. The Administration did not seek a general modernization of FISA before 2006, in part out of the concern for protecting sensitive intelligence sources and methods. Moreover, FISA is a complicated statute, and it has taken time for the Executive Branch to reach consensus on how to modernize FISA. What is most important, however, is that we now stand ready to work with Congress to streamline and to modernize FISA. Indeed, the Administration has put forward a comprehensive proposal to modernize FISA as Title IV of its proposed FY 2008 Intelligence Authorization Act.

108. On January 25, over six months ago, Senators Reid, Kennedy, and Feingold and I sent a letter to President Bush asking what changes in the law he believes are necessary to permit effective surveillance of suspected terrorists, and why these changes are needed. We still have not received a response. I have attached this letter.

Please respond to the questions raised in our letter.

ANSWER: As the President and other officials have explained on a number of occasions, there are several problems with the current procedures for obtaining an order authorizing electronic surveillance under FISA. Most importantly, through sheer happenstance, the definition of "electronic surveillance" has come to sweep in activities of the sort Congress specifically excluded from the scope of FISA in 1978. We believe the definition should be changed to reflect this reality, and we should do so in a way that does not depend on specific technologies. We also believe that the FISA application process can and should be streamlined. These changes would, we believe, better protect the Nation and better protect the privacy of U.S. persons in the United States.

109. If the Specter bill is enacted into law as currently drafted, will the Administration abide by its terms in all circumstances?

ANSWER: The Executive Branch has followed—and will continue to follow—the laws of the United States, including the Constitution and FISA.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00146 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.098

110. If the Specter bill is enacted into law as currently drafted, can you assure us that the President will not issue a signing statement claiming that the law or a portion of the law is unconstitutional?

ANSWER: This question concerns S. 2453, which was introduced in the 109th Congress. S. 2453 has not been reintroduced in this Congress.

111. If, pursuant to the Specter bill, the Attorney General submits the NSA program to the FISA court and the FISA court holds that the program is illegal, can you assure us that the Administration will abide by such a ruling?

ANSWER: This question concerns S. 2453, which was introduced in the 109th Congress. S. 2453 has not been reintroduced in this Congress. In addition, as you are aware, on January 10, 2007, a judge of the FISC issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that at least one of the communicants is a member or an agent of al Qaeda or an affiliated terrorist organization. As a result of these orders, any electronic surveillance that may have been occurring as part of the Terrorist Surveillance Program now is subject to the approval of the FISC.

112. The Specter bill would add a new section to FISA that would say:

> **Nothing in this Act shall be construed to limit the constitutional authority of the President to gather foreign intelligence information or monitor the activities and communications of any person reasonably believed to be associated with a foreign enemy of the United States.**

Why is this section needed? Would the Administration continue to support the Specter bill if this section were removed from the bill?

ANSWER: Please see my answers to Questions 28 and 49.

113. In the Administration's view, does the Specter bill give the President the power to do anything that he cannot already do under his inherent constitutional authority?

ANSWER: This question concerns S. 2453, which was introduced in the 109th Congress. S. 2453 has not been reintroduced in this Congress.

114. The Specter bill would repeal the provision of FISA that makes FISA and the criminal wiretap statute the "exclusive means" for conducting electronic surveillance. The Administration has taken the position that the Authorization to Use Military Force implicitly repeals the "exclusive means" provision.

If your position is correct, then why is it necessary for the Specter bill to repeal

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00147 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.094

the "exclusive means" provision?

ANSWER: The Administration has taken no such position. As set forth in the Department of Justice's *Legal Authorities Supporting the Activities of the National Security Agency Described by the President* (Jan. 19, 2006) ("*Legal Authorities*"), we do not believe that the text of FISA requires an amendment to FISA to authorize additional electronic surveillance. Rather, by expressly excepting from its prohibition electronic surveillance undertaken "as authorized by statute," 50 U.S.C. § 1809(a)(1), FISA contemplates that surveillance may be authorized by another statute without following the specific and detailed procedures set forth in FISA. *See Legal Authorities* at 21-24. The Authorization for Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (Sept. 18, 2001) ("Force Resolution"), is just such a statute authorizing the President to conduct electronic surveillance of al Qaeda and affiliated terrorist organizations without prior judicial approval. *See Legal Authorities* at 23-28. Therefore, the Force Resolution did not impliedly repeal section 2511(2)(f); it instead is best read as an authorization to conduct electronic surveillance outside the procedures expressly enumerated in FISA.

This interpretation is consistent with the understanding that section 109(b) of FISA incorporates other laws, which thereby constitute procedures for purposes of section 2511(2)(f). *See Legal Authorities* at 22-23 & n.8. Indeed, at the time FISA was enacted, pen-register surveillance was "electronic surveillance" within the meaning of FISA, but was not authorized by either Title III or by FISA when conducted for ordinary law enforcement purposes. Congress adopted the affirmative defense in section 109(b) of FISA's criminal penalty provision to ensure that such activities could continue in the domestic law enforcement context despite the so-called exclusivity provision in section 2511(2)(f). *See* H.R. Rep. No. 95-1283, Part I, at 100 n.54 (1978) ("As noted earlier, the use of pen registers and similar devices for law enforcement purposes is not covered by [Title III] of this Act and [the exclusivity provision in section 2511(2)(f)] is not intended to prohibit it. Rather, because of the criminal defense provision of section 109(b) [of FISA, 50 U.S.C. § 1809(b)], the 'procedures' referred to in section 2511(2)(f) include acquiring a court order for such activity. It is the committee's intent that neither this [exclusivity provision] nor any other provision of the legislation have any effect on the holding in *United States* v. *New York Telephone* that rule 41 of the Federal Rules of Criminal Procedure empowers federal judges to authorize the installation of pen registers for law enforcement purposes."). Hence, it cannot be—and is not—the case that section 2511(2)(f) prohibits all electronic surveillance that is conducted outside the specific and detailed procedures set forth in section 104 of FISA.

In addition, if section 2511(2)(f) were read, as the question suggests, to prohibit all electronic surveillance other than that authorized by the express procedures of FISA, serious constitutional questions would arise. It is well established that the President has constitutional authority to conduct electronic surveillance without prior judicial approval for the purpose of collecting foreign intelligence. *See In re Sealed Case*, 310 F.3d 717, 742 (For. Intel. Surv. Ct. Rev.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00148 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.095

2002); *United States v. Truong Dinh Hung*, 629 F.2d 908, 913-17 (4th Cir. 1980); *United States v. Butenko*, 494 F.2d 593, 602-06 (3d Cir. 1974) (en banc); *United States v. Brown*, 484 F.2d 418, 425-27 (5th Cir. 1973); *United States v. bin Laden*, 126 F. Supp. 2d. 264, 271-77 (S.D.N.Y. 2000). Accordingly, FISA cannot eliminate the President's constitutional authority to conduct foreign intelligence surveillance without prior judicial approval against a hostile foreign power. *See In re Sealed Case*, 310 F.3d at 742. The question's proffered interpretation of the exclusivity provision of FISA risks a constitutional clash between the Executive Branch and Congress. *See Legal Authorities* at 19-23. We believe, consistent with repeated holdings of the Supreme Court, that FISA must be interpreted, if "fairly possible," to avoid raising these serious constitutional concerns. *See INS v. St. Cyr,* 533 U.S. 289, 299-300 (2001) (citations omitted); *Ashwander v. TVA*, 297 U.S. 288, 345-48 (1936) (Brandeis, J., concurring). As noted above, our interpretation of FISA does not involve any implied repeal. It does, however, gain strength from the well-established canon of constitutional avoidance. Nevertheless, we have also explained that if these arguments were unavailable, the Force Resolution would in fact constitute a limited, implied repeal of the exclusivity provision. *See Legal Authorities* at 36 n.21.

115. In its findings, the Specter bill inaccurately states that the 9/11 Commission concluded that the FBI could not meet the requirements to obtain a FISA order to search Zacarias Moussaoui's computer before 9/11. In fact, the 9/11 Commission report actually concluded that the FBI did not submit a FISA application for Moussaoui's computer because they believed they did not have enough evidence to obtain a FISA warrant. A report issued by Senators Leahy, Specter, and Grassley concluded that the FBI misinterpreted FISA and they could have in fact obtained a warrant.

Is the Moussaoui finding in the Specter bill inaccurate?

ANSWER: Regardless of which description is accurate—and I am not in a position to speak with any authority regarding the FBI's actions concerning Mr. Moussaoui—the application procedures under FISA should be revised as noted above.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00149 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.096

Senator Arlen Specter
FISA for the 21st Century
Wednesday, July 26, 2006
Questions for Bryan Cunningham

1. Technology has changed tremendously since 1978. What are some of the technological hurdles that make FISA obsolete today? Do you agree with how S. 2453 deals with emerging technological issues? Is it feasible for the FISA Court to make the type of determinations and issue the type of program-wide warrants that the bill envisions?

2. What do you think of the modifications made to FISA under my bill, S. 2453? Do you agree that FISA should be altered so that the NSA may monitor phone calls in and out of the United States, when the targets of the surveillance are suspected members of al queda?

3. Not only has the FISA court been able to maintain its secrecy where both the Executive and Legislative branches have allowed leaks, but they are in the best position to weigh and balance the nature of the threat, the scope of the program, how many people are being intercepted, what is being done with the information, what is being done on minimization, how successful the program has been, if any projected terrorist threats have been thwarted, and all factors relating to the specifics on the program. Do you believe that the best solution to the possible problem that the president may lack the authority to conduct warrantless wiretaps is to submit the program to the FISA Court of Review and allow them to determine the constitutionality of the program?

4. We have read in the press about the "minimization" of information pertaining to U.S. persons and FISA. In addition, some of the legislation we will mark up tomorrow includes provisions on "minimization procedures." Do you believe that such minimization procedures are an adequate way of protecting people from unnecessary eavesdropping?

43453.097

CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Keeping the Internet Open, Innovative and Free

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

June 23, 2008

The Honorable Patrick J. Leahy
Chairman
Senate Judiciary Committee
224 Dirksen Senate Office Building
Washington DC 20510

Dear Chairman Leahy:

On behalf of the Center for Democracy & Technology, I am pleased to submit these answers to follow-up questions that Senators submitted for the record after the Committee's July 26, 2006 hearing, "FISA for the 21st Century."

Questions Submitted by Senator Arlen Specter

1. Would you have any objection to the question of the constitutionality of the NSA program being assessed by the FISA court?

Answer: CDT fully supports judicial review of the statutory legality and constitutionality of the NSA program. However, we believe that the "ordinary" district courts and appellate courts are every bit as capable of adjudicating these issues as the FISA Court and the FISA Court of Review. We are opposed to turning the FISA court into a national security court, and we fear that transfer of cases from the district courts to the FISA court would set a bad precedent in that regard.

2. In your written testimony, you assert that congress should not legislate on FISA until all of the facts are known. You note that this will require several more hearings. However, given the highly classified nature of the Terrorist Surveillance Program it is doubtful that we will ever discover the intricate details which it contains. Accordingly, would you agree that the best way guard against further executive over-reach would be to submit the Terrorist Surveillance Program to the FISA Court of Review in order determine the constitutionality of the program?

Answer: Both Congress and the courts have important responsibilities to fulfill in guarding against executive over-reach; even within the executive branch itself there are offices that should serve as a guard on executive over-reach. We fully appreciate that this Administration has been perhaps unique in modern history in its resistance to legislative oversight, and we agree that the TSP should be subject to judicial review, but, as noted

above, we do not believe that submitting the program to the FISA Court of Review would be the best way to achieve judicial review. Nor do we believe that constitutionality is the only test of executive over-reach.

3. One purpose of my bill is to give the public confidence in the constitutionality of the NSA program. Given the amount of time you feel is necessary to adequately modernize FISA, wouldn't you agree that it is important for Congress to legislate and the courts to rule on this issue in a timely way, so that the American people can feel confidant that the NSA is not currently over-reaching in its surveillance?

Answer: We have consistently applauded your efforts to obtain a resolution of the issues posed by the TSP, and we agree that both the national security and constitutional values would be better served if the legality of the program were judicially reviewed. One concern we have with the FISC and FISCR processes is that they are shrouded in secrecy. In the granting of surveillance orders such secrecy is fully justified, but it is unnecessary in cases turning on questions of law. Nevertheless, we fear that the FISC and the FISCR, if they reviewed the TSP, might act with a degree of secrecy that would undermine public confidence in their conclusions.

4. Technology has changed tremendously since 1978. What are some of the technological hurdles that make FISA obsolete today? Do you agree with how S. 2453 deals with emerging technological issues? Is it feasible for the FISA Court to make the type of determinations and issue the type of program-wide warrants that the bill envisions?

Answer: S. 2453 would not have dealt appropriately with emerging technological issues. Changes in technology since 1978 render FISA obsolete in ways that require stronger, not weaker standards for the conduct of electronic surveillance. Some of these changes, such as the routing of international communications through the United States, actually make the job of the intelligence agencies much easier in some ways, since they can access foreign-to-foreign communications from US soil. Beyond that, everything we know about the digital revolution indicates that, on balance, it has been a windfall for the snoopers: With globalization, cell phones, and the Internet, more electronic information than ever before is available to the government, and the government's ability to process that information is exponentially greater than ever before. Whether the government is able to digest the massive amount of information at its disposal is a different question, but the availability of oceans of sensitive personal data is no reason to weaken standards for government collection of that data. To the contrary, the increasing amount of information about our daily lives that is exposed to electronic surveillance calls for stronger, not weaker standards. We believe that it is feasible for the FISA Court to make the determinations necessary to issue program-wide warrants, and we believe that a narrowly drawn blanket warrant could pass constitutional muster, but the programmatic warrants contemplated by S. 2453 would be far too broad. Indeed, one version of S. 2453 would have authorized blanket warrants to intercept the contents of purely domestic calls

43453.099

of American citizens without probable cause, without specific suspicion, and where the call has nothing to do with terrorism of any kind.

5. Can you provide an example of standards that would allow the Administration to access mobile technology being used by terrorists, such as prepaid cell phones, email or text messaging, which allow virtual anonymity, without reducing the privacy protection enjoyed by those in the United States? How would you balance the need to protect our homeland with the danger of reducing the standards to a point where every domestic conversation is potentially subject to a wiretap?

Answer: None of these technologies offers perfect anonymity, but at the same time no system of rules, even one that imposed no legal limits on government surveillance, would offer perfect coverage or guarantee good intelligence. As your question suggests, the goal is to achieve a balance, which we believe will continue to involve questions about the kind of technology at issue, presumptions about whether the target is in the U.S. or abroad, and judgments about which communications to target. Selection and prioritization are central to the intelligence process, even when it is conducted overseas, beyond the reach of statutes such as FISA. Selection and prioritization decisions are made on the basis of various factors, including analysis of transactional data associated with communications and intelligence available from outside the communications stream. Whether the courts are involved or not, these decisions have to be made – what to collect, what to translate and analyze, what to retain and disseminate. When surveillance is likely to involve the communications of persons inside the U.S., we believe that a court should be involved in assessing the decision rules by which the intelligence agencies are making these decisions, to ensure that they are reasonably calibrated to obtain intelligence without unduly infringing on the rights of innocent persons.

Questions Submitted by Senator Dianne Feinstein

Background. In the 95th Congress back in 1978, language was eliminated from the 1968 Title III wiretap statute that expressly recognized the constitutional power of the President. It was replaced it with the current requirement that FISA "shall be the exclusive means" for conducting such surveillance.

In considering FISA in 1978, Congress also refused to enact language proposed by the Ford Administration that "[n]othing contained in this chapter shall limit the constitutional power of the President."

However, the Specter-White House bill now before us states, "Nothing in this Act shall be construed to limit the constitutional authority of the President to collect intelligence with respect to foreign powers and agents of foreign powers." The bill also contains other references authorizing unspecified actions "under the Constitution."

- *In your opinion, what is the impact of having this language in the bill?*

43453.100

Answer: This language would have serious negative consequences both for national security and for civil liberties. It would make FISA merely optional, turning the clock back to the 1970s and, if the President chose to act outside FISA, casting a cloud of constitutional doubt over what the Administration claims are critical intelligence activities. A central purpose of FISA was to place intelligence gathering on a sound constitutional basis. Senator Specter's bill, if the President took up its invitation to act without court approval, would make a constitutional case of every national security wiretap and expose to potential liability both government employees and the corporate communications service providers upon whose cooperation they depend.

Background. In the 1952 *Youngstown* case, Justice Jackson divided Presidential action into three areas:

1. When the President acts consistent with the will of Congress;
2. When the President acts in an area in which Congress has not expressed itself; and
3. When the President acts in contravention of the will of Congress.

In the first circumstance, Presidential power is at it greatest, in the third, Presidential power is at its lowest. Justice Jackson wrote that:

> "When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter."

- *In your opinion, how will the new Specter bill be analyzed in a Youngstown analysis given the deletion of the "exclusivity" language in FISA and with the addition of new language about the President's ability to act under the constitution?*

Answer: Chairman Specter's bill would cast the President's power into a grey zone or zone of uncertainty. As we suggested above, under Senator Specter; bill, every intelligence surveillance conducted by the President outside the procedures established by FISA would be subject to constitutional doubt. Perhaps a given surveillance would be legal under the intermediate strength Presidential power, perhaps it would be illegal. The intelligence agencies and the communication service providers would not know until the Supreme Court had ruled on that particular surveillance, with possibly unclear implications for the next surveillance. In our view, that is not an effective way to conduct the "war" on terror.

- *What legal limits, if any, would exist on the President's ability to conduct electronic surveillance for foreign intelligence without following FISA if we pass the new Specter bill?* Please answer according to what are the legal restrictions that the Specter bill places on the President, not what DOJ or the President may or may not do.

43453.101

Answer: Under Chairman Specter's bill, the President would still be subject to the limits set by the Fourth Amendment, which have never been clearly defined, and which it would be very difficult to adjudicate, given the state secrets doctrine and the standing hurdles that challenges to the President's program would face. However, if the government were ever to seek to introduce evidence form the TSP in a criminal case, then the constitutional issues would be squarely presented, and crucial evidence might be excluded.

Background. Sen. Specter's new FISA bill eliminates the 15-day window on surveillance outside of FISA after a declaration of war. This could be interpreted to mean that after a declaration of war the President may unilaterally wiretap whomever he chooses until the end of the war without limitation.

While wars do not have specific end dates, usually there is some identifying action that signals the end – such as surrender of one party, annexation of a territory under dispute, a peace treaty, when one party unilaterally withdraws, etc. However, in the "war on terror" it is highly unlikely that there would be a similar triggering event that would signify the end.

- *If the new Specter bill were to pass, how long would the President's authority last under the "war on terror"? Could it last decades? When would that authority end?*

Answer: We do not fully understand either the intent or the likely result of repealing the FISA provision allowing warrantless surveillance for 15 days after a declaration of war. Your question highlights both some of the problems with the use of the concept of "war" in reference to the struggle against terrorist groups and a problem with Senator Specter's bill. Already, the President has used the concept of a "war on terror" to exercise authority in ways that have harmed the America's standing in the world and undermined our efforts to fight terrorist groups.

Background. Under the new Specter-Administration bill, a new blanket exception would be created to the FISA warrant requirement, allowing surveillance of anyone who is inside the United States but is not a U.S. person. Under the bill, such individuals could be wiretapped for up to a year upon a declaration by the Attorney General that they possess foreign intelligence information.

- *Does "foreign intelligence" include economic trends overseas? What else does it include? Trade policies between the U.S. and another country? The strength of the dollar in another country? Currency valuations? Foreign stock prices and market fluctuations?*

Answer: The FISA definition of "foreign intelligence information" is broad. It includes not only information concerning potential attacks by foreign nations or international terrorists, but also "information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to -- (A) the national

43453.102

defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States." 50 U.S.C. §1801(e)(2). A lot could hinge on the interpretation of what is "necessary," but there is no public definition in statute, case law or Administration guideline as to what is "necessary."

It appears that this new Specter bill would authorize wiretapping of almost any individual in the United States who is not a U.S. person so long as this certification is made by the Attorney General.

- *Is that correct? What are the limitations to such a broad authority?*

Answer: The Fourth Amendment would impose some undefined limits on this authority, but the language does purport to 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 language 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.

- *How would this section affect foreign workers – including skilled workers on H-1-B visas – that U.S. companies routinely bring into the United States every day? If the Attorney General certified that a skilled worker possessed foreign intelligence, would this bill allow the Government to wiretap that worker while he is here in the U.S.? Would this include all of his calls or emails with other U.S. corporate executives or other persons – without a FISA warrant or other court oversight?*

Answer: It appears that this bill would allow the Government to wiretap such a worker while he is here in the U.S. It seems it would include all of his calls or emails with other U.S. corporate executives or other persons, including citizens.

Questions Submitted by Senator Edward M. Kennedy

1. From its enactment in 1978 until now, the Foreign Intelligence Surveillance Act has been the backbone of our statutory system for obtaining foreign intelligence through wiretapping or all other forms of electronic surveillance in the United States.

During the late 1970's, we knew that such surveillance could be a useful part of the Government's gathering of certain kinds of information. We also knew that it could be a deep and indiscriminate invasion of the privacy of our citizens, and that it was essential to reach a fair balance that would protect our security without infringing on citizens' basic rights.

43453.103

Congress included a specific provision in the Act stating that the statutory scheme enacted was to be the exclusive means for federal agencies to conduct electronic surveillance in the United States. The legislative intent was clear. The history of the Act makes clear that the warrant procedures in the law must be followed to conduct electronic surveillance in the United States. Most important, we thought we were putting an end to the debate over the meaning and scope of the President's inherent powers. Yet, the current compromise would eliminate the provision stating that the Act is the exclusive means for authorizing foreign intelligence surveillance.

Question:

- **What is the impact of repealing the "exclusive means" provision in the 1978 Act?**

Answer: Repealing the exclusivity provision would have serious negative consequences both for national security and for civil liberties. It would make FISA merely optional, turning the clock back to the 1970s and, if the President chose to act outside FISA, casting a cloud of constitutional doubt over what the Administration claims are critical intelligence activities. A central purpose of FISA was to place intelligence gathering on a sound constitutional basis. Senator Specter's bill, if the President took up its invitation to act without court approval, would make a constitutional case of every national security wiretap and expose to potential liability both government employees and the corporate communications service providers upon whose cooperation they depend.

2. The current compromise goes on to state: "Nothing in this Act shall be construed to limit the constitutional authority of the President to collect intelligence with respect to foreign powers and agents of foreign powers."

Question:

- **Doesn't that provision nullify the entire compromise? Doesn't this say that the President can do whatever he wants, regardless of any limits that Congress may try to impose? At the hearing, Senator Specter claimed "that line was in the FISA Act of 1978". Wasn't this provision dropped before FISA was passed in 1978?**

Answer: Yes, the language cited by Senator Specter was dropped from the FISA Act of 1978, after Congress concluded that it could and should limit the constitutional authority of the President. If the Chairman's bill passes, the President could do whatever he wants, subject to the outer limits set by the Fourth Amendment, which have never been clearly defined, and which it would be very difficult to adjudicate, given the state secrets doctrine and the standing hurdles that challenges to the President's program would face. Of course, if the government were ever to seek to introduce evidence form the TSP in a criminal case, then the constitutional issues would be squarely presented, and crucial evidence might be excluded.

43453.104

3. This provision gives the President a free hand to ignore the 1978 Act and engage in any surveillance that he believes is within his constitutional authority, without having to ask any court for authorization.

Questions:

- **Under the Chairman's legislation negotiated with the White House, would there be any limits on the President's power to collect this kind of intelligence?**

Answer: The only limit would be the Fourth Amendment, the contours of which are undefined in national security cases. However, the Hamdi and Hamdan cases indicate that the President, even in the exercise of his Commander in Chief powers, does not have a blank check, so it is possible that the Fourth Amendment would be interpreted to preclude entire classes of wiretaps executed in the name of national security. That is a risky roll of the dice in time of "war," whereas compliance with FISA would place the President's power at its zenith.

- **What role does the Chairman's proposed legislation leave for Congress in this area? What role does it leave for the courts?**

Answer: Congress retains the power of the purse, a blunt instrument. The courts retain the power to say what the law is, in particular, to conclusively interpret the Constitution, assuming that a case could ever come before them without being dismissed under the states secret doctrine or standing principles.

4. Some have suggested that, under the so-called compromise, an entire "program" of surveillance could be submitted to the Foreign Intelligence Surveillance Court for a determination that it is lawful. No individual determination would need to be made on whether particular applications of the program were lawful.

Question:

- **How do you determine whether an entire program complies with the Fourth Amendment's prohibition of unreasonable searches, without knowing which specific individuals are to be the subjects of the surveillance, and under what circumstances? Doesn't the Fourth Amendment require that information?**

Answer: Programmatic warrants are presumptively unconstitutional under the Fourth Amendment, which, as a general rules, requires particularized suspicion (i.e., searches are generally unreasonable if not based on a warrant describing with particularity the person or place to be searched). The courts have upheld general searches in administrative cases, under circumstances fundamentally different from those posed by secret intelligence searches that may result in criminal prosecution.

5. According to the compromise, any litigation challenging the legality of "classified communications intelligence activity relating to a foreign threat" must be transferred to the Foreign Intelligence Surveillance Court of Review, if the Attorney General certifies

43453.105

that further proceedings might harm national security. As you have both testified, dozens of lawsuits have been filed around the country challenging the program and challenging the participation of telecommunications companies in the surveillance.

Question:

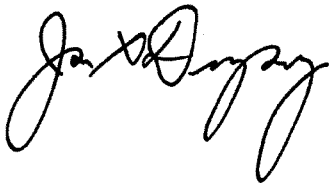
- **What is your view of the real goal of this change? Isn't this blatantly stripping the federal courts of jurisdiction, so that the President can obtain secret rulings from this secret court?**

Answer: In our view, this is forum shopping at the discretion of the government. In fact, the government would get two bites at the apple: it could keep the case in district court if it thinks the assigned judge will rule in its favor on procedural or substantive grounds or it could remove the case to the FISCR, where the case would be heard by three judges designated by the Chief Justice.

* * *

As always, the Center for Democracy & Technology is honored to be asked to present its views to the Committee. We look forward to working with all members of the Committee to achieve true, balanced FISA reform.

Sincerely,



James X. Dempsey
Vice President for Public Policy

43453.106

Senator Arlen Specter
FISA for the 21st Century
Wednesday, July 26, 2006
Questions for Mary DeRosa

1. You have complained that my bill does not include your policy preference that FISA plus FISC oversight must be the exclusive mechanism for ANY exercise of the President's authority to conduct electronic surveillance. To the extent that the President possesses some measure of inherent constitutional authority to utilize electronic surveillance in his capacity as Commander in Chief, why is of any consequence that my bill acknowledges that which is self-evident? Do you concede that Congress cannot vitiate powers vested in the President by the Constitution?

2. You testified that public perception is extraordinarily important when it comes to these surveillance programs. I agree. Don't you think that the provision in my bill that provides for judicial review both before and after the surveillance will add to the public's confidence and acceptance of the NSA program?

3. Do you think the new digital communications environment has "outpaced" FISA, and if so how might it need to be updated? Would you have any objection to the NSA program being assessed by the current FISA court?

4. Technology has changed tremendously since 1978. What are some of the technological hurdles that make FISA obsolete today? Do you agree with how S. 2453 deals with emerging technological issues? Is it feasible for the FISA Court to make the type of determinations and issue the type of program-wide warrants that the bill envisions?

43453.107

Senator Dianne Feinstein
FISA for the 21st Century
July 26, 2006

Question for Ms. DeRosa:

Background. In the 95th Congress back in 1978, language was eliminated from the 1968 Title III wiretap statute that expressly recognized the constitutional power of the President. It was replaced it with the current requirement that FISA "shall be the exclusive means" for conducting such surveillance.

In considering FISA in 1978, Congress also refused to enact language proposed by the Ford Administration that "[n]othing contained in this chapter shall limit the constitutional power of the President."

However, the Specter-White House bill now before us states, "Nothing in this Act shall be construed to limit the constitutional authority of the President to collect intelligence with respect to foreign powers and agents of foreign powers." The bill also contains other references authorizing unspecified actions "under the Constitution."

- *In your opinion, what is the impact of having this language in the bill?*

Questions for Ms. DeRosa:

Background. In the 1952 *Youngstown* case, Justice Jackson divided Presidential action into three areas:

1. When the President acts consistent with the will of Congress;
2. When the President acts in an area in which Congress has not expressed itself; and
3. When the President acts in contravention of the will of Congress.

In the first circumstance, Presidential power is at it greatest, in the third, Presidential power is at its lowest. Justice Jackson wrote that:

> "When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb, for then he

43453.108

can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter."

- *In your opinion, how will the new Specter bill be analyzed in a Youngstown analysis given the deletion of the "exclusivity" language in FISA and with the addition of new language about the President's ability to act under the constitution?*

- *What legal limits, if any, would exist on the President's ability to conduct electronic surveillance for foreign intelligence without following FISA if we pass the new Specter bill?* Please answer according to what are the legal restrictions that the Specter bill places on the President, not what DOJ or the President may or may not do.

Question for Ms. DeRosa:

Background. Sen. Specter's new FISA bill eliminates the 15-day window on surveillance outside of FISA after a declaration of war. This could be interpreted to mean that after a declaration of war the President may unilaterally wiretap whomever he chooses until the end of the war without limitation.

While wars do not have specific end dates, usually there is some identifying action that signals the end – such as surrender of one party, annexation of a territory under dispute, a peace treaty, when one party unilaterally withdraws, etc. However, in the "war on terror" it is highly unlikely that there would be a similar triggering event that would signify the end.

- *If the new Specter bill were to pass, how long would the President's authority last under the "war on terror"? Could it last decades? When would that authority end?*

Questions for Ms. DeRosa:

Background. Under the new Specter-Administration bill, a new blanket exception would be created to the FISA warrant requirement, allowing surveillance of anyone who is inside the United States but is not a U.S. person. Under the bill,

43453.109

such individuals could be wiretapped for up to a year upon a declaration by the Attorney General that they possess foreign intelligence information.

- *Does "foreign intelligence" include economic trends overseas? What else does it include? Trade policies between the U.S. and another country? The strength of the dollar in another country? Currency valuations? Foreign stock prices and market fluctuations?*

It appears that this new Specter bill would authorize wiretapping of almost any individual in the United States who is not a U.S. person so long as this certification is made by the Attorney General.

- *Is that correct? What are the limitations to such a broad authority?*

- *How would this section affect foreign workers – including skilled workers on H-1-B visas – that U.S. companies routinely bring into the United States every day? If the Attorney General certified that a skilled worker possessed foreign intelligence, would this bill allow the Government to wiretap that worker while he is here in the U.S.? Would this include all of his calls or emails with other U.S. corporate executives or other persons – without a FISA warrant or other court oversight?*

43453.110

Senator Edward M. Kennedy
Questions for the Record
From Senate Judiciary Committee hearing on "FISA for the 21st Century"
Held on July 26, 2006

To Mary DeRosa

1. From its enactment in 1978 until now, The Foreign Intelligence Surveillance Act has been the backbone of our statutory system for obtaining foreign intelligence through wiretapping or all other forms of electronic surveillance in the United States.

During the late 1970's, we knew that such surveillance could be a useful part of the Government's gathering of certain kinds of information. We also knew that it could be a deep and indiscriminate invasion of the privacy of our citizens, and that it was essential to reach a fair balance that would protect our security without infringing on citizens' basic rights.

Congress included a specific provision in the Act stating that the statutory scheme enacted was to be the exclusive means for federal agencies to conduct electronic surveillance in the United States. The legislative intent was clear. The history of the Act makes clear that the warrant procedures in the law must be followed to conduct electronic surveillance in the United States. Most important, we thought we were putting an end to the debate over the meaning and scope of the President's inherent powers. Yet, the current compromise would eliminate the provision stating that the Act is the exclusive means for authorizing foreign intelligence surveillance.

Question:

- **What is the impact of repealing the "exclusive means" provision in the 1978 Act?**

2. The current compromise goes on to state: "Nothing in this Act shall be construed to limit the constitutional authority of the President to collect intelligence with respect to foreign powers and agents of foreign powers."

Question:

- **Doesn't that provision nullify the entire compromise? Doesn't this say that the President can do whatever he wants, regardless of any limits that Congress may try to impose? At the hearing, Senator Specter claimed "that line was in the FISA Act of 1978". Wasn't this provision dropped before FISA was passed in 1978?**

43453.111

3. This provision gives the President a free hand to ignore the 1978 Act and engage in any surveillance that he believes is within his constitutional authority, without having to ask any court for authorization.

Questions:

- **Under the Chairman's legislation negotiated with the White House, would there be any limits on the President's power to collect this kind of intelligence?**
- **What role does the Chairman's proposed legislation leave for Congress in this area? What role does it leave for the courts?**

4. Some have suggested that, under the so-called compromise, an entire "program" of surveillance could be submitted to the Foreign Intelligence Surveillance Court for a determination that it is lawful. No individual determination would need to be made on whether particular applications of the program were lawful.

Question:

- **How do you determine whether an entire program complies with the Fourth Amendment's prohibition of unreasonable searches, without knowing which specific individuals are to be the subjects of the surveillance, and under what circumstances? Doesn't the Fourth Amendment require that information?**

5. According to the compromise, any litigation challenging the legality of "classified communications intelligence activity relating to a foreign threat" must be transferred to the Foreign Intelligence Surveillance Court of Review, if the Attorney General certifies that further proceedings might harm national security. As you have both testified, dozens of lawsuits have been filed around the country challenging the program and challenging the participation of telecommunications companies in the surveillance.

Question:

- **What is your view of the real goal of this change? Isn't this blatantly stripping the federal courts of jurisdiction, so that the President can obtain secret rulings from this secret court?**

43453.112

Central Intelligence Agency

Washington, D.C. 20505

6 October 2006

The Honorable Arlen Specter
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Attention: Barr Huefner

Dear Mr. Chairman:

Enclosed please find the responses to your 2 August 2006 letter regarding follow-up questions from my testimony before your Committee at the "FISA for the 21st Century" hearing. Please note that this is a partial response and the remaining inquires will be answered as soon as possible. Given that I testified under the auspices of my former capacity as Director of the National Security Agency, rather than my current position, I am coordinating the remaining responses with the appropriate agencies.

As always, I appreciate the interest Congress takes in the Intelligence Community and was pleased to have the opportunity to testify before your Committee.

Sincerely,

Michael V. Hayden
General, USAF
Director

Enclosures

Questions for the Record
FISA for the 21st Century -- July 26, 2006 Hearing
U.S. Senate Judiciary Committee

Responses to Questions from Chairman Arlen Specter (R-PA)
to
Director of the CIA, General Michael Hayden

QUESTION: 1. Is it feasible for the FISA Court to make the type of determinations and issue the type of program-wide warrants that my bill envisions?

ANSWER: (U) Yes. The types of findings that the bill calls for the Foreign Intelligence Surveillance Court ("FISC") to make in authorizing electronic surveillance programs are comparable to the determinations that the court has made for years in authorizing surveillance orders under the Foreign Intelligence Surveillance Act of 1978 ("FISA"). Indeed, many of the "necessary findings" set forth in Section 6 of the bill that the FISC would have to make before authorizing surveillance mirror those contained in section 105 of FISA, 50 U.S.C. § 1805(a).

QUESTION: 2. Under my bill, the Administration is required to submit certain information about the so-called Terrorist Surveillance Program. Is this information sufficient to allow a FISA Court judge to determine the NSA program's constitutionality?

ANSWER: (U) We believe the information is sufficient to allow the FISC to determine the constitutionality of an electronic surveillance program, including the Terrorist Surveillance Program described by the President. The bill requires any application for an order authorizing an electronic surveillance program to include detailed information on a number of subjects, including "an explanation of how the electronic surveillance program is reasonably designed to ensure that the communications to be intercepted are communications of or with . . . a foreign power . . . [or] an agent of a foreign power that is engaged in international terrorism activities or in preparation therefore; or . . . a person reasonably believed to have communication with or be associated with a foreign power that is engaged in international terrorism activities or in preparation therefore or an agent of [such] a foreign power." *See* § 5. The bill would also require any application submitted to include a statement of the means and operational procedures by which the electronic tracking will be executed and affected, a statement of proposed minimization procedures, and, for programs that are being reauthorized, a statement of facts concerning the implementation of the program. *Id.* Moreover, in the event that the court concludes it lacks sufficient information on which to make a determination, the bill specifically provides that the FISC "may require the Attorney General to furnish such other information as be necessary to make a determination" (*id.*) that, among other things, "approval of the electronic surveillance program in the application is consistent with the Constitution of the United States." *Id.* § 6.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00167 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.114

QUESTION: 3a. Technology has changed tremendously since 1978. What are some of the technological hurdles that make FISA obsolete today?

ANSWER: (U) FISA was written in 1978 in a manner that took into account then-current technology, making the necessity to obtain a court order dependent in part on the means of communication and the location in which the Government sought to acquire it. While we believe the intent of the 1978 law was to protect the private communications of people in the United States by imposing a judicial process when such persons were the targets of surveillance, the law does not accomplish this well in today's technological environment. The principal differences between the 1978 telecommunications environment and that of today result from both the evolution of the internet and the changed circumstances in which particular communications technologies are used. Because FISA is technology-specific, the result of these changes is that the FISA frequently requires judicial authority to collect the communications of non-U.S. persons outside the United States. This clogs the FISA process with applications for court orders that have little to do with protecting U.S. privacy rights. The FISA should be amended so that it is technology-neutral. This would return it to its original purpose of focusing privacy protections on Americans in the United States.

QUESTION: 3b. Do you agree with how S.2453 deals with emerging technological issues?

ANSWER: (U) The revolution in telecommunications technology has extended the actual impact of the FISA regime far beyond what Congress could ever have anticipated in 1978. At present, the requirement for a court order is determined in part by the location at which surveillance is conducted, and the particular communications technology employed. Neither of these factors is selected by a communicant, yet the Government's obligation to obtain a court order turns on these and similar factors that do not go to the essence of the issue: what kind of protection from Governmental intrusion ought to be provided to people in the United States, and to U.S. persons abroad? The intent of S.2453 as we understand it is to return the statute to its original intent. While I agree with this goal, it is necessary that we review the legislation to determine how the proposed language will impact the operational effectiveness of each of the intelligence agencies that rely on the authorities set out in the FISA.

QUESTION: 4. What recommendations do you have to improve my legislation?

ANSWER: (U) The Administration is proud to have worked closely with you on this bill, and we already have given you numerous comments on earlier drafts. We look forward to working further with you and Congress as we move this bill through the legislative process. Because of the importance of FISA reform, we hope that Congress will move expeditiously. All suggestions we had for improving the draft legislation have already been made in the informal process of consultation.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00168 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.115

QUESTION: 5. In your opinion, would the President continue the Terrorist Surveillance Program if the Foreign Intelligence Surveillance Court or the Court of Review concluded that the program is unconstitutional?

ANSWER: (U) Subject, of course, to ordinary appellate review of such a decision, I am confident that the President would terminate the Terrorist Surveillance Program if there were a final judgment of the FISC or the Foreign Intelligence Surveillance Court of Review concluding that the Program is unconstitutional. I am also confident, however, that the Terrorist Surveillance Program is lawful and that the courts will come to the same conclusion.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00169 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.116

Questions for the Record

FISA for the 21st Century -- July 26, 2006 hearing
U.S. Senate Judiciary Committee

Responses to Questions posed by Senator Charles E. Schumer
to
Director of the CIA, General Michael Hayden

QUESTION: 1.a. On July 13, Senator Specter announced that he had reached a deal with the White House on his legislation to authorize the Terrorist Surveillance Program and rewrite much of the Foreign Intelligence Surveillance Act (FISA). This was just two weeks after the Supreme Court's decision in *Hamdan*, which many have characterized as a rebuke of the Administration's legal defense of the President's warrantless surveillance program. Do you continue to believe that the NSA Surveillance Program is legal and Constitutional and that it would survive any legal challenge in the FISA Court?

ANSWER: (U) Yes. As Assistant Attorney General Moschella explained in his detailed response to your June 30 letter, it is our considered legal judgment that Supreme Court's decision in *Hamdan v. Rumsfeld* does not affect the analysis set forth in the Department's January 19th *Legal Authorities* memorandum outlining the legal basis for the Terrorist Surveillance Program. As the Moschella letter explains, there are many reasons to support that conclusion, but at bottom, the relevant statutory scheme at issue in *Hamdan* is fundamentally different from the one implicated by the Terrorist Surveillance Program. FISA expressly contemplates that Congress may authorize electronic surveillance through a subsequent statute without amending FISA. *See* 50 U.S.C. § 1809(a)(1) (prohibiting electronic surveillance "except as authorized by statute"). The primary provision at issue in *Hamdan*, Article 21 of the Uniform Code of Military Justice ("UCMJ"), has no analogous provision. Moreover, the Supreme Court recognized in *Hamdi v. Rumsfeld*, 542 U.S. 519 (2004), that the Force Resolution satisfies a statute similar to FISA prohibiting detention of U.S. citizens "exception pursuant to an Act of Congress." 18 U.S.C. § 4001(a). Because the Terrorist Surveillance Program implicates a statutory regime analogous to the one at issue in *Hamdi*, we believe that the reasoning of that decision is far more relevant to the Program than *Hamdan*. Because of that, we believe that the Program would survive a legal challenge.

QUESTION: 1.b. If the [A]dministration has "the authority, both from the Constitution and the Congress, to undertake this vital program," as President Bush asserted in January, what need is there to legislate on this issue from your perspective?

ANSWER: (U) Although the Administration has made it clear that no additional legislation is needed to authorize the Terrorist Surveillance Program, the Administration

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00170 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.117

has been interested in working with Congress on electronic surveillance issues, including legislation addressing the Terrorist Surveillance Program. Indeed, as the Attorney General noted, the Administration previously discussed the idea of seeking specific authorization of the Terrorist Surveillance Program, but a bipartisan group of legislators warned that it would be unlikely that such legislation could be enacted without compromising the Program by disclosing its existence. *See* Remarks by Homeland Security Secretary Chertoff and Attorney General Gonzales on the USA PATRIOT Act, *available at* http://www.dhs.gov/dhspublic/display?content=5285. The legislation proposed by Chairman Specter and Senator DeWine would confirm and supplement the President's authority in this area and would regularize the procedures for the review and reauthorization of the Program. In addition, the Chairman's legislation would make many long overdue amendments to update FISA to account for technological changes that have occurred during the past 30 years.

QUESTION: 1.c. Would you prefer that Congress not legislate in this area at all?

ANSWER: (U) No. As indicated above, the Administration wants to work with Congress on electronic surveillance issues, including legislation addressing the Terrorist Surveillance Program.

QUESTION: 1.d. Did the Supreme Court's recent ruling in *Hamdan* play any role in the Administration's decision to support Senator Specter's legislation?

ANSWER: (U) No. The Administration was working with Senator Specter on this legislative package before the *Hamdan* decision was announced.

QUESTION: 2. Senator Specter has characterized his bill as simply allowing the Court to decide the Constitutionality of the program, including whether the President has the authority to authorize the surveillance. It has been said that if kept in its precise current form, the President will submit the program to the FISA Court. Why doesn't the Administration just submit the program to the FISA Court now, without any legislation?

ANSWER: (U) The answer to this question is being coordinated with the appropriate entities within the Executive Branch and will be provided separately.

QUESTION: 3. If the Specter bill is passed in its current form, what signing statement do you anticipate the President issuing in connection with it?

ANSWER: (U) The answer to this question is being coordinated with the appropriate entities within the Executive Branch and will be provided separately.

QUESTION: 4. If the Specter bill is passed in its current form, and the Administration then voluntarily submitted the program to the FISC, would the Administration argue that the Specter bill authorized the NSA's Terrorist Surveillance Program.?

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00171 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.118

ANSWER: (U) The answer to this question is being coordinated with the appropriate entities within the Executive Branch and will be provided separately.

QUESTION: 5. Do you believe that the portion of the Specter bill that allows the President to submit the NSA surveillance program to the FISA Court is constitutional? Specifically, do you believe this provision does not run afoul of the constitutional proscription against advisory opinions?

ANSWER: (U) The answer to this question is being coordinated with the appropriate entities within the Executive Branch and will be provided separately.

QUESTION: 6.a. The Specter bill provides that any cases pending right now – upon application by the Attorney General – must be transferred to the FISA Court of Review. The bill also provides that the decision of that FISA Court "shall be subject to certiorari review in the United States Supreme Court." Is it your understanding that one who is challenging a FISA Court decision favorable to the government may obtain review before the Supreme Court under the bill?

ANSWER: The answer to this question is being coordinated with the appropriate entities within the Executive Branch and will be provided separately.

QUESTION: 6.b. What are the arguments against allowing the constitutional review in a traditional Federal District Court, with expedited review, to the Supreme Court, so long as the court applies the procedures and standards of the Classified Information Procedures Act?

ANSWER: (U) The answer to this question is being coordinated with the appropriate entities within the Executive Branch and will be provided separately.

QUESTION: 7. During his February appearance before the Committee, Senator Biden asked Attorney General Gonzales what harm had been caused by public disclosure of the warrantless surveillance program. He responded: "You would assume that the enemy is presuming we are engaged in some kind of surveillance. But if they're not reminded about it all the time in the newspapers and in stories, they sometimes forget." When I asked him the same question in July, he deferred to the intelligence community.

ANSWER: (U) The answer to this question is being coordinated with the appropriate entities within the Executive Branch and will be provided separately.

QUESTION: 7a. Do you have a better answer as to how the disclosure that wiretapping is going on harmed national security?

ANSWER: (U) Disclosure of this Program puts at risk efforts by the U.S. Government to prevent catastrophic al Qaeda-sponsored acts within the United States. Even the

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00172 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.119

smallest reduction in the effectiveness of the President's Program could be catastrophic in an environment in which we cannot afford to miss one plot, one event, one individual, or one movement that might have been discovered through this Program.

(U) In general, while it is impossible to assess the full impact of unauthorized disclosures on U.S. intelligence capabilities, the damage is staggering, with some of the losses being permanent and irreversible.

(U) Foreign intelligence services and non-state groups such as terrorists capitalize on this public hemorrhage of U.S. secrets, which becomes a serendipitous "bonus" enriching the unclassified open source collection activities many of our opponents already perform.

(U) These unauthorized disclosures also have a chilling effect on cooperation, affecting both friendly governments and individual clandestine sources. To put it starkly, if we cannot be trusted to keep our own secrets, why should others share sensitive information with us?

QUESTION: 8. Do you have legal or constitutional concerns about the use of warrantless physical searches in the United States?

ANSWER: (U) The answer to this question is being coordinated with the appropriate entities within the Executive Branch and will be provided separately.

QUESTION: 9. To your knowledge, has the Administration ever used its commander-in-chief powers or the AUMF to justify warrantless physical searches?

ANSWER: (U) The answer to this question is being coordinated with the appropriate entities within the Executive Branch and will be provided separately.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00173 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.120

Questions for the Record

FISA for the 21st Century -- July 26, 2006 hearing
U.S. Senate Judiciary Committee

Responses to Questions posed by Senator Dianne Feinstein
to
Director of the CIA, General Michael Hayden

QUESTION: 1.a. Are there any intelligence programs carried out by your agencies, or otherwise within the intelligence community that you know of, that have not been briefed to the Congressional intelligence committees?

ANSWER: (U) Consistent with long-standing practice and the notification provisions of the National Security Act of 1947, CIA keeps the Congressional intelligence committees fully and currently informed of CIA intelligence activities through appropriate briefings. I defer to the Office of the Director of National Intelligence and the heads of the other elements of the intelligence community on whether there are any intelligence programs outside of CIA that have not been briefed to the intelligence committees.

QUESTION: 1.b. Did anyone in the Administration offer, grant, or otherwise provide in any way some sort of promise of immunity or offer of protection against civil or criminal liability to telecommunications or internet service providers or financial entities or any other company for their cooperation in any of the surveillance programs? If yes, under what legal authority?

ANSWER: (U) Operational information about the Program is highly classified and exceptionally sensitive. Revealing information about the operational details of the Program could compromise its value and facilitate terrorists' attempts to evade it. Accordingly, we cannot confirm or deny operational details of the Program in this setting. As you are aware, the operational details of the Program have been and continue to be reviewed by the oversight committees and, in certain circumstances, congressional leadership.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00174 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.121

Questions for the Record

FISA for the 21st Century -- July 26, 2006 hearing
U.S. Senate Judiciary Committee

Responses to Questions posed by Senator Patrick Leahy
to
Director of the CIA, General Michael Hayden

QUESTION: 1.a. You and the President have talked about listening to phone calls involving suspected al Qaeda terrorists where one party to the conversation is overseas. Let's say the suspected al Qaeda terrorist is overseas, in Yemen, say, or Iraq, and the government is targeting his phone calls. That does not require a warrant under FISA or any other law, does it, even when he calls someone in the United States?

ANSWER: (U) In the mid-1970's, several federal circuit courts of appeals held that the President possesses the authority under the constitution to engage in warrantless searches and seizures – to include electronic surveillance – for the purpose of obtaining foreign intelligence information. The FISA in 1978 imposed a statutory requirement on the President to obtain a court order to conduct electronic surveillance in some situations unless he was otherwise authorized to do so by law. Those situations, as noted above, are dependent on factors such as the location from which the surveillance is carried out and the particular communications technology in question.

(U) Therefore, turning to the specific example in the question, the appropriate answer is: "It depends." While it is true that the constitution does not require a "warrant" to target the calls of a foreign terrorist overseas, the FISA may require the Government to obtain a court order. Whether it would depends on factors that we think are not relevant to the heart of the issue, such as the location from which the Government seeks to acquire the communications and the technology employed to complete the call.

QUESTION: 1.b. At least some of the time, what the President is talking about can already be carried out legally under FISA as written, isn't that correct?

ANSWER: (U) It is true that with respect to a single communication traversing the global communications infrastructure, the terms of Title I of the FISA would require the Government to obtain a court order to acquire it at some times and in some locations, and not at other times and locations.

(U) Current law is not agile enough to handle the threat posed by sophisticated international terrorist organizations like al Qaeda. This is because the FISA has not kept

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00175 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.122

pace with communication technology and was not designed for the types of threats we now face. As the failed UK airplane bombing plot shows, terrorism is still a real threat and FISA should be modernized to improve its effectiveness as a counterterrorism tool.

QUESTION: 2.a. You said at your press conference on December 19, 2005, that surveillance under the so-called Terrorist Surveillance Program is generally for "far shorter periods of time" than surveillance under FISA, and is " not designed to collect reams of intelligence, but to detect and warn...about attacks." At our hearing on July 26, you indicated that the Terrorist Surveillance Program is used "when we are in hot pursuit of" international communications involving al Qaeda. Does warrantless surveillance under this program cease once the "pursuit" is no longer "hot" and if not, why not?

ANSWER: (U) The answer to this question is being coordinated with the appropriate entities within the Executive Branch and will be provided separately.

QUESTION: 2.b. What is the longest period of time that communications have been monitored under this program?

ANSWER: (U) Operational information about the Program is highly classified and exceptionally sensitive. Revealing information about the operational details of the Program could compromise its value and facilitate terrorists' attempts to evade it. Accordingly, we cannot confirm or deny operational details of the Program in this setting, including the longest period of time that communications have been monitored under the Program. As you are aware, the operational details of the Program have been and continue to be reviewed by the oversight committees and, in certain circumstances, congressional leadership.

QUESTION: 2.c. What is the average time?

ANSWER: (U) Operational information about the Program is highly classified and exceptionally sensitive. Revealing information about the operational details of the Program could compromise its value and facilitate terrorists' attempts to evade it. Accordingly, we cannot confirm or deny operational details of the Program in this setting, including the average length of time that communications have been monitored under the Program. As you are aware, the operational details of the Program have been and continue to be reviewed by the oversight committees and, in certain circumstances, congressional leadership.

QUESTION: 2.d. What if anything prevents the government from seeking an individualized warrant when surveillance continues beyond the "hot pursuit" stage?

ANSWER: (U) After September 11th, speed and agility were especially crucial in fulfilling the President's constitutional obligation of protecting the Nation from further attacks. The Terrorist Surveillance Program targets communications only where one party is outside the United States and there is probable cause to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. FISA itself uses a "probable cause" standard.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00176 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.123

Questions for the Record

FISA for the 21st Century -- July 26, 2006 hearing
U.S. Senate Judiciary Committee

Responses to Questions posed by Senator Edward M. Kennedy
to
Director of the CIA, General Michael Hayden

QUESTION: 1. Is the standard used by the NSA reasonableness or probably cause, in determining the targets for wiretapping under the NSA's warrantless wiretapping program? Has the standard ever changed from "probable cause" at any time, for any reasonable period, since September 11th?

ANSWER: (U) The Terrorist Surveillance Program is narrowly tailored to target for interception only communications where one party is outside the United States and there are reasonable grounds to believe that at least one party is a member or agent of al Qa'ida or an affiliated terrorist organization. The "reasonable grounds to believe" standard is a "probable cause" standard of proof, *see Maryland v. Pringle*, 540 U.S. 366, 371 (2003) ("We have stated . . . that '[t]he substance of all the definitions of probable cause is a reasonable ground for belief of guilt.'"). The Program has consistently employed this standard.

QUESTION: 2.a. What is the justification for a standard that is even broader than the current standard, which requires probable cause that one person involved in the communication is directly "affiliated with al Qaeda" or associated with al Qaeda." [The standard most recently articulated by General Hayden at the July 26, 2006 hearing before the Senate Judiciary Committee]?

ANSWER: (U) The answer to this question is being coordinated with the appropriate entities within the Executive Branch and will be provided separately.

QUESTION: 2.b. What would be the basis and legal standard to conclude that a U.S. person is "associated with" al Qaeda or an organization determined to be affiliated with al Qaeda under the proposed legislation?

ANSWER: (U) The answer to this question is being coordinated with the appropriate entities within the Executive Branch and will be provided separately.

QUESTION: 3.a. Members of the Administration have repeatedly claimed that the publicly announced program has saved an untold number of American lives. Why

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00177 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.124

did the Administration insist on a bill that would allow the authorization of a program that spies on even more Americans?

ANSWER: (U) The answer to this question is being coordinated with the appropriate entities within the Executive Branch and will be provided separately.

QUESTION: 3.b. Is this just another attempt to expand Executive authority even further, or does the Administration have specific, documented need to spy on far larger numbers of innocent Americans than are at risk under the current program?

ANSWER: (U) The answer to this question is being coordinated with the appropriate entities within the Executive Branch and will be provided separately.

QUESTION: 3.c. What are the Administration's justifications for such a broad program that far exceed [sic] the program described publicly by each of you in past statements and in testimony before this Committee?

ANSWER: (U) The answer to this question is being coordinated with the appropriate entities within the Executive Branch and will be provided separately.

QUESTION: 4.a. What is the legal definition of an "affiliate terrorist organization?"

ANSWER: (U) The answer to this question is being coordinated with the appropriate entities within the Executive Branch and will be provided separately.

QUESTION: 4.b. Who makes the determination that an organization is one that is an "affiliate terrorist organization" to al Qaeda? What criteria are used?

ANSWER: (U) The answer to this question is being coordinated with the appropriate entities within the Executive Branch and will be provided separately.

QUESTION: 4.c. How quickly is such a determination made?

ANSWER: (U) The answer to this question is being coordinated with the appropriate entities within the Executive Branch and will be provided separately.

QUESTION: 5. Will the Administration agree to report on the legal standards being used now? Obviously, the standards provided to Congress in 2000 have become outdated and, perhaps, obsolete.

ANSWER: (U) The answer to this question is being coordinated with the appropriate entities within the Executive Branch and will be provided separately.

QUESTION: 6. The procedures required by FISA are often blamed for the Administration's difficulties in predicting and responding to 9/11. However, as has

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00178 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.125

been widely reported, the NSA intercepted statements on September 10th referring to the September 11th attacks, but these warnings were not translated until September 12th - too late to provide any warning of the devastation planned for New York and Washington, DC. In the five years since September 11th, the media has continued to report that intelligence agencies, including the NSA, do not have the ability to keep up with the translation demands of the war on terror.

QUESTION: 6.a. In your tenure at the NSA, what did you and others do to hire more translators of Arabic and other languages that are critical to fighting terrorism?

ANSWER: (U) The counterterrorism crisis and continuing military campaign have placed an enormous burden on NSA's population of civilian and military language and intelligence analysts. Supplemental funding has helped to expand the contract linguist population in several low-density crisis languages, increase analytic training across the extended SIGINT enterprise, immediately activate a civilian Cryptologic Reserve Program, and significantly expand the Military Reserve program. The Agency continues to need skilled linguists and analysts, and is aggressively pursuing qualified applicants.

QUESTION: 6.b. During your time at the NSA, was there a backlog in translating intelligence information? If so, what was the average amount of time between an interception that took place under surveillance and its translation?

ANSWER: (U) Yes, depending on the source of the information there could be time lags between when it was intercepted and when it was available for a linguist to review at NSA Headquarters. Given the wide differences in targets and the methods of communicating, it is very difficult to derive at an estimate of an average time lag.

QUESTION: 6.c. To your knowledge, has there been an improvement in the translation backlog?

ANSWER: (U) As Former Director of the NSA, I appreciate the Senator's interest in improvement of the translation backlog. However, this question is most appropriately answered by the current NSA leadership. I will forward your question to the NSA and ask them to respond to you directly.

QUESTION: 6.d. If there was a backlog in translation, what impact did this have on your ability to protect America from future terrorist attacks?

ANSWER: (U) There is no reason to think the translation backlog had any effect on NSA's ability to help protect America from terrorist attacks. First, it is important to bear in mind that SIGINT is only one component of America's defense and it is highly unlikely, given the vague and fragmentary nature of terrorist communications, that a single piece of SIGINT will ever be able to prevent a terrorist attack. What SIGINT can do is work hand in glove with other intelligence agencies, the military, and law enforcement to enable key takedowns, as occurred recently in the UK, so that the details

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00179 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.126

of a plot can be uncovered through interrogation and forensics exploitation. That being said, the translation backlog can prevent the timely delivery of key information to NSA's customers and stall development efforts against new targets.

QUESTION: 6.e. What resources do you believe are required for the NSA to increase its translation efficiency to a level at which translation will not be an impediment to protecting America?

ANSWER: (U) NSA must have a robust hiring and contracting program for GWOT languages, with a particular focus on the identification and recruitment of high-caliber, clearable native speakers, and the agility to adapt to the constantly-changing needs of the terrorist target set. NSA will also need Human Language Tools to help focus efforts on the most lucrative leads, since it will never be possible to fully exploit all of the material that we have the capacity to collect. Finally, NSA needs a high-quality GWOT language training program to help our current linguists acquire the necessary skills to address this challenging target set.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00180 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.127

Questions for the Record

FISA for the 21st Century -- July 26, 2006 hearing
U.S. Senate Judiciary Committee

Responses to Questions posed by Senator Dick Durbin
to
Director of the CIA, General Michael Hayden

QUESTION: 1. In your testimony you state:

> **The revolution in telecommunications technology has extended the actual impact of the FISA regime far beyond what Congress could have ever anticipated in 1978. And I don't think that anyone could make the claim that the FISA statute is optimized to deal with a 9/11 or to deal with a lethal enemy who likely already had combatants in the United States.**

If the Foreign Intelligence Surveillance Act is not "optimized to deal with a 9/11," as you testified, why, almost five years after 9/11 and after we enacted and reauthorized the PATRIOT Act, has the Administration not previously requested changes in the law to "optimize" FISA?

ANSWER: (U) The consensus view in the discussions with Members of Congress was that it was unlikely, if not impossible, that more specific legislation could be enacted without compromising the Terrorist Surveillance Program by disclosing operational details, limitations, and capabilities to our enemies. Such disclosures would necessary have compromised our national security.

QUESTION: 2. On January 25, 2006, over six months ago, Senators Reid, Kennedy and Feingold and I [sic] sent a letter to President Buss asking what changes in the law he believes are necessary to permit effective surveillance of suspected terrorists, and why these changes are needed. We still have not received a response to this letter, which I have attached to these questions. Please respond to the questions raised in our letter.

ANSWER: (U) The answer to this question is being coordinated with the appropriate entities within the Executive Branch and will be provided separately.

QUESTION: 3. It is somewhat unusual for the Director of the Central Intelligence Agency to testify at a hearing on warrantless surveillance of Americans in the United States. Did you appear at this hearing solely because of your role in the

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00181 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.126

development of the NSA's warrantless surveillance program? Can you assure me that the CIA is not engaged in any surveillance of Americans inside the United States?

ANSWER: (U) I came at the invitation of the Committee Chairman. Regarding whether or not CIA is engaged in any surveillance of Americans inside the United States, Section 2.4 of Executive Order 12333 prohibits the CIA from engaging in electronic surveillance inside the United States except as a countermeasure to hostile electronic surveillance or for training and testing purposes, which are done under rules approved by the Attorney General. The CIA operates in conformance with this Executive Order prohibition and does not pursue electronic surveillance inside the U.S.

QUESTION: 4. We met in my office in May 10, 2006. At the time, you told me that Chairman Specter's National Security Surveillance Act was considerably broader than the President's warrantless surveillance program. Is that still your opinion?

ANSWER: (U) Yes, because S. 2453 defines electronic surveillance program as a program to engage in electronic surveillance to gather foreign intelligence information or to protect against international terrorism or clandestine intelligence activities by obtaining the substance of or information regarding electronic communications sent by, received by, or intended to be received by a foreign power, an agent or agents of a foreign power, or a person or persons who have had communication with a foreign power seeking to commit an act of international terrorism or clandestine intelligence activities against the United States. This makes S. 2453 broader than TSP because it covers many types of electronic surveillance.

QUESTION: 5. On January 23, 2006, you gave a speech at the National Press Club on the NSA's warrantless surveillance program. You said, "Had this program been in effect prior to 9/11, it is my professional judgment that we would have detected some of the 9/11 al Qaeda operatives in the United States and we would have identified them as such."

QUESTION: 5.a. What is the basis for your conclusion?

ANSWER: (U) According to the 9-11 Joint Inquiry report, after the meeting of al-Qaeda operatives in Malaysia, Khalid al-Mihdhar entered the United States in January 2000. Thereafter, the Intelligence Community obtained information indicating that an individual named "Khaled" at an unknown location had contacted a suspected terrorist facility in the Middle East. It was not until after September 11, 2001 that the FBI determined from domestic toll records that these contacts had been made from future hijacker Khalid al-Mihdhar while he was living within the domestic United States. Because the Terrorist Surveillance Program is focused on precisely this type of communication, i.e., communications where at least one party is outside the United States and there are reasonable grounds (probable cause) to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization,

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00182 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.129

the Program would have identified a contact between a number in the United States with a suspected terrorist facility in the Middle East.

QUESTION: 5.b. Did the government have legal authority before 9/11 to conduct electronic surveillance on the calls and e-mails of suspected terrorists?

ANSWER: (U) Yes. On January 19, 2006, the Department of Justice released a 42-page paper setting out a comprehensive explanation of the legal authorities supporting the Program. *See Legal Authorities Supporting the Activities of the National Security Agency Described by the President* (Jan. 19, 2006). That paper reflects the substance of the Department's legal analysis of the Terrorist Surveillance Program. In addition, the Intelligence Community has conducted electronic surveillance for years under the authority of Executive Order 12333 and its predecessors. Executive Order 12333, which was issued by President Reagan in 1981 and is currently in effect, governs the conduct of intelligence activities applicable to all intelligence agencies, and also identifies specific responsibilities for each of the agencies. The overall scheme of the Order is premised upon the determination that the "[c]ollection of [foreign intelligence information] is a priority objective and will be pursued in a vigorous, innovative and responsible manner that is consistent with the Constitution and applicable laws and respectful of the principles upon which the United States was founded." Primary among these principles is the need to respect the rights of U.S. persons.

QUESTION: 6. In your January 23rd speech, you said the NSA program "is not a drift net over Dearborn or Lackawanna or Freemont, grabbing conversations, that we then sort out by these alleged keyword searches or data-mining tools or other devices that so-called experts keep talking about." On the other hand, Homeland Security Secretary Michael Chertoff has said the NSA is "culling through literally thousands of phone numbers" and "trying to sift through an enormous amount of data very quickly." Moreover, USA Today reports that the NSA has collected the phone call records of tens of millions of Americans into what one source in the story called "the largest database ever assembled in the world."

QUESTION: 6.a. Does the NSA maintain such a database?

ANSWER: (U) The Administration has neither confirmed nor denied the accounts referenced in the USA Today story. My January 23, 2006 speech was referring to the TSP program discussed by the President in his December 17, 2005, statement.

QUESTION: 6.b. Are there other NSA programs, besides the warrantless surveillance program, that comb through phone calls and e-mails to pick out communications of interest?

ANSWER: (U) It would be inappropriate to discuss in this setting the existence (or non-existence) of specific intelligence activities or the operations of any such activities. Consistent with long-standing practice, the Executive Branch notifies Congress

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00183 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.130

concerning the classified intelligence activities of the United States through appropriate briefings of the oversight committees and congressional leadership.

QUESTION: 7. On July 7, 2006, Deputy Defense Secretary Gordan England issued a memo (the England memo) stating that all Defense Department personnel are required to abide by Common Article 3 of the Geneva Conventions. On July 18, 2006, when Attorney General Gonzales appeared before the Judiciary Committee, he said that all U.S. personnel, including intelligence personnel, are now required to abide by Common Article 3. Do you agree with Attorney General Gonzales?

ANSWER: (U) Yes.

QUESTION: 8. The England memo directs DoD leadership as follows: "You will ensure that all DoD personnel adhere to these standards. In this regard, I request that you promptly review all relevant directives, regulations, policies, practices and procedures under your purview to ensure that they comply with the standards of Common Article 3?"

ANSWER: (U) A review at CIA of relevant directives, regulations, policies, practices and procedures began shortly after the *Hamdan* decision was announced without the need of a memo directing such a review.

QUESTION: 9. Are all CIA directives, regulations, policies, practices and procedures required to comply with the standards of Common Article 3?

ANSWER: (U) CIA directives, regulations, policies, practices and procedures required to comply with U.S. law. They therefore may not authorize conduct that would violate U.S. obligations under Common Article 3 of the Geneva Conventions.

QUESTION: 10. What steps have you taken to implement the *Hamdan v. Rumsfeld* ruling on Common Article 3? Have any specific interrogation techniques been prohibited as a result of the *Hamdan v. Rumsfeld* ruling on Common Article 3?

ANSWER: (U) I am not going to discuss any CIA interrogation techniques in an unclassified letter. I can confirm for you that CIA will comply with U.S. law, including U.S. obligations under Common Article 3 of the Geneva Conventions.

QUESTION: 11. What steps have you taken to implement the Detainee Treatment Act of 2005? Have any specific interrogation techniques been prohibited as a result of the Detainee Treatment Act?

ANSWER: (U) I am not going to discuss any CIA interrogation techniques in an unclassified letter. I can confirm for you that CIA will comply with U.S. law, including the Detainee Treatment Act.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00184 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.131

QUESTION: 12. As a Senate Armed Services Committee [sic] on March 17, 2005, then-CIA Director Porter Goss described waterboarding (the use of a wet towel and dripping water to induce the misperception of drowning) as a "professional interrogation technique." Do you agree with that characterization?

ANSWER: (U) I have read the transcript of then-Director Goss's appearance before the Senate Armed Services Committee on March 17, 2005, and I believe interpreting the exchange between Director Goss and Senator McCain on page 14 of the transcript as Director Goss describing waterboarding as a professional interrogation technique is a misreading. Senator McCain had asked Director Goss whether the Director believed there were sufficient policy guidelines in place for interrogations. As Director Goss was answering, Senator McCain interjected, "Well, some of those policies at one time were to make one have the prisoner feel that they were drowning." Director Goss responded, "You're getting into, again, an area of what I will call professional interrogation techniques, and I would like. . ." Therefore, what Director Goss did was to advise the senator that he was not going to discuss professional interrogation techniques in an open session. That is, he was not going to respond to questions on techniques, including whether any specific method was an interrogation technique. I too will not discuss what CIA's interrogation methods were or were not in an unclassified letter.

QUESTION: 13. Does waterboarding constitute torture or cruel, inhuman or degrading treatment?

ANSWER: (U) You are asking for a legal judgment, for which I respectfully refer you to the Department of Justice.

QUESTION: 14. Is waterboarding humane?

ANSWER: (U) You are asking for a legal judgment, for which I respectfully refer you to the Department of Justice.

QUESTION: 15. Is waterboarding consistent with Common Article 3 of the Geneva Conventions?

ANSWER: (U) You are asking for a legal judgment, for which I respectfully refer you to the Department of Justice.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00185 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.132

August 3, 2006

Mayer, Brown, Rowe & Maw LLP
71 South Wacker Drive
Chicago, Illinois 60606-4637

Main Tel (312) 782-0600
Main Fax (312) 701-7711
www.mayerbrownrowe.com

John R. Schmidt
Direct Tel (312) 701-8597
Direct Fax (312) 706-8397
jschmidt@mayerbrownrowe.com

United States Senate
Committee on the Judiciary
Attention: Barr Heufner
Senate Judiciary Committee
224 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Mr. Huefner:

I am in receipt of your letter dated August 2, 2006, in which you enclosed written questions from Committee members regarding the July 26, 2006 hearing on "FISA for the 21st Century".

My answers are attached herewith and a copy is being electronically sent to your office.

Sincerely,

John R. Schmidt

Enclosure

Berlin Brussels Charlotte Chicago Cologne Frankfurt Houston London Los Angeles New York Palo Alto Paris Washington, D.C.
Independent Mexico City Correspondent: Jauregui, Navarrete y Nader S.C.

Mayer, Brown, Rowe & Maw LLP operates in combination with our associated English limited liability partnership in the offices listed above.

Senator Arlen Specter
FISA for the 21st Century
Wednesday, July 26, 2006
Questions for John Schmidt

Question:

1. **How do you think FISA should be modified? In your opinion, should FISA be altered so that the NSA may monitor phone calls in and out of the United States, when the target of the surveillance are suspected members of al queda?**

Answer:

1. I think it is important to establish a mechanism that allows the effective monitoring of calls into and out of the U.S. that involve suspected Al Qaeda members—and also calls among suspected Al Qaeda members within this country when that is necessary. The best mechanism to do this is to expand the jurisdiction of the FISA court (at the lower court or the Court of Review level) to allow court approval of the constitutionality of a surveillance program that the President, the Attorney General and the security agencies believe is reasonable and necessary to achieve that objective. No one can say today what the precise elements of such a program need to be over the life of our need to combat the threat of Al Qaeda terrorism, let alone over the future course of our need to deal with other foreign threats to the U.S. A court approval process is flexible and not tied to the specific elements of any current program, yet gives to all parties—including the President—the assurance that actions are being taken consistent with the Constitutional rights of American citizens.

Question:

2. **In your opening statement March 31, 2006, when you testified before the Senate Judiciary Committee regarding *"An Examination of the Call to Censure the President"*, you stated that Article II of the Constitution provided the President with authority to authorize the NSA program, "notwithstanding the fact that it was inconsistent with the terms of the Foreign Intelligence Surveillance Act."**

   a. **Do you feel that my NSSA bill conflicts with the President's Article II Commander-in-Chief powers in any way? If so, how?**

Answer:

2. No. I believe your bill is consistent with the President's Article II power. Giving the FISA court (or the FISA Court of Review) jurisdiction to approve a surveillance program does not conflict with the President's Article II power. Moreover, the provision of the bill that acknowledges that the President retains Article II power, notwithstanding any statutory provisions, eliminates the false implication of the current FISA law that its provisions are "exclusive"—a result which would be an unconstitutional encroachment

13326262

43453.134

on the President's power in the context of surveillance that is ordered in response to a foreign attack on the U.S. As I said in my testimony, that purported "exclusivity" of the statute is also contrary to what I am certain all Senators and Congressmen would recognize to be the case, however narrowly they may choose to define the President's Article II authority.

Question:

3. On March 31, 2006, you testified to the Judiciary committee that you "think there is reason to think seriously about legislation in this area to establish a court process to approve this kind of program." Can you comment on the court process you would legislate to authorize a program such as the Terrorist Surveillance Program?

a. You have read my NSSA Bill. Can you please compare and contrast my proposed legislation with your proposed court process?

Answer:

3. The process in the Specter bill is the kind of structure I had in mind. There are a few things I would do differently, as I noted in my statement. I would submit a surveillance program to the FISA Court of Review, instead of to the lower court; it seems to me that decisions on the constitutionality of a program, as opposed to individualized warrant approvals, should be made at the appellate level. I would also direct the court to submit copies of any opinion approving a surveillance program to the Supreme Court and give the Supreme Court power to review any such decision by writ of certiorari—thereby providing assurance that the ongoing process is consistent with the Supreme Court's view of constitutional requirements. I would also direct the court to make public its decision, to the extent I can do so without compromising the secrecy of the surveillance program. But the central elements of the court process set forth in your bill seem to me to be the appropriate institutional structure to determine issues of this kind—now and in the unpredictable range of circumstances that may confront this country in the future.

Question:

4. In your Chicago Tribune Article, *A historical Solution to the Bush Spying Program,* dated February 12, 2006, you wrote the "rapid-time sequence and the need for security professionals to make quick decisions could not be reconciled with the FISA requirement to determine case-by-case probable cause in a manner that could satisfy the court."

b. Do you feel that my legislation alleviates this problem?

Answer:

4. Yes, your proposed legislation alleviates this problem by allowing for court approval of a surveillance program in which decisions are made by security professionals at the NSA or elsewhere. The program would have to be determined to meet constitutional

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00188 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.135

standards, which might include an assessment of the supervision of those professionals, the standards they are instructed to apply, and the methods of monitoring their conduct. The result is both to broaden the potential means of carrying out surveillance, beyond the specific procedures of the FISA statute, and at the same time to establish a more effective constraint on whatever means are adopted.

Question:

5. Technology has changed tremendously since 1978. What are some of the technological hurdles that make FISA obsolete today? Do you agree with how S. 2453 deals with emerging technological issues? Is it feasible for the FISA Court to make the type of determinations and issue the type of program-wide warrants that the bill envisions?

Answer:

5. Yes, the FISA court can make these determinations. Testing the specifics of a particular program or course of action against the requirements of the constitution is what federal courts do all the time. The job of the court will not be to second guess the President or the security professionals on technical or other aspects of a program or the particular foreign threat that makes it necessary. But through the submissions required under the statute—and the court's power to request any additional information it deems necessary—the court will be able to understand what is proposed to be done, the justification for it, the protections that are included to protect constitutional rights and the means of assuring that those protections are observed. It would be a mistake for Congress to try to make these kinds of particularized judgments and put them into statutory provisions that will inevitably turn over time into a legal straitjacket that cannot keep pace with new technologies and new threats. The Specter bill is an institutional structure than can go a long way to create confidence and cooperation, as opposed to the current confrontation, over the appropriate means to serve the most vital national security interests of this country.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00189 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.136

Senator Edward M. Kennedy
Questions for the Record
From Senate Judiciary Committee hearing on "FISA for the 21st Century"
Held on July 26, 2006

To John Schmidt

In the hearing before the Senate Judiciary Committee on July 26, 2006, you made the following claim:

> If it were true that the President was, in fact, limited to a statutory surveillance process, it would mean that if on the morning of 9/11 General Hayden had called President Bush and said, "We want to go forward immediately with the interception of calls at airports around this country where we think al Qaeda has people on the ground prepared to carry out further attacks," the President's only lawful response to that would be to say, "Well, we need to get the Attorney General, we need to begin examining whether each of those intercepts complies with the FISA statute, and maybe we will be able to get you authority by this afternoon or tomorrow morning."

However, FISA allows the NSA to begin tapping a source immediately and continuously for up to 72 hours while it pursues a warrant. This can be done entirely at the discretion of the Attorney General, so long as he makes a good-faith effort to "reasonably determine[]" that "an emergency situation exists" and that "the factual basis for the issuance of an order … exists". 50 U.S.C. §1805.

Question:

- **If the problem with the current law is the inability of the NSA to process the required number of FISA petitions within the 72-hour window, why not simply amend the statute to extend the grace period? If the grace period were extended to a month, or three months, the NSA could discard useless information and use the ample extra time to apply for warrants to obtain any useful information. Why do we need the Chairman's sweeping overhaul if the actual problem can be solved in a targeted manner?**

- **If the concern is about the time that it takes for the Attorney General to approve wiretapping under the emergency 72-hour provision, why does it take longer to meet the requirements of FISA ("reasonably determin[ing] that "an emergency situation exists" and that "the factual basis for the issuance of an order…exists") than the Administration's standard for the warrantless wiretapping program ("a communication we believe to be affiliated with al Qaeda, associated with al Qaeda, one end of which is in the United States, and we believe at least one end we have a probable cause standard is al Qaeda")? Could this problem be solved by delegating this responsibility to specified senior officials with legal proficiency in these matters? Or the allocation of additional resources to the FISA Court or the relevant federal agencies gathering intelligence?**

13326247

43453.137

Answer:

- The statute requires that before the Attorney General authorizes emergency surveillance he must reasonably determine that "the factual basis for the issuance of an order exists"—that is that there is probable cause to believe that each U.S. person who is a target of the surveillance is an "agent of a foreign power" and that "each facility" being intercepted is being used by that target. In the circumstance I described—where the need is for immediate interception of calls at other U.S. airports after the 9/11 attack—there would be no basis for making either of these determinations as to all of the proposed interceptions—nor would there be time to get the Attorney General or any other specified official involved in making such determinations. Any U.S. President in these circumstances—in the immediate aftermath of an attack by a foreign power in the U.S. —would direct the NSA to go forward with any surveillance that might reasonably be thought necessary to obtain information on a possible further attack. I cited this example not in the context of urging specific FISA changes but to make the point that all rational people must recognize that there are circumstances where the President possesses Article II surveillance power to respond to foreign attack that cannot be circumscribed by any statute. That is why it is "dangerous" (to use Ed Levi's phrase) for Congress to pass a statute purporting to have that effect. In the immediate context of the Specter bill, given that everyone must recognize that the President does have Article II power that goes beyond any statute, there is no reason for objection to the provision of the bill that contains that acknowledgment—without purporting to define the limits of that Article II authority.

- The immediate problem that led to the authorization of the NSA program—that is, the need to make quick decisions in following the trail of Al Qaeda from calls intercepted outside the U.S. to calls into or out of this country—could conceivably be solved by "delegating" the authority to make surveillance decisions to a large number of NSA security professionals. But that is a less desirable result than the Specter bill approach that would allow a surveillance program of that nature to be submitted for court review of its constitutionality—requiring the court to be advised of all elements of the program (the manner in which surveillance targets will be identified, the supervision of personnel making such decisions, the process for monitoring to make sure decisions are being made appropriately, etc)—as well as ongoing court review at specified intervals of the continued need for the program and the manner of its implementation. Moreover, "fixing" the statute with that kind of specific modification only solves the particular need we have identified today without creating an institutional mechanism that can deal with the inevitable other problems that will arise in the future—as a result of the unpredictability of foreign attacks on this country and the constantly changing communications technology that affects both the types of communications to be intercepted and our capacities to carry out that interception. A flexible court process is far preferable to trying to "write the NSA program into the law."

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00191 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.138

SUBMISSIONS FOR THE RECORD

STATEMENT FOR THE RECORD OF

LT GEN KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY

BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

JULY 26, 2006

Good morning Mr. Chairman, Senator Leahy, and Members of the Committee.

I am pleased to be here today to provide testimony in support of the National Security Surveillance Act of 2006 (S. 2453), which would amend the Foreign Intelligence Surveillance Act of 1978. The changes proposed in the bill are, I believe, intended to recapture the original Congressional intent of the statute – ensuring the protection of the rights of people in the United States as the Government engages in electronic surveillance. At the same time, the proposed bill would remove from the statute's coverage surveillance directed at individuals who are not due protection under the Fourth Amendment, such as foreign persons located overseas.

While some of the specifics that support my testimony and support passage of this bill 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 the statute. While the FISA as originally drafted incorporated the unique features of 1978 technology to achieve agreed-upon goals, the stunning technological changes in the communications environment that we have witnessed since that time have brought within the scope of the statute communications that we believe the 1978 Congress did not intend to be covered.

43453.139

Today, the U.S. Government is often required by the terms of the statute to make a constitutionally based showing of probable cause 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. Obtaining a court order, based on the constitutionally required 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. In that respect, we frequently sacrifice to detailed and rigorous process one of our greatest advantages in our effort to collect foreign intelligence -- the ability to access a vast proportion of the world's communications infrastructure located in our own nation.

The FISA sought -- in simple terms -- 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 stated: "[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, the judgment of Congress at that time was that Court supervision was important -- if not absolutely essential -- when significant Fourth Amendment interests were implicated.

Yet the Fourth Amendment is clearly not always at issue when NSA or another intelligence agency acts, and the FISA surely 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 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

---

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

43453.140

without any resort to the court and without reliance on a showing of probable cause.

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 at ensuring the constitutional reasonableness of NSA's surveillance activities, and at eliminating 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 definitions of "electronic surveillance" contained in the current statute are constructed, the answers to several questions are relevant to the determination of whether a FISA order is required in order for NSA 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 in 1978, but that today appears to have unintended effects.

In many cases, the decision whether the Government must obtain an order from the FISA Court, and in doing so must make a showing that relies on the constitutional notion of probable cause, depends in part on such issues as the communications technology employed and the location in which the collection efforts take place. We believe such issues to be ancillary, if not irrelevant, to the more fundamental issue. Thus, in some cases, whether NSA seeks to acquire a communication from inside the United States, or seeks to acquire the very same communication outside the United States, becomes a question clothed in undue significance. So, too, the technology employed by the provider of the communications service can in some cases

43453.141

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.

Senate Bill S. 2453 would effect the required change, making relevant only those questions that independently carry significance - particularly in the telecommunications environment of 2006. 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, irrespective of where the surveillance is conducted or what means are used to transmit a communication, would receive under this Bill the protection afforded by Court approval. At the same time, people outside the United States who are not U.S. persons, again irrespective of where the surveillance is effected or the technology employed, would not receive such protection. Targeting of U.S. persons outside the United States would be treated exactly as it is today, only with specific approval of the Attorney General based on appropriate findings. In short, we believe the bill currently under consideration contains language appropriate to restore to the statute appropriate protection of those who are located in the United States.

Moreover, the current FISA – at least in some places – already recognizes the principles the bill seeks to inject throughout the statute. 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 quite precisely 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. 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 irrespective of whether the communications are domestic or international and likewise irrespective of where the surveillance is being carried out.[2] The same legislative history

[2] Id. at 50.

regarding that first definition of electronic surveillance makes equally clear, however, that the statute does not regulate the acquisition of communications of U.S. persons in the United States when those persons are not the actual targets of the surveillance.[1]

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, never directly relevant in principle but once relevant in the context of yesterday's telecommunications infrastructure, are today utterly irrelevant to the central question at issue – who are the people requiring protections. 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 changes to the definition of electronic surveillance, other changes in the bill are important as well. First, and most crucially, the Government must retain a means to compel communications providers to provide information to the Government even in the absence of a Court Order. The Bill would authorize the Attorney General to require such cooperation, and would also insulate from liability those companies that assist the IC in preventing future attacks on the United States.

Finally, other changes are not as crucial to the continued success of the intelligence community in countering threats, but will make a better bill. For instance, the bill recognizes the inadequacy of the manner in which FISA defines the phrase "agent of a foreign power," and adds to the category visitors to the United States who may not be working for a particular government and may not be terrorists, saboteurs or spies, but who nonetheless have and may transmit or receive significant foreign intelligence information.

---

[1] Id.

43453.143

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 significant factors, while setting aside ancillary issues such as the technical means employed or the location from which the surveillance was conducted.

43453.144

WASHINGTON
LEGISLATIVE OFFICE

July 26, 2006

The Honorable Arlen Specter, Chairman
Senate Judiciary Committee
United States Senate
Washington, DC 20530

Re. Opposition to the latest version of S. 2453, the National Security Surveillance Act of 2006

AMERICAN CIVIL LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

CAROLINE FREDRICKSON
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

OFFICERS AND DIRECTORS
NADINE STROSSEN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

KENNETH B. CLARK
CHAIR, NATIONAL
ADVISORY COUNCIL

RICHARD ZACKS
TREASURER

Dear Chairman Specter:

On behalf of the American Civil Liberties Union, and its hundreds of thousands of activists, members and fifty-three affiliates nationwide, we write to renew our strong opposition to S.2453, the "National Security Surveillance Act of 2006." We ask that our letter be submitted for the record.

While we appreciate your desire to do something in response to the fact that the administration has willfully and unrepentantly violated the plain directions of Congress regarding electronic surveillance, this bill would allow the administration to take the nation farther down the wrong path, away from restoring the rule of law and meaningful checks and balances. It would in fact be a betrayal of your legacy as Chairman and the responsibilities of this Committee to move forward on a bill that eviscerates the Fourth Amendment.

Before addressing this legislation, it is important to put the Committee's agenda this week in context, given last year's extensive debate about how the Patriot Act "modernized" the Foreign Intelligence Surveillance Act (FISA) and our strong concerns about how that law eroded civil liberties. The Committee needs to conduct a thorough investigation in light of the serious concerns about the version of the bill the Vice President helped write.

We have three overarching concerns about S. 2453, which includes pages of brand-new amendments to FISA that have not been fully vetted by the Committee and are not be ripe for a vote. We believe these changes would result in legalizing a range of unauthorized surveillance programs without Congress being fully informed about what it is approving or the true rationales for such changes. First, the bill allows warrantless surveillance of all international calls and e-mails of American residents or businesses, without any evidence of any conspiracy with al Qaeda. Second, the bill makes FISA optional while embedding into law the president's claim that he has inherent power to wiretap Americans without a court order. Far from changing nothing, the administration would use these changes to claim the president is empowered to act at maximum unchecked authority. Third, we are very concerned about the bill's attempt to prevent randomly assigned judges from considering Americans' constitutional claims about the program.

43453.145

The Patriot Act Lesson. The Judiciary Committee has attempted to frame the debate this week as the need for the "Modernization of FISA." Yet, every member of this Committee knows well that "modernization" is precisely the rationale for the sweeping amendments to FISA made by the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" (the USA Patriot Act). As former Bush official John Yoo stated, "the primary provision in the Patriot Act makes amendments to the Foreign Intelligence Surveillance Act, which is the secret court you hear about that issues secret wiretaps and so on. What the Patriot Act did is that it modernized that statute. . . . We go to the federal courts for warrants and to get the kind of wiretaps to fight terrorism." CNN, Apr. 27, 2005. President Bush made similar statements about the law that April:

> Now, by the way, any time you hear the United States Government talking about wiretap, it requires--a wiretap requires a court order. Nothing has changed, by the way. When we're talking about chasing down terrorists, we're talking about getting a court order before we do so. It's important for our fellow citizens to understand, when you think PATRIOT Act, constitutional guarantees are in place when it comes to doing what is necessary to protect our homeland, because we value the Constitution.

Eight months after these assurances that Americans' civil liberties were being protected it came to light that, in fact, the Bush Administration--on the advice of Mr. Yoo and other political appointees—had been monitoring Americans' phone conversations for the past nearly five years without any such check.

A Full Judiciary Committee Investigation Is Warranted. Rather than address the administration's failure to abide by what it then publicly acknowledged the Constitution "guarantees," the Chairman's bill would use these revelations as a springboard to more warrantless surveillance of Americans in the guise of "modernizing" the law. The law already allows the court to order wiretaps of the cell phones or other phones of Americans conspiring with al Qaeda. The wiretap can start immediately in case of an emergency with judicial review sought afterward. But the President has failed to comply with these exclusive, mandatory procedures. Between the Patriot Act and the Intelligence Authorization Acts, FISA has been changed many times. http://www.fas.org/sgp/crs/intel/m071906.pdf. Despite these changes, the president has not faithfully executed these exclusive procedures.

In fact, now we are hearing the claim that FISA does not permit the wiretapping of cell phones. This assertion is refuted by numerous sources, including the testimony of the Attorney General of the United States:

> Section 206 of the USA PATRIOT Act ... provided terrorism investigators with an authority that investigators have long possessed in traditional criminal investigations. Before the passage of the Act . . . each time an international terrorist or spy switched communications providers, for example, by *changing cell phones or Internet accounts*, investigators had to return to court to obtain a new surveillance order, often leaving investigators unable to monitor key conversations.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00199 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.146

April 6, 2005 Hearing before the House Judiciary Committee (emphasis added). Therefore, the sudden claim this month that FISA must be modernized to facilitate wiretapping of cell phones should be viewed with great skepticism, to say the least.

The standards in U.S. foreign intelligence surveillance laws should not be amended without a clear and unequivocal commitment by the President to follow--to the letter--the bills passed by Congress and signed into the law. The first order of business must be to restore the rule of law.

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 significant 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 all phone calls made to or from an American in the U.S. 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 US government monitoring. This change is made worse by the provision stating that Americans' communications are only protected if the NSA "reasonably believes" all the senders and recipients are in the US; if NSA does not so believe, it need not seek a warrant.

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 Americans and businesses in the U.S. 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 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. The extensive facts uncovered by that non-partisan effort is described in more detail in the letter of the civil liberties coalition on June 7, 2006, which we ask be included in the record. Suffice it to say, representatives of this Judiciary 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 and this Committee's failure to hold a hearing with the telecommunication companies or former Bush officials, it would be difficult to believe this Committee has the answers to questions that should be answered before FISA is amended in such a drastic way. 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.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00200 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.147

Making Genuine Warrants Optional. Our long-standing concerns about the bill's so-called "program warrant" proposal are detailed in our letters of May 16, 2006, and April 6, 2006, and we would ask that they be included in the record (they are appended to this letter). The bill would bypass Congress in favor of court approval for electronic surveillance of untold numbers of Americans. The process is a sham—it basically directs the court to allow wiretaps without any showing of individualized wrongdoing or any showing that the persons whose conversations are eavesdropped upon are agents of a foreign government or terrorist organization. The decision to execute the surveillance is made in secret and without any adversarial process. The Fourth Amendment requires particularity but the bill would allow the court to approve surveillance without ever knowing the names and number of Americans being monitored.

The bill also takes an unwarranted dragnet approach that would sweep up the communications of innocent Americans, such as reporters, lawyers, and hotel clerks just doing their jobs. The bill steers the court to allow surveillance of Americans without the government ever identifying to the court who is being targeted or how many are subject to the secret surveillance by the NSA.

Perhaps the most troubling thing about this part of the bill is that it makes FISA optional while endorsing the President's unitary executive authority claim. The bill would change federal criminal law to allow the president to conduct warrantless spying on Americans' communications, embedding in a federal statute language allowing presidents to wiretap without any judicial check under FISA or the criminal code. It also requires FISA to be interpreted so as not to limit the president's claimed unilateral power to search Americans without any check. This is designed to insulate the president from accountability as well as rebuke by the Supreme Court. And then, to add insult to injury, the bill increases the penalties for unauthorized disclosure of information relating to the program and implicitly applies them to whistleblowers. Under the bill, the criminal penalties-- previously focused on government officials who wiretap Americans without court orders-- would be greatly increased (from $10K to $100K and 5 to 15 years).

The bill is also extremely troubling because it would allow warrantless physical searches of Americans' homes or businesses indefinitely, as well as warrantless wiretaps, whenever the U.S. is in a military conflict. It would do this by repealing the provision that requires the President to follow FISA even if Congress declares war, except the first 15 days after the declaration of war. By both eliminating the provision allowing for warrantless searches in the first 15 days after a declaration of war, and imbedding in the statute the President's assertion that he has the constitutional authority to engage in wiretapping without judicial review, bill will likely be interpreted by the administration to mean that whenever the US is in a military conflict the President can authorize secret searches of Americans without judicial review. In repealing this limitation for secret physical searches (FISA sneak and peek/black bag jobs), the bill would destroy one of the pillars of FISA and allow the president to engage in unchecked surveillance of Americans.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00201 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.148

The bill basically requires blind trust that the President and future presidents will never misuse such a grant of power to secretly wiretap or search whomever they want without check. The bill also takes Congress out of the equation by triggering presidential surveillance authority without a declaration of war or 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 4th Amendment or to delegate to the President such a "right." Congress has no business waiving Americans' individual rights, let alone waiving them in advance. The bill is not saved by the provision that the President report some limited information to Congress.

The Bill Also Thwarts Independent Judicial Review of Illegal Spying. The bill is also severely flawed because it would prevent independent courts and randomly selected judges from across the country from hearing Americans' claims that their rights have been violated by warrantless surveillance. The bill works a great injustice in the way it tips the scales of justice. It would require the transfer to the secret FISA Court of Review (FISCR) of all federal or state cases involving "the legality of classified communications intelligence activity"--an undefined term that could be argued to reach FOIA cases (such as the torture FOIA documents that were stamped classified) or national security whistleblower cases. The FISCR could dismiss the lawsuits "for any reason under law." These provisions overreach. Americans are entitled to have their constitutional claims heard by a fairly chosen Article III court, not a pre-selected chamber.

Other Serious Civil Liberties Concerns. In addition to these overarching concerns, we have concerns about the substantial changes to the definitions of FISA. 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. The bill would inexplicably delete that important protection while also changing the law to allow more Americans conversations to be retained, even though "unintentionally acquired." The bill would also expand warrantless access by allowing the Attorney General to obtain "stored communications" from telephone companies, landlords and others without a court order and pay them for the secret cooperation. It is unclear how far into Americans' homes or businesses the Attorney General could reach with these changes.

Additionally, it appears that the bill contemplates that any datamining by the NSA into Americans' phone records or other data would be allowed to continue without any judicial check at all. It is clear that the bill allows by its terms the "electronic tracking" of Americans and would exclude "dialing, routing, addressing or signaling" information from the types of information subject to a so-called "program warrant." This means that government tracking of such information would not be subject even to the limited judicial examination provided in the bill. Under current law, the government is

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00202 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.149

required to obtain a pen register or trap and trace court order under FISA to obtain such information. However, the administration has certainly indicated that it does not feel obligated to follow FISA's requirements for getting a judicial order for the contents of Americans' communications through wiretaps, and we believe that the same reasoning the Administration uses to support its position on warrantless wiretapping is likely being used to support the notion that pen register and trap and trace surveillance – can be conducted without court orders. In other words, by excluding this information from the coverage of the bill, the bill leaves dialing, routing, addressing and signaling information subject to the Administration's expansive interpretation of the President's purported authority to engage in electronic surveillance, without even the minimal procedures in the program warrants provision of the bill.

Signals and dialing data are "content" under FISA because they reveal the identity of parties to a communication and the existence of that communication. This is sensitive, consequential information that the bill excludes from its definition of "substance." The government should not be able to obtain sensitive information about whom an individual calls or e-mails, or what Internet websites he or she visits, or secretly pinpoint his or her location via electronic signals emitted by a cellular phone, without judicial check. Unlike the approach in this bill, courts have found that GPS signaling information is protected by the Fourth Amendment, and that a court order is required to track that information. Such information should not be beyond judicial oversight by creatively altering definitions.

We also believe the bill should not move forward on the heels of Attorney General Alberto Gonzales's 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.

The bill also fails to take into account recent judicial decisions recognizing limits on presidential power. A federal court in an NSA case recently reiterated that the Constitution protects the privacy of Americans' phone 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)). And S.2453 ignores the crux of the *Hamdan* decision.

Congress should not approve the transfer of power this bill represents when the administration has shown that it is unwilling to operate within the laws as written and that it is 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

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00203 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.150

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, our liberties may never recover.

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 the bill is no blank check but basically it is a check written to the administration in the amount it wants, diminishing privacy rights and the checks and balances that protect them. We ask that you reconsider this bill and return to the bill you co-sponsored with Senator Feinstein, S. 3001, the Foreign Intelligence Surveillance Improvement and Enhancement Act of 2006. It would reinforce the rule of law while streamlining procedures, but without unwarranted expansions of unchecked power. Your instinct in trying to address the administration's assertions is a good one, but short-circuiting any Senate investigation and the retrospective ratification of illegal acts by the administration is unacceptable from a civil liberties standpoint.

Accordingly, we urge the Committee to investigate thoroughly the ongoing illegal surveillance programs currently being conducted by the National Security Agency at the direction of the President, and we hope the Committee will reaffirm its vital role as a check on the executive. Thank you for considering our views.

Sincerely,

Caroline Fredrickson
Director, Washington Legislative Office

Lisa Graves
Senior Counsel for Legislative Strategy

Enclosure

cc: Members of the Senate Judiciary Committee

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00204 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.151

Department of Justice

STATEMENT

OF

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

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

CONCERNING

FISA FOR THE 21ST CENTURY

PRESENTED ON

JULY 26, 2006

STATEMENT

OF

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

BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

CONCERNING
FISA FOR THE 21ST CENTURY

PRESENTED ON
JULY 26, 2006

Thank you, Mr. Chairman, Senator Leahy, and Members of the Committee. I appreciate the opportunity to appear here today to discuss proposed revisions to the Foreign Intelligence Surveillance Act of 1978.

Foreign intelligence surveillance is a critical tool in our common effort to prevent another catastrophic terrorist attack on the United States. The enemies we face operate in obscurity, through secret cells that communicate globally while plotting to carry out surprise attacks from within our own communities. We all recognize the fundamental challenge the War on Terror presents for a free society: To detect and prevent the next 9/11, while steadfastly safeguarding the liberties we cherish. Maintaining the constitutional balance between security and liberty must be our polestar in any legislative effort to reframe the FISA statute.

The past 28 years since the enactment of FISA have seen perhaps the greatest transformation in modes of communication of any period in history. In 1978, almost all

43453.153

transoceanic communications into and out of the United States were carried by satellite, and those communications were intentionally kept 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 is so expert in exploiting 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 designed for the last century and geared more toward traditional case-by-case investigations.

The limitations of the traditional FISA process and the acute need to establish an early warning system to detect and prevent further al Qaeda attacks in the wake of 9/11 led the President to authorize the Terrorist Surveillance Program. As described by the President, that program, which has been the subject of prior hearings before this Committee, 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.

This Committee is currently considering several pieces of legislation addressing FISA and the Terrorist Surveillance Program. I want to thank the Chairman for his

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00207 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.154

leadership on these issues and for his hard work in crafting a comprehensive approach that will help us fight terrorists more effectively and gather critical foreign intelligence more efficiently. I also wish to thank Senator DeWine, who sits both here and on the Intelligence Committee; Senator DeWine has also introduced a bill, co-sponsored by Senator Graham, which represents a very positive approach to the issues presented by the Terrorist Surveillance Program. The Administration urges the Committee to approve both of these bills promptly, and we look forward to working with the Congress as a whole as this legislation moves ahead, and with the Intel Committees, where technical changes can be appropriately discussed to ensure that FISA as amended will provide the Nation with the tools it needs to confront our new adversaries.

I intend to focus my remarks today primarily on the Chairman's bill.

Fundamentally, Chairman Specter's legislation recognizes that in times of national emergency and 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 surveillance targeted at the terrorists and designed to detect and prevent the next attack. Article II of the Constitution gives the President authority to act in this way to defend the Nation. The provisions in Chairman Specter's legislation providing that FISA does not interfere with the President's constitutional authority simply reaffirm the same proposition stated by the FISA Court of Review in its seminal decision in 2002. That court "[took] for granted that the President does have that [constitutional] authority," and concluded that "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).

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00208 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.155

At the same time, however, Chairman Specter's legislation will provide an important new role for the Judicial Branch in the review of such presidential programs, in addition to oversight by the Intelligence Committees of the Congress. His bill would add a new title to FISA under which the FISA Court, subject to certain requirements, would have jurisdiction to issue an order approving a program of terrorist surveillance authorized by the President. This legislation would create for the first time an innovative procedure whereby the President (acting through the Attorney General) will be able to bring such a surveillance program promptly to the FISA Court for a judicial determination that it is constitutional and reasonable, in compliance with the requirements of the Fourth Amendment. The FISA Court would also be authorized to review the particulars of the program and the minimization procedures in place, to help ensure that the surveillance is focused on the terrorist threat and that information collected about U.S. persons is properly minimized. The availability of these procedures and the ability of the FISA Court to issue an order approving a program of electronic surveillance will strongly encourage Presidents in the future to bring such programs under judicial supervision.

As Chairman Specter has announced, in response to this proposal and the other positive innovations contained in the Chairman's bill, the President has pledged to the Chairman that he will submit his Terrorist Surveillance Program to the FISA Court for approval, if the Chairman's legislation were enacted in its current form, or with further amendments sought by the Administration.

Chairman Specter's legislation would also protect sensitive national security programs from the risk of disclosure and uneven treatment in the various district courts

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00209 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.156

where litigation may be brought. Under his bill, the United States (acting through the Attorney General) could require that litigation matters putting in issue the legality of alleged classified communications intelligence activities of the United States be transferred to the FISA Court of Review, subject to the preservation of all litigation privileges. The Court of Review would have jurisdiction to make authoritative rulings as to standing and legality under procedures that would ensure protection of sensitive national security information and promote uniformity in the law.

In addition to the innovations I have described, Chairman Specter's legislation 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 in protecting the Nation from the unique threats of international terrorism.

Changes contained in the Chairman's bill would correct the most significant anachronisms in FISA. Most fundamentally, Chairman Specter's legislation would change the definition of "electronic surveillance" in title I of FISA to return FISA to its 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 foreign intelligence activities in light of changes in international communications technology that have occurred since 1978.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00210 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.157

The bill would also change the definition of "agent of a foreign power" 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 who is not an agent of a foreign government or a suspected terrorist will enter the United States in circumstances where the Government knows that he possesses potentially valuable foreign intelligence information, and the Government currently has no means to conduct surveillance of that person under FISA.

Finally, Chairman Specter's bill would also significantly streamline the FISA application process. Among other things, the Chairman's legislation would limit the amount of detail required for applications and would specify that an Executive Branch officer specially designated by the President to conduct electronic surveillance for foreign intelligence purposes may certify a FISA application. And, very importantly, the "emergency authorization" provisions would be amended to permit emergency surveillance for up to seven days, as opposed to the current three days, and to specify that the Executive Branch officer specially designated by the President may approve emergency authorizations, with appropriate notification to the Attorney General.

* * *

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. And, today, we urge the Committee to give speedy approval to the bills introduced by Chairman Specter and Senator DeWine.

# # #

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00211 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.158

July 14, 2006

The Hon. Bill Frist
Majority Leader
United States Senate
Washington, D.C. 20510

The Hon. Harry Reid
Minority Leader
United States Senate
Washington, D.C. 20510

The Hon. J. Dennis Hastert
Speaker
U.S. House of Representatives
Washington, D.C. 20515

The Hon. Nancy Pelosi
Minority Leader
U.S. House of Representatives
Washington, D.C. 20515

The Hon. Arlen Specter
Chairman
Senate Judiciary Committee
United States Senate
Washington, D.C. 20510

The Hon. Patrick Leahy
Ranking Minority Member
Senate Judiciary Committee
United States Senate
Washington, D.C. 20510

The Hon. F. James Sensenbrenner, Jr.
Chairman
House Judiciary Committee
U.S. House of Representatives
Washington, D.C. 20515

The Hon. John Conyers
Ranking Minority Member
House Judiciary Committee
U.S. House of Representatives
Washington, D.C. 20515

The Hon. Pat Roberts
Chairman
Senate Select Committee on Intelligence
United States Senate
Washington, D.C. 20510

The Hon. John D. Rockefeller, IV
Vice Chairman
Senate Select Committee on Intelligence
United States Senate
Washington, D.C. 20510

The Hon. Peter Hoekstra
Chairman
Permanent Select Committee
on Intelligence
U.S. House of Representatives
Washington, D.C. 20515

The Hon. Jane Harman
Ranking Minority Member
Permanent Select Committee
on Intelligence
U.S. House of Representatives
Washington, D.C. 20515

43453.159

Dear Members of Congress:

We are a group of constitutional law scholars and former government officials, writing in our individual capacities. Earlier this year we wrote you two letters (dated January 9 and February 2, 2006) explaining why, in our view, the recently disclosed National Security Agency (NSA) electronic surveillance program is unlawful under the Foreign Intelligence Surveillance Act of 1978 (FISA), and why the Department of Justice (DOJ)'s legal defense of that surveillance program is unpersuasive.[1]

We will not repeat our previous arguments here. We write now merely to explain how the Supreme Court's recent decision concerning military commissions, *Hamdan v. Rumsfeld*, 126 S. Ct. 2749 (2006), further refutes the only two legal arguments that the DOJ has offered in support of the NSA program—(i) that the September 18, 2001 Authorization to Use Military Force (AUMF) authorizes the NSA program; and (ii) that if FISA prohibits the NSA program, it unconstitutionally restricts the President's powers under Article II of the U.S. Constitution.

In a letter to Senator Charles Schumer dated July 10, 2006, the DOJ asserts that the Court's decision in *Hamdan* "does not affect our analysis of the Terrorist Surveillance Program." Letter to the Honorable Charles Schumer from William E. Moschella, Assistant Attorney General, U.S. Department of Justice ("DOJ July 10th Letter") at 1. In our view, not only does *Hamdan* "affect" the analysis, it significantly weakens the Administration's legal footing. The Court in *Hamdan* addressed arguments regarding the military commissions that are very similar (in some respects identical) to the DOJ's arguments regarding NSA spying, and the Court's reasoning strongly supports the conclusion that the President's NSA surveillance program is illegal.[2]

1. The Court in *Hamdan* held that the military commissions the President established in 2001 transgressed two statutory restrictions that Congress had enacted.

First, the Court held that because Article 36 of the Uniform Code of Military Justice (UCMJ), 10 U.S.C. § 836, prescribes that the rules applied in courts-martial, provost courts, and military commissions must be "uniform insofar as practicable," the rules applicable to courts-martial apply to military commissions absent a showing that

---

[1] Those letters, together with the DOJ memoranda to which we were responding, are collected in a recent issue of the Indiana Law Journal. *See* 81 Ind. L.J. 1355 (2006), *republished at* http://www.acslaw.org/files/Microsoft%20Word%20-%2012_NSA_Debate.pdf.

[2] Other observers who had previously defended the NSA program's legality have candidly acknowledged that *Hamdan* calls the NSA program into serious question. *See, e.g.*, Cass Sunstein, *The NSA and Hamdan*, http://balkin.blogspot.com/2006/07/nsa-and-hamdan.html ("after *Hamdan*, the NSA surveillance program, while still not entirely indefensible, seems to be on very shaky ground, and it would not be easy to argue on its behalf in light of the analysis in *Hamdan*"); Andrew C. McCarthy, *Dead Man Walking*, http://article.nationalreview.com/?q=YTljNWU3ZTRmYTY5YzNlOTUyM2M2Yjc4OTZkMmY2MTI= ("*Hamdan* is a disaster because it sounds the death knell for the National Security Agency's Terrorist Surveillance Program.").

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00213 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.160

such rules would be impracticable for use by such commissions—a showing the Administration had failed to make. 126 S. Ct. at 2790-2793; *see also id.* at 2804-2808 (Kennedy, J., concurring).

Second, the Court held that Article 21 of the UCMJ, 10 U.S.C. § 821, requires that such military commissions comply with the international laws of war, including treaty obligations imposed by the Geneva Conventions. 126 S. Ct. at 2774, 2786; *see also id.* at 2799 (Kennedy, J., concurring). The court found that the Administration's commissions violated Common Article 3 of the Geneva Conventions, which requires, among other things, that detainees in an armed conflict such as our conflict with Al Qaeda be tried for violations of the laws of war only by "a regularly constituted court, affording all the judicial guarantees which are recognized as indispensable by civilized peoples." *Id.* at 2795-2797 (majority opinion). The Court held that the Administration's commissions were not "regularly constituted" because their procedures deviated from the statutorily authorized courts-martial system in ways that had not been justified by any practical need. *Id.* at 2796-2797; *see also id.* at 2802-2804 (Kennedy, J., concurring).

In sum, the Court held that the commissions established by the President "exceed[] the bounds Congress has placed on the President's authority" in two statutory provisions of the UCMJ. *Id.* at 2808 (Kennedy, J., concurring).

2. More importantly for present purposes, the Court also *rejected* two arguments for why the President might be able to circumvent such statutory limits. Those two arguments parallel the ones the DOJ has offered in defense of the President's decision to authorize the NSA to ignore FISA's limitations.

First, the Administration argued in *Hamdan* that when Congress enacted the September 18, 2001 AUMF against Al Qaeda, it implicitly authorized the President to implement his military commissions, notwithstanding any limits that might have been found in preexisting statutes such as the UCMJ. The Court summarily rejected this argument: "[W]hile we assume that the AUMF activated the President's war powers, and that those powers include the authority to convene military commissions in appropriate circumstances, there is nothing in the text or legislative history of the AUMF even hinting that Congress intended to expand or alter the authorization set forth in Article 21 of the UCMJ." 126 S. Ct. at 2775 (citations omitted). The Court also cited *Ex parte Yerger*, 75 U.S. (8 Wall.) 85, 105 (1869), for the proposition that "'[r]epeals by implication are not favored.'" *Id.* And it explained in a footnote that even where (unlike here) Congress has not only enacted a force authorization but also *declared war*, such steps in and of themselves do not authorize the President to do what pre-existing statutes forbid. *Id.* at 2775 n.24 (citing *Ex parte Quirin*, 317 U.S. 1, 26-29 (1942)).

Second, the Court went out of its way to address whether the President has authority under Article II to contravene statutes that restrict his ability to engage and defeat the enemy in times of war, even though the Solicitor General had not pressed that

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00214 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.161

argument directly.[3] The Court explained that even assuming the President has "independent power, absent congressional authorization, to convene military commissions," nevertheless "he may not disregard limitations that Congress has, in proper exercise of its own war powers, placed on his powers." *Id.* at 2774 n.23 (citing the "lowest ebb" passage of Justice Jackson's concurrence in *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 637 (1952) (Jackson, J., concurring)).

Justice Kennedy elaborated on the Article II question in his separate concurrence, invoking Justice Jackson's three-tiered categorization of presidential power in *Youngstown*. Justice Kennedy explained that *Hamdan* was a case on the lowest tier of presidential power, because the President had acted "in a field with a history of congressional participation and regulation," where the UCMJ had established "an intricate system of military justice," with authorizations and restrictions alike, and where, in the Court's view, the President had acted in violation of certain of those pre-established restrictions. 126 S. Ct. at 2800-2801 (Kennedy, J., concurring, joined by Souter, Ginsburg and Breyer, JJ.).

3. The Court's analysis in *Hamdan* confirms that the two arguments that the DOJ has advanced in its support of the NSA surveillance program are flawed.

a. *The AUMF Argument.*

As with the military commissions in *Hamdan*, so too, here, there is "nothing in the text or legislative history of the AUMF even hinting that Congress intended to expand or alter the authorization set forth [in FISA]." 126 S. Ct. at 2775. The AUMF does not even mention either surveillance or FISA, let alone purport to eliminate FISA's conditions and restrictions. And nothing in the legislative history of the AUMF suggests any intent by Congress to override FISA or to impliedly repeal any of its provisions.

In fact, the Administration's AUMF argument is considerably weaker in the NSA context than in *Hamdan*. The statutory limits on military commissions that the Court identified in the UCMJ and in Common Article 3 were ambiguous and subject to reasonable dispute. *See id.* at 2840-2849 (Thomas, J., dissenting). By contrast, FISA's limitations on electronic surveillance are crystal clear, and uncontroverted: FISA expressly declares that FISA itself, together with certain provisions of title 18 of the U.S. Code, prescribe the "exclusive means" of engaging in electronic surveillance, 18 U.S.C.

---

[3] In the court of appeals, the DOJ *had* argued that interpreting the UCMJ "to reflect congressional intent to limit the President's authority" would "create[] a serious constitutional question." Brief for Appellants at 56-57, *Hamdan v. Rumsfeld*, No. 04-5393 (D.C. Cir., filed Dec. 8, 2004). In the Supreme Court, the Solicitor General also invoked the President's Article II powers as a basis for a narrow construction of the UCMJ, arguing that "'the detention and trial of petitioners—ordered by the President in the declared exercise of the President's powers as Commander in Chief of the Army in time of war and of grave public danger—are not to be set aside by the courts without the clear conviction that they are in conflict with the Constitution or laws of Congress.'" Brief for Respondents at 23, *Hamdan v. Rumsfeld*, No. 05-184 (U.S., filed Feb. 23, 2006) (quoting *Quirin*, 317 U.S. at 25).

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00215 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.162

§ 2511(2)(f), and makes it a crime to conduct electronic surveillance "except as authorized by statute," 50 U.S.C. § 1809(a)(l). FISA even includes a specific wartime surveillance provision, *id.* § 1811, which authorizes surveillance outside the FISA framework for only 15 days after a declaration of war. If the AUMF cannot be read to authorize conduct contrary to the statutory limitations *implicit* in the UCMJ, then surely there is no warrant for finding that Congress intended the AUMF to authorize a deviation from the specific, express, and carefully crafted limitations that FISA imposes.

The DOJ's July 10th Letter makes two arguments in an attempt to distinguish *Hamdan*'s holding with respect to the AUMF. Neither is persuasive.

i. The DOJ first notes that the criminal-sanctions provision of FISA, 50 U.S.C. § 1809(a)(1), imposes criminal penalties for electronic surveillance undertaken "except as authorized by statute"—while there is no analogous "except as authorized by statute" clause in the UCMJ provisions at issue in *Hamdan*. DOJ July 10th Letter at 1-2. The DOJ argues, in effect, that even if the AUMF does not *supersede* FISA, it *satisfied a condition* in FISA, namely, the "authorized by statute" clause of 1809(a)(1).

There are several problems with this argument. First, just as there is "nothing in the text or legislative history of the AUMF even hinting that Congress intended to expand or alter the authorization set forth in [the UCMJ]," *Hamdan*, 126 S. Ct. at 2775, likewise nothing in the AUMF's text or legislative history provides any reason to conclude that Congress intended that enactment to satisfy the "except as authorized by statute" condition of the FISA criminal provision. "'Congress . . . does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions—it does not, one might say, hide elephants in mouseholes.'" *Gonzales v. Oregon*, 126 S. Ct. 904, 921 (2006) (quoting *Whitman v. American Trucking Ass'ns*, 531 U.S. 457, 468 (2001)).[4]

Second, FISA itself specifies that a declaration of war—which invariably includes an authorization to use military force, *see* 81 Ind. L.J. at 1416—authorizes only 15 days of warrantless surveillance. To read the AUMF to authorize *unlimited* warrantless surveillance during the conflict with Al Qaeda would contradict Congress's clear intent to require an explicit statutory amendment to depart any further from FISA's rules during wartime.

---

[4] Moreover, the Congressional Research Service concluded that the legislative history of FISA "appears to reflect an intention that the phrase 'authorized by statute' was a reference to chapter 119 of Title 18 of the U.S. Code (Title III) and to FISA itself, rather than having a broader meaning." Congressional Research Service, *Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information*" at 40 (Jan. 5, 2006). Similarly, in recent Senate testimony, David Kris, the Associate Deputy Attorney General in charge of national security earlier in the Bush Administration, explained that "[t]aking FISA as a whole, the penalty provision's reference to a surveillance 'authorized by statute' is best read to incorporate another statute only if it is listed in the exclusivity provision [18 U.S.C. § 2511(2)(f)] (or . . . if it effects an implicit repeal or amendment of that provision." Testimony of David S. Kris before the Committee on the Judiciary, United States Senate at 5 (Mar. 28, 2006), http://balkin.blogspot.com/kris.testimony.pdf.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00216 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.163

Finally, for the NSA spying program to be lawful, the AUMF would also have to be read to have implicitly repealed another provision of FISA, providing that it and specified provisions in Title 18 are the "exclusive means" of lawful electronic surveillance. 18 U.S.C. § 2511(2)(f). But the Court in *Hamdan* indicated that such an implied repeal is "'not favored.'" 126 S. Ct. at 2775 (quoting *Ex parte Yerger*, 75 U.S. (8 Wall.) at 105).

ii. The DOJ's second statutory argument is that whereas the UCMJ "expressly deals with the Armed Forces and with armed conflict and wars," Congress "by contrast" allegedly "left open the question of what rules should apply to electronic surveillance during wartime." DOJ July 10th Letter at 2.

But even if the existence of an express wartime provision were relevant to the statutory argument, FISA *does* deal expressly with electronic surveillance during wartime, in its limited 15-day authorization of warrantless surveillance after a declaration of war. 50 U.S.C. § 1811. FISA specifically contemplates that the President cannot authorize electronic surveillance without a court order and outside the FISA framework *during wartime*—and nothing in the AUMF even purports to affect FISA's limits on wartime electronic surveillance.[5]

b. *The Article II Argument.*

The Court's analysis in *Hamdan* also undermines the DOJ's argument that FISA impermissibly interferes with the President's Article II authority as Commander in Chief. As the Court made clear, the President is obligated to comply with statutory restrictions, even during wartime, as long as those restrictions constitute a "proper exercise" of Congress's own powers. 126 S. Ct. at 2774 n.23; *see also id.* at 2799 (Kennedy, J., concurring) (the President must comply with laws that are "duly enacted" by Congress "in the proper exercise of its powers"). The DOJ has offered no plausible basis for concluding that FISA is any less "proper" an exercise of Congress's powers than were the UCMJ provisions at issue in *Hamdan*.

i. The DOJ first questions whether Congress even had the constitutional authority to enact FISA. It contends that whereas the UCMJ was enacted pursuant to Congress's express Article I authorities, "[t]here is no similarly clear expression in the Constitution of congressional power to regulate the President's authority to collect foreign intelligence necessary to protect the Nation." DOJ July 10th Letter at 2. This argument borders on the frivolous. A bipartisan majority in Congress enacted FISA, with presidential input and approval. The statute has been in place for almost thirty years, during which time Republican and Democratic administrations alike have operated under its modest

[5] The DOJ repeats its argument that the AUMF should be construed as *supplying* the additional authority contemplated in § 1811 "for the armed conflict with al Qaeda." DOJ July 10th Letter at 2. But as we have previously explained, 81 Ind. L.J. at 1416, if that were the case, then every declaration of war would itself indefinitely *extend* the 15-day window for the duration of the conflict, since each such declaration necessarily (and historically) includes a force authorization. Such a reading would render § 1811 superfluous.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00217 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.164

limitations and conditions, with no suggestion that FISA is not appropriate Article I legislation.

FISA was enacted pursuant to at least three Article I powers. Like the statutes that restricted the President's war powers in the leading cases of *Little v. Barreme*, 6 U.S. (2 Cranch) 170 (1804), and *Youngstown*, and like countless other current federal statutes involving wire and electronic communications systems, FISA is valid Commerce Clause legislation, Art. I., § 8, cl. 3, because it regulates and protects wire communications transmitted between states and between nations. *See* 50 U.S.C. § 1501(l) (defining "wire communication" to mean "any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities *for the transmission of interstate or foreign communications*"). FISA is also properly viewed as a statute "necessary and proper for carrying into execution . . . powers vested by this Constitution in the Government of the United States, or in . . . any officer thereof." Art. I, § 8, cl. 18. Just as the Necessary and Proper Clause empowered Congress to create the NSA in the first instance, *cf. M'Culloch v. Maryland*, 17 U.S. (4 Wheat.) 316 (1819), it authorizes Congress to set the terms under which that agency shall operate. Finally, as the NSA is part of the Department of Defense, FISA's application to that agency is also an exercise Congress's power "[t]o make Rules for the Government and Regulation of the land and naval Forces." Art. I., § 8, cl. 14.

ii. The DOJ also argues that the President's authority to collect foreign intelligence is "a direct corollary of his authority, recognized in *Hamdan*, to direct military campaigns." DOJ July 10th Letter at 2. But that does not *distinguish* this case from *Hamdan*, because *Hamdan* likewise concerned an Executive war powers function—the trial of enemy combatants for violations of the laws of war—that "'by universal agreement and practice'" is an "'important incident of war.'" *Hamdi v. Rumsfeld*, 542 U.S. 507, 518 (2004) (plurality opinion) (quoting *Quirin*, 317 U.S. at 28).[6] The Court found no constitutional concern with construing a congressional statute to limit the President in his trial of enemy combatants. So, too, there is no constitutional impediment to Congress restricting the President's ability to conduct electronic surveillance within the United States and targeted at United States persons.

Hamdan thus refutes the DOJ's argument that "serious constitutional questions" are raised whenever Congress enacts statutes that "interfere . . . at all" with what the Administration calls "a core exercise of Commander in Chief control over the Armed Forces during armed conflict"—in particular, "the Commander-in-Chief's control of the means and methods of engaging the enemy in conflict." 81 Ind. L.J. at 1404 n.15. Not a single Justice in *Hamdan* offered the slightest indication that the UCMJ, as construed by the Court, would violate Article II—even though the statutory restrictions in *Hamdan*

[6] Indeed, the Solicitor General argued to the Supreme Court in *Hamdan* that the power to try the enemy for war crimes is "part of the prosecution of the war," in "'furtherance of the hostilities directed to a dilution of enemy power.'" Brief for Respondents at 21 (quoting *Hirota v. MacArthur*, 338 U.S. 197, 208 (1949) (Douglas, J., concurring)).

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00218 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.165

dealt solely with the President's treatment of alleged unlawful enemy combatants, and (unlike FISA) not with the conduct of non-enemy U.S. persons inside the United States.[7]

iii. Finally, the DOJ argues that it would be "considerably easier" to show that FISA, as opposed to the UCMJ, prevents the President from performing a constitutional *duty*, namely, to defend the Nation. DOJ July 10th Letter at 3 (citing the general separation-of-powers principle articulated in *Morrison v. Olson*, 487 U.S. 654, 691 (1988)). But the President also has a duty to take care that Congress's laws are faithfully executed. And the duty to defend the Nation does not give the President a blank check to ignore congressional statutes or the Constitution. *See Hamdan*, 126 S. Ct. at 2799 (Breyer, J., concurring); *see also id.* at 2798 (majority opinion) ("the Executive is bound to comply with the Rule of Law that prevails in this jurisdiction"). Moreover, nothing in FISA makes defense of the Nation impossible—and the President was perfectly free to seek an amendment to it if he deemed change necessary.

In sum, in authorizing the NSA to engage in warrantless surveillance, the President is acting—just as he did in authorizing the military commissions—"in a field with a history of congressional participation and regulation," where the political branches had established "an intricate system" of laws containing authorizations and restrictions alike. *Id.* at 2800-2801 (Kennedy, J., concurring). As Justice Kennedy explained in *Hamdan* (*id.* at 2799), even in a time of armed conflict it is important under our constitutional scheme that the Executive should adhere to such "standards deliberated upon and chosen in advance of crisis, under a system where the single power of the Executive is checked by other constitutional mechanisms":

> 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 standards tested over time and insulated from the pressures of the moment.* (Emphasis added.)

[7] The DOJ suggests (DOJ July 10th Letter at 3) that the *Hamdan* Court's discussion of the Article II argument is not binding because, as Justice Stevens noted, the government "d[id] not argue" that the President "may disregard limitations that Congress has, in proper exercise of its own war powers, placed on his powers." 126 S. Ct. at 2774 n.23. As noted above, however, *supra* note 3, the Government did invoke the President's Article II powers as a reason why the Court should construe the UCMJ to authorize the tribunals. In any event, even if the Court was not required to resolve whether the President's Article II powers allowed him to override statutory dictates in *Hamdan*, it is fair to assume the Court would not have gone to such lengths to construe the statutes as it did, and to determine that the President had exceeded their limitations, if it had serious doubts about whether Congress could constitutionally limit the President here—and that the dissenting Justices would have raised any constitutional doubts they might have had as a further basis for construing the statutes to uphold the commissions.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00219 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.166

We hope that you find these views useful as you address the President's authorization of the NSA electronic surveillance program.

Sincerely,

Curtis A. Bradley
Richard and Marcy Horvitz Professor of Law, Duke University*
Former Counselor on International Law, Department of State, Office of the Legal Adviser, 2004

David Cole
Professor of Law, Georgetown University Law Center

Ronald Dworkin
Frank Henry Sommer Professor, New York University Law School

Richard A. Epstein
James Parker Hall Distinguished Service Professor, University of Chicago Law School
Peter and Kirsten Bedford Senior Fellow, Hoover Institution

Harold Hongju Koh
Dean and Gerard C. and Bernice Latrobe Smith Professor of International Law, Yale Law School
Former Assistant Secretary of State for Democracy, Human Rights and Labor 1998-2001
Former Attorney-Adviser, Office of Legal Counsel, DOJ, 1983-85

Philip B. Heymann
James Barr Ames Professor, Harvard Law School
Former Deputy Attorney General, 1993-94

Martin S. Lederman
Visiting Professor, Georgetown University Law Center
Former Attorney Advisor, Department of Justice Office of Legal Counsel, 1994-2002

Beth Nolan
Crowell & Moring LLP, Washington, D.C.
Former Counsel to the President, 1999-2001; Deputy Assistant Attorney General, Office of Legal Counsel, 1996-1999; Associate Counsel to the President, 1993-1995; Attorney Advisor, Office of Legal Counsel, 1981-1985

William S. Sessions
Holland & Knight LLP, Washington, D.C.
Former Director, FBI, 1987-1993
Former United States District Judge, Western District of Texas, 1974-1987 (Chief Judge, 1981-1987)

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00220 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.167

Geoffrey R. Stone
Harry Kalven, Jr. Distinguished Service Professor of Law, University of Chicago
Former Dean of the University of Chicago Law School and Provost of the University of Chicago

Kathleen M. Sullivan
Stanley Morrison Professor, Stanford Law School
Former Dean, Stanford Law School

Laurence H. Tribe
Carl M. Loeb University Professor and Professor of Constitutional Law
Harvard Law School

William W. Van Alstyne
Lee Professor, William and Mary Law School
Former Attorney, Department of Justice, 1958

* Affiliations are noted for identification purposes only.

Cc: Judge Colleen Kollar-Kotelly
Chief Judge, Foreign Intelligence Surveillance Court
U.S. Courthouse
333 Constitution Ave., NW
Washington, DC 20001

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00221 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.168

PROTECTING AMERICANS FROM ATTACK WHILE PRESERVING OUR CIVIL LIBERTIES AND SEPARATION-OF-POWERS

Statement of

H. BRYAN CUNNINGHAM[1]

PRINCIPAL, MORGAN & CUNNINGHAM LLC
www.morgancunningham.net

Former Senior CIA Officer and Federal Prosecutor (1994-2000) and
Deputy Legal Adviser to the National Security Council (2002-2004)

before the

UNITED STATES SENATE COMMITTEE ON THE JUDICIARY

On the subject of

FISA FOR THE 21st CENTURY

July 26, 2006

Mr. Chairman, Ranking Member Leahy, and Members of the Committee, thank you for inviting me to testify this morning on a subject of vital importance to our Nation. The Chairman's bill and these hearings are, in my view, key steps toward modernizing the Foreign Intelligence Surveillance Act in a way that allows the President to protect our people from attack while preserving the cherished liberties and separation-of-powers that our Constitution demands. As a national security and information security and privacy lawyer for most of my career (serving six years in the Clinton Administration, and two years in the George W. Bush Administration, as well as being a Member of the Markle Foundation Task Force on National Security in the Information Age and concentrating on these issues in private practice),[2] I am confident that:

- We can balance these crucial interests;
- We must balance them correctly, or risk far worse damage to our civil liberties, following a catastrophic attack, than any of us have yet contemplated; but
- *Only* if the Foreign Intelligence Surveillance Act is significantly modified, generally along the lines suggested in the Chairman's bill, S. 2453.

In addition to responding to your questions, I will address today three key issues. First, I will discuss the constitutional and legal analysis, based on numerous court decisions and Executive Branch legal opinions, leading me to the conclusion that – depending upon the precise facts and circumstances of the Terrorist Surveillance Program (TSP) – the program is constitutional and, therefore, legal, notwithstanding the current Foreign Intelligence Surveillance Act (FISA). This analysis, as I will explain, is not affected by the United States Supreme Court's recent decision in *Hamdan v. Rumsfeld.* Second, I will explain why I believe that this constitutional conclusion, as well as the fact that FISA, as currently written, cannot be carried out in the post-9/11 world in a way that protects our people, compels the need for legislation like the Chairman's bill, sooner rather than later. Third, I will provide some observations on the Chairman's draft bill itself.

At the outset, a brief word about bi-partisanship. In my career, I have served longer under a Democratic President than under Republicans. I commend Chairman Specter and other Members of Congress who have sought reasonable solutions to the problems we discuss today without regard to partisan concerns. I also commend the President and Attorney General for their willingness to work with this Committee and others to craft reasonable legislation. To state the obvious, your work today and in the future on this issue will affect the activities of future Presidents, of both parties, far more than President Bush. More importantly, our people expect their lives and their liberties to be protected regardless of which party is in power. Bipartisan consensus on the constitutional aspects of the TSP is represented by the common ground I suspect I will find today with former Clinton Administration Associate Attorney General John Schmidt, and have found with former Associate Deputy Attorney General David Kris, who served in senior FISA-related positions in both the Clinton and Bush Administrations, and who has testified recently before this Committee.[3]

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00223 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.170

The President's Constitutional Foreign Affairs/Foreign Intelligence Authority to Authorize the Terrorist Surveillance Program[4]

The hearing today, quite appropriately, is about the merits of proposed FISA reform legislation. I support the Chairman's bill, S. 2453, and will provide observations about the proposal later in my statement. It is first necessary, however, to summarize what I believe to be the proper constitutional framework for analyzing the TSP, as it is crucial to address squarely the President's constitutional authority to conduct the program. I reach this conclusion *not* because I believe the Chairman's bill is necessary to provide the President with legal authority to conduct the program. To the contrary, a proper understanding of the President's existing constitutional (and, therefore, legal) authority is necessary, I believe, precisely because the current and all future presidents *do have* the constitutional authority to carry out such a program, and our Supreme Court would uphold that authority, notwithstanding the *Hamdan* decision.[5]

Because presidents have not only this authority, but the unique constitutional responsibility to protect us from attack, I believe that *all presidents*, of whatever party, would be using that authority today, will use it in the future, at least if we are still at war, and, indeed, would be horribly negligent in carrying out their responsibilities *not to conduct such a program.* Therefore, because I also believe that our security and liberty is best protected with the active involvement of all three branches of government, I support the Chairman's bill to help enhance the involvement of Congress and the Judiciary in the TSP, a program to protect us from attack from attack that clearly is going to continue whether or not FISA is amended.

Both the Administration and its opponents have discussed the President's authority to authorize the TSP principally in the context of Article II, Section 2, of the Constitution, in which the President is given authority as "the Commander in Chief of the Army and Navy of the United States." This focus is understandable, given the apparent recognition by all sides of the debate that the TSP is part of the ongoing global military campaign against terror announced by the President in response to al Qaeda's attacks on our homeland, and recognized by Congress in the AUMF.

The focus to date on the Commander-in-Chief power is, at best, incomplete, however, because it fails to give due weight to a critical series of United States Supreme Court and other federal court decisions and Executive Branch legal opinions analyzing the President's constitutional authority to control foreign intelligence operations such as the TSP. Based on this ample and significant precedent, it is clear that programs such as the TSP fall principally under the President's constitutional *foreign affairs* authority.[6] In my view, the perplexing failure to recognize this fact, or even to *address* this extensive, and directly applicable, precedent (or only cursorily to do so), fatally undermines much of the published constitutional analysis of the TSP to date, including by the small task force selected by the President of the American Bar Association, the Congressional Research Service, and by a number of self-described constitutional scholars.

The United States Constitution, in its text, places the duty on the President – and *only* the President – to "preserve, protect, and defend the Constitution."[7] At least since 1898, Supreme Court authority, and Executive Branch opinions under both political parties relying on such

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00224 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.171

authority, has recognized that the President has the first, strongest, and most direct authority and responsibility for the protection of our national security, and that this authority and responsibility flows, at least in significant part, from the President's "plenary" authority over the conduct of our foreign affairs.[8]

Supreme Court decisions over many decades strongly support this view, including, importantly, a number of cases decided both before and after Justice Jackson's famous concurring opinion in *Youngstown Sheet and Tube v. Sawyer,*[9] the touchstone for most opponents of the TSP. For example, in *Department of the Navy v. Egan,* Justice Harry Blackmun, writing for the majority, reiterated that the "Court . . . has recognized 'the generally accepted view that foreign policy was the province and responsibility of the Executive.'"[10]

Perhaps most famously, the Supreme Court forcefully affirmed, in its 1936 decision in *U.S.* v. *Curtiss-Wright Export*, the:

> *delicate, plenary and exclusive* power of the President as the sole organ of the federal government in the field of international relations--a power which does not require as a basis for its exercise an act of Congress, but which, of course, like every other governmental power, must be exercised in subordination to the applicable provisions of the Constitution.[11]

Not only has the Supreme Court never reversed its holding in *Curtiss-Wright*, but a Westlaw search indicates it has been cited by our courts well over 150 times, including in numerous cases decided well after *Youngstown*.

To cite but two additional examples, both from the so-called Pentagon Papers case, Justice Stewart, in his concurring opinion joined by Justice White, noted that:

> In the governmental structure created by our Constitution, the Executive is endowed with enormous power in the two related areas of national defense and international relations. This power [is] *largely unchecked by the Legislative and Judicial branches.*[12]

Similarly, Justice Thurgood Marshall, concurring, stated that it: "is beyond cavil that the President has broad powers by virtue of his primary responsibility for the conduct of our foreign affairs and his position as Commander in Chief."[13]

While Congress has, of course, certain enumerated powers under Article I, to declare war, to raise and support the Army, provide for a Navy, and the like, it is the President, then, who -- in addition to his express powers to make treaties, appoint and receive ambassadors, and serve as Commander-in-Chief -- has the "plenary and exclusive" power to conduct foreign affairs, as intended by the framers of our Constitution.[14]

As firmly established is the President's plenary constitutional position in foreign affairs generally, however, it is even stronger in the conduct of foreign intelligence operations, such as the TSP. In a 1988 decision upholding the authority of the President's senior intelligence official to terminate the employment of a CIA officer's employment, on sexual preference grounds, Justice O'Connor stated:

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00225 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.172

> The functions performed by the Central Intelligence Agency and the Director of Central Intelligence lie *at the core of* "the very delicate, plenary and exclusive power of the President as the sole organ of the federal government in the field of international relations."[15]

Federal appeals courts ruling on the President's authority to conduct foreign intelligence electronic surveillance operations have recognized the President's constitutional preeminence in the collection of foreign intelligence to protect our national security. These decisions, all decided well *after* Justice Jackson's concurring opinion in *Youngstown*, recognize the President's core authority in the conduct of foreign intelligence operations such as the TSP.[16] Notably, they also stress the fundamental difference between purely, or primarily, *domestic* cases, such as *Youngstown*, and those involving the collection of intelligence regarding foreign threats to our nation's security, such as the TSP, and have looked with disfavor on legislative restrictions on the latter.[17]

More than 20 years after *Youngstown*, the Fifth Circuit Court of Appeals, in *United States v. Brown*, upheld the President's inherent constitutional authority to authorize warrantless wiretaps for foreign intelligence purposes, explaining that:

> [B]ecause of the President's constitutional duty to act for the United States in the field of foreign relations, and his inherent power to protect national security in the context of foreign affairs, *we reaffirm. . . that the President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence. Restrictions upon the President's power which are appropriate in cases of domestic security become artificial in the context of the international sphere.* Our holding . . . is buttressed by a thread which runs through the Federalist Papers: that the President must take care to safeguard the nation from possible foreign encroachment, whether in its existence as a nation or in its intercourse with other nations.[18]

Similarly, in *United States v. Truong Dinh Hung*, a case cited with approval in 2002 by the Foreign Intelligence Surveillance Court of Review, the Court of Appeals for the Fourth Circuit, in approving warrantless electronic surveillance for foreign intelligence purposes, stated the matter plainly:

> Perhaps most crucially, the executive branch . . . is . . . constitutionally designated as the pre-eminent authority in foreign affairs . . . . Just as the separation of powers in *Keith* forced the executive to recognize a judicial role when the President conducts domestic surveillance, so the separation of powers requires us to acknowledge the *principal responsibility of the President for foreign affairs and concomitantly for foreign intelligence surveillance.*[19]

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00226 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.173

The special Foreign Intelligence Surveillance Court of Review apparently agreed, as it recognized, in a post-FISA, and 9/11, case, that:

> [t]he *Truong* court, as did all the other courts to have decided the issue, held that the President did have the 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.*[20]

Separation of Powers: The Decisive Constitutional Principle

Virtually everyone who has taken a position on the TSP's constitutionality agrees that the fundamental constitutional principle of separation of powers is a decisive part of the analysis, though there is strong disagreement as to which way that principle cuts. Conceding, for the sake of argument, that Congress has attempted to occupy the field for intercepting international communications through FISA as the "exclusive means," and the President's exercise of any power in this area is at *Youngstown's* "lowest ebb" from a separation-of-powers perspective, if FISA impermissibly interferes with the proper execution of the President's own authorities and responsibilities as Chief Executive, Commander-in-Chief, and "sole organ" of foreign relations, FISA is unconstitutional as applied.

Our Supreme Court, long after *Youngstown*, has repeatedly rejected the approach many have taken in applying Justice Jackson's concurrence to the TSP, namely, that, once a President is at his "lowest ebb," Congress' will must prevail regardless of the constitutionality of a statute as applied to a particular set of facts. Rather, the Supreme Court has made clear that a balancing of powers approach must be used. In *Nixon v. Adm'r of General Services*, for example, the Court held that "in determining whether [a legislative] Act disrupts the proper balance [of power] between the coordinate branches, the proper inquiry focuses on the extent to which it prevents the executive from accomplishing its constitutionally assigned functions."[21]

In *Public Citizen v. United States*[22], the Supreme Court was faced with the issue of whether the Federal Advisory Committee Act (FACA), which established procedures by which the Executive branch utilizes private advisory committees, was constitutional *as applied* to a putative private advisory committee formed by the American Bar Association (ABA) that advised the President on the qualifications of potential federal judicial nominees. Under Article II, the President has the power to appoint judges, but the Senate also has a clear and important advise and consent power. The majority in *Public Citizen* recognized that applying FACA in this context raised serious separation-of-powers questions, and, invoking the constitutional avoidance doctrine, ruled that Congress intended to have FACA apply only to advisory committees that were established or controlled by the Executive. *Id.* at 461.

Accordingly, because the ABA committee was not established or controlled by the Executive, FACA did not apply in this case. Justice Kennedy, however, joined by then-Chief Justice Rehnquist and Justice O'Connor, all concurring in the result, found it necessary to reach the constitutional question, and stated that applying FACA to the manner in which the President

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00227 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.174

obtains advice on potential nominees would violate the separation of powers:

> In some of our more recent cases involving the powers and prerogatives of the President, we have employed something of a balancing approach, asking whether the statute at issue prevents the President 'from accomplishing [his] constitutionally assigned functions' . . . . and whether the extent of the intrusion on the President's powers "is justified by an overriding need to promote objectives within the constitutional authority of Congress."[23]

Applying FACA to the appointments process surely would not prevent the President from nominating whomever he chose to be a federal judge. Nevertheless, Justice Kennedy recognized that FACA's impairment of the exercise of even a small part of that presidential power -- namely, the ability to receive unfettered advice from the private sector in the aid of his appointment power -- was sufficient to disable the legislative branch from regulating the exercise of that power.[24]

It cannot be seriously doubted that applying FISA to preclude the TSP would impair the execution of a core constitutional duty of the President to a much greater degree than would have been the case in applying FACA to the ABA advisory committee.

Presidents of both political parties – and their senior most legal advisers – have recognized not only the necessity of such a balancing analysis, but the constitutional authority and, perhaps, responsibility, of a president faced with a statute unconstitutional as applied to particular facts and circumstances. To cite just one example, albeit a highly pertinent one, the constitutional power of the President to gather and share intelligence information was recognized by the Clinton Administration with regard to a statutory preclusion on the sharing of intelligence information gleaned from a criminal wiretap carried out up under Title III.[25] As aptly summarized in a 2000 Office of Legal Counsel Opinion for President Clinton's Administration:

> In extraordinary circumstances electronic surveillance conducted pursuant to Title III may yield information of such importance to national security or foreign relations that the President's constitutional powers will permit disclosure of the information to the intelligence community notwithstanding the restrictions of Title III. . . . *Where the President's authority concerning national security or foreign relations is in tension with a statutory rather than a constitutional rule, the statute cannot displace the President's constitutional authority and should be read to be "subject to an implied exception in deference to such presidential powers." Rainbow Navigation, Inc. v. Department of the Navy*, 783 F.2d 1072, 1078 (D.C. Cir. 1986) (Scalia, J.). We believe that, if Title III limited the access of the President and his aides to information critical to national security or foreign relations, *it would be unconstitutional as applied in those circumstances.*[26]

As discussed above, the conduct of foreign intelligence operations is a core constitutional function of the President, which Congress may not constitutionally impair. Recognition of this constitutional fact may have led the Congress that passed FISA to state, even as it was passing the law, that:

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00228 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.175

> The conferees agree that the establishment by this act of exclusive means by which the President may conduct electronic surveillance *does not foreclose a different decision by the Supreme Court*. The intent of the conferees is to apply the standard set forth in Justice Jackson's concurring opinion in the [*Youngstown*] case.[27]

This statement, by the Congress that passed FISA, is significant for several reasons. First, it acknowledges that Congress itself had some doubt about the constitutionality of FISA's attempt to completely control the President's authority to conduct electronic surveillance for foreign intelligence purposes. Second, it suggests that Congress understood that, even within Justice Jackson's zone of "lowest ebb," there are limits to the degree to which Congress may constitutionally restrict the President in the area of foreign intelligence collection. Finally, the statement indicates that Congress specifically contemplated that the degree to which FISA might constitutionally tie the President's hands could one day reach the Supreme Court. This makes sense if, *but only if*, Congress contemplated that then-President Carter, or a future President, might be required to act outside the FISA statute, exercising the very inherent authority that Congress was attempting to limit.

How, then, to balance "core" presidential authorities with Congress' far weaker ones, but in the context of Congress' clear intent to "occupy the field" and foreclose the President's options? One solid framework is that articulated by former Clinton and Bush FISA-expert David S. Kris in his March 28, 2006 testimony before this Committee:

> [R]eal and hypothetical examples illustrate what Professor Corwin famously called the Constitution's "invitation to struggle" for dominance in foreign affairs. Depending on the vigor of the struggling parties, I believe the constitutional (and perhaps political) validity of the NSA Program will depend on two operational questions. The first question concerns the need to obtain the information sought (and the importance of the information as compared to the invasion of privacy involved in obtaining it). To take a variant on the standard example as an illustration of this point, if the government had probable cause that a terrorist possessed a nuclear bomb somewhere in Georgetown, and was awaiting telephone instructions on how to arm it for detonation, and if FISA were interpreted <u>not</u> to allow surveillance of every telephone in Georgetown in those circumstances, the President's assertion of Article II power to do so would be quite persuasive and attractive to most judges and probably most citizens. The Constitution is not a suicide pact. . . . The second question concerns the reasons for eschewing the use of FISA in obtaining the information. [28]

This is, in my view, the correct analysis. The final answer, of course, is unknowable without many more facts than currently available, at least to me. Based on the factual assumptions I have made, the considerations discussed below, and the weight of authority by our Supreme Court and other courts, as well as more than 200 years of Executive practice, the TSP easily satisfies this test and a proper constitutional analysis leads to but one conclusion. FISA is unconstitutional as applied to the TSP to the extent it impermissibly impedes the President's ability to carry out his constitutional responsibilities to collect foreign intelligence and protect our Nation from attack.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00229 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.176

Hamdan v. Rumsfeld Does Not Alter This Conclusion

Within days of publication of the Supreme Court's voluminous, and somewhat baroque, opinion in *Hamdan v. Rumsfeld,*[29] opponents (and some supporters) of the TSP announced that this decision undermines, perhaps fatally, the statutory and constitutional underpinnings of the TSP. This conclusion is remarkable and, at least with regard to a proper *constitutional* analysis is, in my view, flatly mistaken, for several reasons.

First, the majority opinion in *Hamdan* is overwhelming a *statutory* one, delving deeply into the details of the Detainee Treatment Act, the Authorization to Use Military Force, and the like. The *Hamdan* majority clearly does *not* to reach significant separation-of-powers questions. By contrast, at least under the analysis I put forward today, the question of the legality of the TSP is almost entirely a constitutional one.

In the few paragraphs in which the majority opinion discusses issues arguably related to separation of powers, if anything, Justice Stevens, speaking for the majority, *reinforces* the analysis discussed in my testimony today, as he quotes from *Ex parte Milligan*:

> [N]either can the President, in war more than in peace, intrude upon the proper authority of Congress, *nor Congress upon the proper authority of the President.*[30]

This, of course, is precisely the position I take. In the context of the TSP, however, based on the facts assumed herein, it is FISA, as applied, that "intrudes" upon the "proper authority of the President." As such, as taught more than two centuries ago by legendary Chief Justice John Marshall, any attempt by Congress to so "intrude," through FISA, on the President's constitutional authority, is "entirely void."[31] Justice Stevens appears to acknowledge this constitutional truism by noting that the President may not disregard statutory limitations placed "in the *proper exercise*" of Congress' own powers.[32]

Even Justice Kennedy's plurality concurring opinion, most often cited as arguably undercutting the constitutional basis for the TSP, clearly supports the separation-of-powers analysis discussed above. Justice Kennedy declares, again based on *Ex parte Milligan*, that:

> *Subject to constitutional limitations* . . . Congress has the power and responsibility to determine the necessity for military courts, and to provide the jurisdiction and procedures applicable to them.[33]

It is worth noting that this quoted passage by Justice Kennedy appears in the very same paragraph as the language cited for the proposition that *Hamdan* undermines the TSP's constitutionality, though it is not quoted by them. Also worth noting is that Chief Justice John Roberts did not participate in *Hamdan* because he had ruled (with the government, as it happens) on that very case as a D.C. Circuit Court of Appeals judge. It seems unlikely, at best, that, in a challenge to the TSP, on which the Chief Justice would vote, Justice Kennedy's *Hamdan* concurrence would gather a fifth vote.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00230 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.177

Far more importantly, even if one were to assume that *Hamdan* intended to reach the constitutional separation-of-powers question, it would no more undercut the constitutionality of the TSP than does *Youngstown* itself, for both the *Hamdan* majority and the Kennedy plurality clearly rest their analysis on the considerable independent authorities *explicitly committed to Congress in the text of the Constitution itself*, in the specific context of providing law governing the conduct of military justice. Thus, Justice Kennedy relies on "a long tradition of legislative involvement in matters of military justice." *Id.* Justice Stevens, for the majority, relies on Congress' express constitutional authorities to: "declare War . . . and make Rules concerning Captures on Land and Water . . . [and] make Rules for the Government and Regulation of the land and naval Forces,"[34] Congressional authorities *all* directly relevant to the activities at issue in *Hamdan*.

In stark contrast, no such textual power or "long history" exists for Congress in the areas of foreign intelligence collection programs such as the TSP (or even in foreign affairs generally). Quite the contrary. As demonstrated by even the cursory discussion in my testimony of a few of the many relevant cases, the "core" constitutional authority for such activities is, and must be, vested almost exclusively in the President.

Thus, were the Supreme Court (even, or perhaps especially, in the wake of *Hamdan*) to conduct a separation-of-powers analysis, based on its own balancing test, of facts and circumstances in which FISA, as applied to the post-9/11 world, impairs or impedes the President's ability to carry out such a "core" function, it is likely the Court would find FISA itself, as applied to the facts and circumstances of the TSP, and not the TSP, unconstitutional and, as such, "void."

The Need for S. 2453 and Some Observations

Precisely because I believe the TSP already is constitutional (and, therefore, legal), and critical for this and future Presidents in preventing attacks on our people, I support Chairman Specter's draft legislation, S. 2453. The bill, or one very much like it, is critical, in my view, to ensure that constitutional activities necessary to protect our people from attack, which will continue with or without FISA reform, are afforded the meaningful participation of all three branches of our government.

Programmatic Judicial Review and Approval

On February 5, 2005, along with former Democratic House of Representatives staff member Daniel Prieto, I published an Op-Ed recommending, among other measures to protect civil liberties, that Congress and the President, in reforming FISA:

> *Ensure a role for the courts.* To preserve and promote appropriate judicial oversight, new methods of court involvement must be considered. As one example, courts could pre-approve categories of electronic surveillance. This would allow the government to apply strict, pre-determined criteria to particular communications without the need for case-by-case court approvals. Categories, criteria and eavesdropping activity would be subject to regular re-examination, with approvals subject to periodic court renewals.[35]

43453.178

Based on my review of S. 2453, creating clear jurisdiction for the Foreign Intelligence Surveillance Court (FISC) to conduct just such "programmatic" review, approval, and oversight is the central function of the legislation. As such, I strongly support the bill, and believe it is absolutely necessary.

S. 2453 clearly establishes jurisdiction in the FISC to approve an "electronic surveillance program," upon application of the Executive Branch, including information required by the statute, and if the FISC makes a series of required judicial findings. This type of programmatic approval – that is, a system of prior judicial approval of a collection program (rather than individual communications intercepts) based on criteria articulated in statute, will help ensure the participation of our Judiciary, and, through articulating the required criteria, of Congress. With clearly established criteria, I believe – although there is room for reasonable lawyers and judges to differ on this – that FISC orders approving (or denying) TSP applications likely would satisfy the Constitution's "case and controversy" requirement.

S. 2453 avoids what I believe to be one of the fatal flaws of the 1978-era FISA, namely the requirement for individualized, target-by-target approval, based on known facts which often, in the post-9/11 world, will be *unknown* in any timely fashion, and perhaps *unknowable* given the technology and enemies we now face.

Selected Reasons FISA is Unworkable Today

As has been discussed publicly by technically and legally knowledgeable experts, there are a host of technological developments which have rendered FISA, as currently drafted, unworkable against the post-9/11 terrorist threat to our Nation, including the development of "packet-based" communications, the use of proxy servers and Internet-based, encrypted, highly mobile telephone communications and PDAs, and the routing of vast amounts of purely overseas Internet communications through the United States.[36]

In my view, equally fatal to the ability of any President to comply with all of the substantive and procedural requirements of the 1978 FISA is the current statute's target-by-target dependence upon two principal factors for determining the predicates necessary for approval of intercepts: (1) whether or not a potential target is a known or presumed United States Person (a citizen or Permanent Resident Aliens); and (2) whether the collection of information takes place within the territory of the United States or overseas. Based on my personal experience across multiple decades and Administrations, these two criteria are no longer workable in the post-9/11 world. Because these two pieces of information often will be *unknowable* given today's (and tomorrow's) technology – or *at least* unknowable in a timely enough way to secure FISA warrants to capture brief but crucial terrorist attack warning information – FISA, as written, easily could impede (indeed, prevent entirely) the President from carrying out his constitutional duty to prevent attacks.

I am not alone in my view as to the feasibility of using these factors in the post-9/11 world. For example, the non-partisan Markle Foundation Task Force on National Security in the Information Age, on which I was proud to serve with two of my fellow panelists today,

concluded, after several years of factual research and legal and policy debate, that these two standards are "outdated."[37] I must be clear that the Task Force, in reaching these conclusions about the unworkability of the U.S. Person and place-of-collection rules in the post-9/11 world, did so *only with regard to access to, and sharing of,* information. The Task Force explicitly did *not* reach a conclusion on this issue with regard to the *collection* of information. But to me, not purporting to speak for the Task Force, the logic is inescapable. If technology has made it unworkable, in a timely fashion, to determine U.S. Person status or place of collection for *sharing* of information, after the fact of collection, these problems are, if anything, far more clearly unworkable with regard to *collection*, which must, of necessity, be done in a far more rapid, time-sensitive fashion than the sharing of similar information.

In my view, programmatic approval of the type to be established by S. 2453 would go far towards ameliorating these, and other, fatal technical and legal problems in the current FISA by not mandating case-by-case substantive requirements and procedures inconsistent with today's technology and the enemies we face.

Some Members of Congress and others have argued that there is no information on the public record suggesting that FISA, as currently drafted, is unworkable. Having served as Assistant General Counsel for the Central Intelligence Agency in the Clinton Administration, in peacetime, involved in delicate negotiations with Congress as to how to gain needed legal change without exposing to our enemies the precise vulnerabilities we were attempting to cure, I can well understand the reticence of the Administration to discuss in public its precise problems with FISA.

It doesn't take classified information, however, to readily envision the problems, as many already have. In addition to the issues identified above, I would suggest one hypothetical, among many potential ways FISA almost certainly is unworkable as currently written. Imagine our government intercepts a communication from al Qaeda senior operational planner Ayman al-Zawahiri, to Bryan Cunningham in Denver. Zawahiri tells me ten nuclear devices are to be set off in five minutes and I'm to call the ten presumed-U.S. Person al Qaeda operatives in the United States and order then to do so. Even under the emergency Attorney General approval provisions of FISA, *it would be literally impossible to gather enough information, process it, and submit it for the Attorney General's approval in time to intercept those following ten telephone calls.*

The failure to recognize this obvious scenario in many quarters, I fear, results from a serious misunderstanding about the emergency approval provisions of the current FISA. What many apparently fail to understand is that *the NSA may not lawfully listen to a single syllable of an "electronic communication" under FISA, until the Attorney General approves (most often in writing) an emergency order.* My example obviously is extreme, but it is easy to imagine that the approval process, in many cases, would not be possible even with hours available for approval (e.g., a CIA officer finds a laptop in an al Qaeda camp with hundreds of U.S. telephone numbers, and evidence of an imminent attack that might be triggered by calls between or among any of them).

Based on my experience, and my current private practice focus on information security and technology, I also can imagine a number of purely technological advances possibly made by the government which could enable collection activity outside the strictest interpretation of the

43453.180

1978-era FISA, but which could be cured by S. 2453. I do not feel it wise, however, to discuss these in open testimony because I do not want to risk alerting our enemies to capabilities of which they may not be aware.

Electronic Tracking

S. 2453 wisely, in my view, recognizes the concept of "electronic tracking," as "the acquisition by an electronic, mechanical, or other surveillance *device*"[38] of certain electronic communications. The draft legislation appears to recognize such tracking as an integral part of an electronic surveillance program eventually leading to the access to the contents by *human beings* of a far fewer number of selected communications than those triaged by computer. This is a crucial distinction, and one that, as technology has evolved, clearly needs recognition in our electronic surveillance laws.

I believe that the use of machines to triage communications content and other sensitive, i.e., personally identifiable, information prior to human review will be crucial over the coming years in balancing privacy and civil liberties and our national security. Depending upon one's interpretation of the current FISA, such "machine triage" – the use of which bi-partisan experts, including the Markle Task Force, have recommended – might today require individual FISA applications. Such a situation, obviously, would present an insurmountable obstacle to the use of machine triage that could *enhance* civil liberties *and* operational capabilities by reducing dramatically the volume of information that must be reviewed by our perennially resource-starved law enforcement and intelligence agencies.[39]

Necessity of Section 801

Section 801 of S. 2453 states: "Nothing in this Act shall be construed to limit the constitutional authority of the President to collect intelligence with respect to foreign powers and agents of foreign powers." The bill also includes several other provisions that appear intended to make clear that electronic communications of foreign powers, or their agents, may be lawfully intercepted under specific statutory authorities *or* under the "Constitution of the United States."

These amendments – as well as any others necessary to conclusively reverse any implication of FISA being the "exclusive means" for such collection – are, in my judgment, critical to the passage and effective implementation of any FISA reform legislation. This is so for at least four reasons.

First, restoring the pre-FISA Congressional statement of the law of foreign intelligence electronic surveillance would recognize, in our public statutes, what I believe, as outlined earlier in my testimony, to be the most accurate statement of the balance of legal authorities in this "core" area of Presidential authority. Second, given the view of the current Administration (and, I believe, of any future President) concerning the constitutional prerogatives and obligations in the area of foreign intelligence collection to prevent attacks on our Nation, it is unlikely any FISA reform legislation not clearly restoring this proper constitutional balance would survive a veto. Thus, inclusion of such language likely is necessary to gain passage of legislation achieving the

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00234 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.181

vitally important goal of enhancing involvement of all three co-equal branches of government in the TSP.

Third, this language will ensure that no future President, of either party, in the event that technology or the nature of our enemies change again significantly enough that FISA, as modified by S. 2453, unconstitutionally impedes or impairs that future President's ability to carry out his, or her, constitutional responsibilities, will face the Hobson's choice of deliberately failing to protect us from attack or being accused of violating the law. Finally, and importantly, codifying Congressional support for constitutionally permissible measures to protect our Nation from attack will provide our career intelligence officers with the assurance they need that no branch of government will second guess their actions or punish them after the fact for acting lawfully. This is crucial to reduce the "risk aversion" for which the Clinton and pre-9/11 Bush Administrations were properly criticized by members of both political parties and several independent Commissions.

Document Management System

S. 2453 also calls for the creation of a "document management system" for processing applications for FISA orders. This is an important step to expedite the processing not only of applications, if S. 2453 is enacted into law, under the TSP, but traditional FISA applications, which will continue to be crucial elements of protecting our national security and carrying out our Nation's other foreign policy interests. Any reasonable steps to streamline what remains a far-too-slow approval process are welcome. No combination of such steps, alone, however, can remedy the fatal flaws, outlined above, in the 1978-era Foreign Intelligence Surveillance Act.

Some Issues for Further Deliberation

Obviously, prior to, and after, approval by this Committee, S. 2453 will face a series of additional deliberations, including in the Intelligence Committee and on the floor of this body, in the other body, and in conference. As that process unfolds, I encourage Members to consider the following steps, to be addressed in the language of the legislation, and/or by way of explanation in its legislative history:

- Further clarify the definitions in the new provisions, and harmonize these new definitions and the definitions in current Section 101;
- Further define the statutory status of the newly defined "electronic tracking." As I noted earlier, I believe that codifying the legal status of what I call machine triage of intercepted communications, and related data, prior to any review by a human being, is an important step forward. It will be important, also, to clarify the legal status of such activities, and the results of them, if they are *not* used to identify communications for further, human, review and/or processing. In my view, unless and until such information actually is reviewed by a human being, it should not be considered "collected" or "acquired," though strict controls should be placed – and enforced – on the data's retention and the ability to access it. Also, the FISC might play a meaningful role in helping to define and enforce these rules, as it does with regard to minimization under the current FISA;

- Clarify whether S. 2453 repeals the current "exclusive means" language in Section 201 of FISA;
- Clarify what I believe to be the constitutionally required balance between the Executive and Judicial branches by making clear that, notwithstanding Section 702, neither the Foreign Intelligence Surveillance Court of Review, nor any other court, has the authority to disclose, or direct the Executive to disclose, classified information (though our courts do, of course, have the authority to order other remedies, including the dismissal of charges, in a criminal prosecution if they conclude the defendant cannot have a fair trial without the disclosure of such information);
- Clarify whether or not S. 2453 intends to disrupt the sometimes uneasy but, in my view, necessary constitutional compromise between all presidents of both parties for the past several decades and the Congress concerning the degree to which each individual member of the Congressional intelligence oversight committees must be equally briefed on highly sensitive intelligence operations; and
- Consider whether additional, or more specifically articulated, criteria for the application for, and granting of, applications for programmatic surveillance orders, might be useful, along with a clear explanation, probably in legislative history, of Congress' views as to how the articulated criteria, if met, satisfy the requirements of the Fourth Amendment to the Constitution.

Conclusion

While it is axiomatic that a "state of war is not a blank check for the President,"[40] it is also true, as Justice Jackson himself warned, that the courts should not "convert the constitutional Bill of Rights into a suicide pact."[41] From the limited information available about the TSP, it appears that the TSP is within the President's constitutional authority to carry out limited electronic surveillance of suspected terrorists who would attack this Nation and kill our people. This President and, I dare say, his successors, will continue with this program, or programs like it, if they believe their constitutional duties require it. Therefore, and for a host of other reasons related to the failure of FISA to keep pace with the evolution of technology and the threats to our people, rapid amendment to FISA is vital, and I support the efforts of the Chairman, other Members of Congress, and the Administration, to do so.

---

[1] As additional relevant experience, I am currently a Principal at the Denver law firm of Morgan & Cunningham LLC, practicing primarily in the areas of information security and privacy. www.morgancunningham.net I was a

43453.183

founding co-chair of the ABA CyberSecurity Privacy Task Force, and, in January 2005, was awarded the National Intelligence Medal of Achievement for work on information issues. I serve on the National Academy of Science Committee on Biodefense Analysis and Countermeasures and am a member of the Markle Foundation Task Force on National Security in the Information Age. The views expressed in my testimony are entirely my own.

[2] While I have worked on numerous FISA-related issues, in both the Clinton and George W. Bush Administrations, I had no knowledge of the Terrorist Surveillance Program while in government, and have received no classified information about it.

[3] I refer specifically to the Section IV of Mr. Kris' March 28, 2006 testimony before this Committee, which I commend to Members as an appropriate constitutional framework for assessing the TSP.

[4] Much of the constitutional analysis in my testimony is drawn directly from my February 3, 2006 letter to this Committee entitled *Additional Constitutional Authorities Relevant to NSA Electronic Surveillance of International Terrorist Communications*, available at (www.morgancunningham.net/downloads/article_22.pdf) and/or from *amicus* briefs I co-authored with the Washington Legal Foundation, in pending litigation challenging the TSP in the Eastern District of Michigan, available at (www.morgancunningham.net/downloads/article_29.pdf) and Southern District of New York, attached hereto, and available at (http://www.wlf.org/upload/wlf%20amicus%20sdny%20brief.pdf). These materials contain many additional citations in support of the constitutional and legal principles discussed in my testimony. *See also* Andrew C. McCarthy, David B. Rivkin, Lee A. Casey, *NSA's Warrantless Surveillance Program: Legal, Constitutional, and Necessary*, *reprinted in* Federalist Society Monograph, *Terrorist Surveillance and the Constitution* (May 2006), *available at*(www.fed-soc.org/pdf/terroristsurveillance.pdf.)

[5] Before proceeding, it must be acknowledged that, in the debate over the constitutional separation of powers between the Executive and Congress -- a debate that has raged from the founding of our Nation -- there is a "poverty of really useful and unambiguous authority applicable to concrete problems of executive power as they actually present themselves" as Justice Jackson famously put it in *Youngstown*, *supra*. Further, because the full details of the TSP are unknown – and may never be known outside of classified hearings given the highly sensitive nature of the methods likely employed – I make certain assumptions for purposes of my testimony about the facts, based on publicly reported descriptions and my own experience as an intelligence and law-enforcement officer and national security attorney:

- Following the single deadliest attack against civilians on US soil by a foreign enemy (al Qaeda) in our history, facilitated, at least in part, by electronic communications between al Qaeda operatives physically located within the United States and those overseas, the President authorized the NSA to intercept international communications of individuals where there is a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, without first obtaining an order under FISA;
- The TSP targets, for interception of content, communications in which at least one party is reasonably believed to be physically located overseas, but at least some of this activity falls within FISA's definition of "electronic surveillance;"
- The President reasonably considered the TSP an important component of what he had determined, and announced – with Congressional support in the form of an authorizing resolution – to be a global campaign against al Qaeda and related terrorist organizations; and
- The President, advised by appropriate intelligence and national security law experts, reasonably concluded that the communications targeted by the TSP could not be collected in a fashion sufficiently timely to carry out, under the bureaucratically demanding strictures of FISA, his constitutional responsibilities to collect foreign intelligence to protect our Nation from attack.

[6] Admittedly, treating the Commander in Chief and foreign affairs powers as completely separate authorities would be inaccurate and artificial. Any serious assessment of the President's constitutional authority to authorize the TSP, however, must include an understanding of the foreign affairs power, and how the Supreme Court and Administrations of both political parties historically have viewed that power, and Congressional attempts to regulate its use.

[7] *U.S. Constitution*, art. II, section 1, clause 8.

[8] "The preservation of our territorial integrity and the protection of our foreign interests is intrusted, in the first instance, to the President. The Constitution, established by the people of the United States as the fundamental law of the land, has conferred upon the President the executive power; has made him the Commander in Chief of the Army and Navy; has authorized him, by and with the consent of the Senate, to make treaties, and to appoint

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00237 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.184

ambassadors, public ministers, and consuls; and has made it his duty to take care that the laws be faithfully executed. In the protection of these fundamental rights, which are based upon the Constitution and grow out of the jurisdiction of this nation over its own territory and its international rights and obligations as a distinct sovereignty, the President is not limited to the enforcement of specific acts of Congress. He takes a solemn oath to faithfully execute the office of President, and to preserve, protect, and defend the Constitution of the United States. To do this he must preserve, protect, and defend those fundamental rights which flow from the Constitution itself and belong to the sovereignty it created. 22 U.S. Op. Atty. Gen. 13, 25-26, *Foreign Cables*, (1898) (citing, *inter alia*, *Cunningham v. Neagle*, 135 U.S. 1 (1890) (emphasis added). Indeed, the founders of our republic specifically recognized the primary position of the President in the field of foreign affairs. For an excellent discussion of this history, *see* Powell, H. Jefferson, *The Founders and the President's Authority over Foreign Affairs*. William & Mary Law Review, Vol. 40, pp. 1471-1537 (May 1999).

[9] 343 U.S. 579 (1952). The same Justice Robert Jackson who wrote the 1952 *Youngstown* concurrence (a primarily domestic case) several years earlier, in *Johnson v. Eisentrager*, wrote for the majority of the Supreme Court that the issues in that case involved "a challenge to [the] conduct of diplomatic and foreign affairs, *for which the President is exclusively responsible*." 339 U.S. 763, 789 (1950) (emphasis added).

[10] 484 US 518, 527, 530 (1988).

[11] 299 U.S. 304, 320 (1936) (emphasis added)

[12] *New York Times Co. v. United States*, 403 U.S. 713, 727-28 (1971) (footnotes omitted) (emphasis added).

[13] *Id.* at 741.

[14] Moreover, the Vesting Clause provides that "[t]he executive Power shall be vested in a President of the United States of America." U.S. Const. art. II, § 1. In sharp contrast, Article I, Section I states only that: "All legislative Powers *herein granted* shall be vested in a Congress of the United States." (emphasis added) The Supreme Court has found this difference important: "The difference between the grant of legislative power under article 1 to Congress which is limited to powers therein enumerated, and the more general grant of the executive power to the President under article 2, is significant. . . .[T]he executive power is given in general terms strengthened by specific terms where emphasis is appropriate, and limited by direct expressions where limitation is needed. . . .[A]rticle 2 grants to the President the executive power of the government . . . [and] the provisions of the second section of article 2, which blend action by the legislative branch, or by part of it, in the work of the executive, are limitations to be strictly construed, and not to be extended by implication." *Myers v. United States*, 272 U.S. 52, 128, 163-64 (1926).

[15] *Webster v. Doe*, 486 U.S. 592, 605-06 (1988) (O'Connor, J., concurring in part, dissenting in part) (emphasis added) (*citing* prior Supreme Court decisions in *United States v. Curtiss-Wright Export Corp.*, *Department of Navy v. Egan*, and *Totten v. United States*, 92 U.S. 105 (1876)). *See also* numerous United States Supreme Court and other decisions cited in Section I of the Cunningham/WLF brief in the Southern District of New York, *supra* note 4.

[16] Of the very few cases beyond *Youngstown* cited by opponents of the TSP for the proposition that the program is unconstitutional, the principal decision is *Little v. Barreme*, 6 U.S. 170 (1804). This case sometimes is cited for the proposition that the Supreme Court has rejected the President's power to act where his actions (seizing boats sailing *from* French ports where Congress authorized only the seizure of boats sailing *to* French ports) were unauthorized or prohibited by Congress. For at least three reasons, *Barreme* provides no support for the TSP's opponents. First, it appears clear that the Executive Branch in *Barreme* was attempting to *comply with the Act*, but made a mistake by including supplemental instructions to seize ships sailing *to* French ports. 6 U.S. at 178. This is reinforced by the fact that "a copy of the act was transmitted by the secretary of the navy, to the captains of armed vessels, *who were ordered to consider* [the Act] *as a part of their instructions*." *Id.* Second, much like the situation in *Youngstown* (and now *Hamdan*), the congressional limitations in *Barreme* dealt with activities primarily committed to Congress in the text of the Constitution itself. These include the powers to: "regulate commerce with foreign nations, and among the several states, and with the Indian tribes," Art. I, § 8, cl. 3; "define and punish piracies and felonies committed on the high seas, and offenses against the law of nations," Art. I, § 8, cl. 10; and "declare war, grant letters of marque and reprisal, and make rules concerning captures on land and water," Art. I, § 8, cl. 11. There are no such explicit constitutional authorities for Congress in the realm of foreign intelligence collection. Finally, the fact that there are *exceptions* to the President's general constitutional primacy in foreign affairs -- which are explicitly spelled out in the Constitution itself and are to be narrowly construed -- only proves the rule of the President's general primacy. Thus, *Barreme* is irrelevant to a separation-of-powers assessment of the TSP which, as demonstrated elsewhere in this testimony, lies at the "core" of the President's constitutional authorities, and not within the core constitutional authorities of Congress.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00238 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.185

[17] Justice Jackson himself, in *Youngstown*, recognized the primarily domestic nature of that case, although many opponents of the TSP seem not to, when he cautioned: "I should indulge the widest latitude of interpretation to sustain [the President's] exclusive function to command the instruments of national force, *at least when turned against the outside world* for the security of our society. But, when it is turned inward, not because of rebellion *but because of a lawful economic struggle between industry and labor*, it should have no such indulgence. *Youngstown* at 645 (emphasis added). Indeed, our courts have long recognized that separation-of-powers conflicts between the Congress and the President raising primarily foreign affairs and national security issues must be analyzed differently than cases like *Youngstown*, which principally involved a domestic issue, but having only indirect or incidental implications for the exercise of the President's foreign affairs authorities. As one court cautioned: "Several important factors must be considered in order to understand the impact of [*Youngstown*]. . . . [A]lthough the executive had argued that the seizures were related to the war power, in essence the President was obtruding into the field of labor relations, an area traditionally assigned to the Congress. Even though the nationalization and the Court's injunction of the President's action might have had some, although indirect, effect on the foreign relations of this country, such import, if any, would have been clearly minimal compared to the drastic change which nationalization by the President would otherwise have brought about in the free enterprise system. Contrasting...[*Youngstown*] with *Curtiss-Wright*, for example, clearly reveals the different set of considerations raised by foreign relations cases. *Atlee v. Laird*, 347 F.Supp. 689, 701-02 (E.D. Pa. 1972), *aff'd*, 411 U.S. 911 (1973) (emphasis added) (footnotes omitted).

[18] 484 F.2d 418, 426 (5th Cir. 1973) (emphasis added) (citations omitted); *Accord United States v. Butenko*, 494 F.2d 593, 603 (3d Cir. 1974), (noting that while the "Constitution contains no express provision authorizing the President to conduct surveillance . . . it would appear that such power is . . . implied from his duty to conduct the nation's foreign affairs"). The passage of FISA, and the passage of years since, in no way undermine the reasoning of the *Brown* court, and other authorities cited herein, as to the constitutional and practical reasoning for Presidential primacy in this area.

[19] *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980) (emphasis added) (citations omitted).. Although adjudicating a pre-FISA fact pattern, the *Truong* court was well aware of FISA's passage as it discussed the important policy considerations in deciding the separation-of-powers question regarding congressional restrictions on the President's foreign intelligence gathering powers.

[20] *In re Sealed Case, No. 02-001*, 310 F.3d 717, 745 (FISA Ct. Rev. 2002) (emphasis added).

[21] 433 U.S. 425, 443 (1977).

[22] 491 U.S. 440 (1989)

[23] *Id.* at 484 (citations omitted).

[24] *Id.* at 482-88. *See also, e.g., Clinton v. Jones*, 520 U.S. 681, 702 (1997), in which the Supreme Court reiterated that a violation of the separation of powers is measured by determining whether the action rises "to the level of constitutionally forbidden impairment of the Executive's ability to perform its constitutionally mandated functions."

[25] Precisely like FISA, Title III prescribes criminal penalties for violating its provisions. 18 U.S.C. § 2511.

[26] *Sharing Title III Electronic Surveillance Material With the Intelligence Community*, Op. Off. Legal Counsel, 2000 WL 33716983 at 9 (Oct. 17, 2000) (emphasis added) (internal citations omitted). Similarly, Walter Dellinger, Assistant Attorney General for the Office of Legal Counsel, and signatory to a January 2006 letter challenging the legality of the TSP, advised President Clinton's Administration of the "general proposition that I believe to be uncontroversial: there are circumstances in which the President may appropriately decline to enforce a statute that he views as unconstitutional." *Presidential Authority to Decline to Execute Unconstitutional Statutes*, 4A U.S. Op. OLC 55, November 2, 1994 at 2 (emphasis added).

[27] *H.R. Conf.Rep.No. 95-1720*, at 35, *reprinted in* U.S.C.C.A.N., 4048, 4064.

[28] *Kris Testimony, supra* note 3, at 9-10.

[29] 548 U.S. ___ (2006).

[30] *Slip. op.* at 29 (emphasis added).

[31] *Marbury vs. Madison,* 5 U.S. (1 Cranch) 137, 178 (1803).

[32] *Hamdan, supra* note 29, *Slip. op.* at 29, n. 23.

[33] *Id., Slip op. (Kennedy Opinion)* at 10 (Kennedy, J., concurring in part).

[34] *Slip op.* at 27.

[35] http://www.morgancunningham.net/show_article.php?id=20.

[36] *See, e.g.,* testimony and writings of Kim Taipale particularly his June 19, 2006 testimony before the House Permanent Select Committee on Intelligence.
[37] *Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment,* July 2006, at 8 (available at http://www.markle.org/downloadable_assets/2006_nstf_report3.pdf.)
[38] Emphasis added.
[39] There are related technologies available today, also endorsed by, among others, the Markle Task Force, such as anonymization of sensitive data, and anonymized searching and matching of that data, that also could have far-reaching positive effects on our civil liberties and ability to win the war on terror. *Supra* note 37 at 63-65. Such technological developments are at least equally applicable to many important well outside national security, including health care, financial, and other information.
[40] *Hamdi v. Rumsfeld*, 542 U.S. 507, 536 (2004) (plurality op.).
[41] *Terminiello v. Chicago*, 337 U.S. 1, 36 (1949) (Jackson, J., dissenting).

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00240 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.187

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

CENTER FOR CONSTITUTIONAL RIGHTS, TINA M. FORSTER, GITANJALI S. GUTIERREZ, SEEMA AHMAD, MARIA LAHOOD and RACHEL MEEROPOL,	:	
Plaintiffs,	:	Case No. 06-cv-313
v.	:	Judge Gerard E. Lynch
	:	Magistrate Judge Kevin Fox
GEORGE W. BUSH, President of the United States; NATIONAL SECURITY AGENCY, LTG Keith B. Alexander, CENTRAL INTELLIGENCE AGENCY, Gen. Michael V. Hayden, Director; DEPARTMENT OF HOMELAND SECURITY, Michael Chertoff, Secretary; FEDERAL BUREAU OF INVESTIGATION, Robert S. Mueller, III, Director; and JOHN D. NEGROPONTE, Director of National Intelligence,	:	: **ECF CASE**
Defendants.	:	

MEMORANDUM OF AMICUS CURIAE WASHINGTON LEGAL FOUNDATION IN OPPOSITION TO PLAINTIFFS' MOTION FOR PARTIAL SUMMARY JUDGMENT AND IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT

H. Bryan Cunningham
MORGAN & CUNNINGHAM LLC
Two Tamarac Center, Suite 425
7535 East Hampden Avenue
Denver, CO 80231
(303) 743-0003

Daniel J. Popeo
Paul D. Kamenar
WASHINGTON LEGAL FOUNDATION
2009 Massachusetts Ave., NW
Washington, DC 20046
(202) 588-0302

Timothy A. Valliere [TV 1198]
BUSHELL & VALLIERE LLP
60 E. 42d Street
Suite 2925
New York, NY 10165
(212) 949-4700

June 6, 2006

43453.188

TABLE OF CONTENTS

INTERESTS OF AMICUS CURIAE 1

INTRODUCTION 2

SUMMARY OF ARGUMENT 4

ARGUMENT 5

I. TO THE EXTENT THAT FISA IMPAIRS THE PRESIDENT'S ABILITY TO CONDUCT ELECTRONIC SURVEILLANCE OF INTERNATIONAL COMMUNICATIONS FROM SUSPECTED TERRORISTS TO OR FROM THE UNITED STATES TO PROTECT THE COUNTRY FROM ATTACK, IT VIOLATES THE SEPARATION OF POWERS 5

A. The Supreme Court Has Consistently Recognized the President's "Plenary" Authority in Foreign Affairs 6

B. Foreign Intelligence Collection Operations Lie at the "Core" of the President's Plenary Foreign Affairs Powers 8

C. Plaintiffs' Reliance on Justice Jackson's Concurring Opinion in *Youngstown* as Trumping the President's Power to Collect Foreign Intelligence under the NSA Program Is Misplaced 13

1. Plaintiffs' Interpretation of Justice Jackson's *Youngstown* Concurrence is Fatally Flawed 13

2. Even if the President's Power is in Zone 3, It is Not Extinguished . . . 15

3. *Youngstown* is Further Distinguishable Because It was Principally a Domestic Case, Whereas the NSA Program is Principally a Foreign Affairs Activity 16

D. FISA, if Applied to the NSA Program, Would Violate Separation of Powers by Encroaching on the President's Constitutional Authority 20

CONCLUSION 24

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00242 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.189

TABLE OF AUTHORITIES

Cases:

Atlee v. Laird, 347 F.Supp. 689 (E.D. Pa. 1972), *aff'd*, 411 U.S. 911 (1973) 18
Chicago & Southern Air Lines v. Waterman S.S. Corp., 333 U.S. 103 (1948) 9
Clinton v. Jones, 520 U.S. 681 (1997) 22
Dep't of the Navy v. Egan, 484 U.S. 518 (1988) 7
Earth Island Inst. v. Christopher, 6 F.3d 648 (9th Cir. 1993) 15
El-Masri v. Tenet, 1:05cv1417, 2006 WL 1391390 (E.D. Va. May 12, 2006) 1
Goldwater v. Carter, 444 U.S. 996 (1979) 1, 19
Haig v. Agee, 453 U.S. 280 (1981) 9
Hamdi v. Rumsfeld, 542 U.S. 507 (2004) 1, 23
In re Sealed Case, No. 02-001, 310 F.3d 717 (FISA Ct. Rev. 2002) 12
Johnson v. Eistentrager, 339 U.S. 763 (1950) 6
Kennett v. Chambers, 55 U.S. 38 (1852) 6
Little v. Barreme, 6 U.S. 170 (1804) 19
Myers v. United States, 272 U.S. 52 (1926) 8
New York Times Co. v. United States, 403 U.S. 713 (1971) 7
Nixon v. Adm'r of General Services, 433 U.S. 425 (1977) 20
Prize Cases, 67 U.S. 635 (1862) 9
Public Citizen v. United States, 491 U.S. 440 (1989) 20, 21
Terminiello v. Chicago, 337 U.S. 1 (1949) 24
Totten v. United States, 92 U.S. 105 (1875) 9
United States v. Belmont, 301 U.S. 324 (1937) 6
United States v. Brown, 484 F.2d 418 (5th Cir. 1973) 10, 18-19
United States v. Butenko, 494 F.2d 593 (3d Cir. 1974) 11
United States v. Curtiss-Wright Export Co., 299 U.S. 304 (1936) 6
United States v. Eliason, 41 U.S. 291 (1842) 16
United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980) 11, 12
United States v. U.S. Dist. Ct., 407 U.S. 297 (1972) 8, 12
Webster v. Doe, 486 U.S. 592 (1988) 10
Youngstown Sheet and Tube v. Sawyer, 343 U.S. 579 (1952) ..... passim

Constitution and Statutes:

U.S. Constitution
Art. I, § 1 7
Art. I, § 8, cl. 3 19
Art. I, § 8, cl. 10 19
Art. I, § 8, cl. 11 19
Art II, § 1 7
18 U.S.C. § 2511 22
50 U.S.C. §§ 1801-62 4

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00243 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.190

Authorization for Use of Military Force, Pub. L. No. 107-40, § 2(a), 115 Stat. 224, (2001) (reported as a note to 50 U.S.C.A. § 1541 ("AUMF") 2, 5, 8

Legislative History and Administrative Materials:

H.R. Conf. Rep. No. 95-1720, reprinted in U.S.C.C.A.N. 4048, 4064 23
Military Order § 1(c), 66 Fed. Reg. at 57,833 (Nov. 16, 2001) 3

Miscellaneous:

Andrew C. McCarthy, David B. Rivkin, Lee A. Casey, *NSA's Warrantless Surveillance Program: Legal, Constitutional, and Necessary, reprinted in* Federalist Society Monograph, TERRORIST SURVEILLANCE AND THE CONSTITUTION (May 2006), *available at* http://www.fed-soc.org/pdf/terroristsurveillance.pdf 2, 13
H. Jefferson Powell, *The Founders and the President's Authority Over Foreign Affairs*, 40 Wm. & Mary L. Rev. 1471 (1999) 7
K. A. Taipale, *Whispering Wires and Warrantless Wiretaps: Data Mining and Foreign Intelligence,* N.Y.U. Rev. of L. & Sec., No. VII Suppl. Bull. on L. & Sec. (Spring 2006) (forthcoming, currently available at http://whisperingwires.info/) 17
President George W. Bush, Remarks at Camp David (Sept. 15, 2001) 2
Proposed Deployment of United States Armed Forces Into Bosnia, 19 Op. Off. Legal Counsel 327 (1995) 15-16
Sharing Title III Electronic Surveillance Material With the Intelligence Community, Op. Off. Legal Counsel, 2000 WL 33716983 at 9 (Oct. 17, 2000) 23
U.S. Dep't of Justice, *Legal Authorities Supporting the Activities of the National Security Agency by the President* (Jan. 19, 2006), *available at* http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf 2, 3

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00244 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.191

INTERESTS OF AMICUS CURIAE

The interests of amicus curiae Washington Legal Foundation (WLF) are more fully presented in its motion for leave to file this Memorandum. WLF is a national, non-profit public interest law and policy center, based in Washington, D.C., with supporters nationwide. WLF has devoted substantial resources to national security and separation-of-powers cases over the last 29 years and has appeared as counsel or amicus in numerous such cases in the Supreme Court and lower federal courts. *See, e.g.*, *Goldwater v. Carter*, 444 U.S. 996 (1979); *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004); *MacWade v. Kelly*, No. 05 Civ. 6921, 2005 U.S. Dist. LEXIS 39695 (S.D.N.Y. Dec. 7, 2005) (supporting New York City's container inspection program for city subways to deter terrorist bombing attacks).

The Defendants are asserting the state and military secrets privileges in this case, which likely will preclude the Court from reaching the merits of Plaintiffs' claims that certain warrantless electronic surveillance of international communications by the Defendants is unlawful. While WLF supports the Defendants' assertion of those privileges, which have been determined to be valid in other cases,[1] WLF nevertheless believes it appropriate for the Court to have before it some additional constitutional counterargument to Plaintiffs and their amici regarding the separation-of-powers issues that this case presents. WLF's Memorandum will help place this case in proper constitutional perspective and may, indeed, assist the Court in ruling on the validity of the privileges asserted.

---

[1] *See, e.g., El-Masri v. Tenet*, 1:05cv1417, 2006 WL 1391390 (E.D. Va. May 12, 2006) (upholding assertion of state secrets privilege to preclude adjudicating claim by German citizen that he was unlawfully abducted and mistreated by the CIA overseas).

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00245 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.192

Amicus will focus primarily on the President's constitutional authority to engage in the NSA Program, further described herein, based upon his well-established constitutional foreign affairs authorities and related authorities to gather foreign intelligence. Because of space limitations, amicus will not address Plaintiffs' other arguments, but submit that they must fail.[2]

INTRODUCTION

Following the largest ever foreign attack on American soil, killing over 3,000 civilians on September 11, 2001, the President of the United States made clear to the American public: "We're at war. There has been an act of war declared upon America by terrorists, and we will respond accordingly." President George W. Bush, Remarks at Camp David (Sept. 15, 2001). Shortly thereafter, 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 . . . in order to prevent any future acts of international terrorism against the United States."[3] Two months later, the President determined that al Qaeda and other foreign terrorist organizations "possess[ed] both the capability and the intention to undertake further terrorist attacks against the United States that, if not detected and

---

[2] For example, even if the merits could be reached, Plaintiffs' Fourth Amendment challenge should be rejected based on voluminous precedent concerning the constitutional analysis of government warrantless surveillance of international electronic communications (which can be, and are, intercepted by foreign countries and other third parties), and the well-recognized "special needs" doctrine. For a fuller discussion of those arguments supporting the legality of the NSA Program, *see* U.S. Dep't of Justice, *Legal Authorities Supporting the Activities of the National Security Agency by the President* (Jan. 19, 2006), *available at* http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf (hereinafter "DOJ Memo"); *see also* Andrew C. McCarthy, David B. Rivkin, Lee A. Casey, *NSA's Warrantless Surveillance Program: Legal, Constitutional, and Necessary, reprinted in* Federalist Society Monograph, TERRORIST SURVEILLANCE AND THE CONSTITUTION (May 2006), *available at* http://www.fed-soc.org/pdf/terroristsurveillance.pdf at 23-135 (hereinafter "McCarthy Monograph").

[3] Authorization for Use of Military Force, Pub. L. No. 107-40, § 2(a), 115 Stat. 224, (2001) (reported as a note to 50 U.S.C.A. § 1541) ("AUMF").

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00246 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.193

prevented, will cause mass deaths, mass injuries, and massive destruction of property, and may place at risk the continuity of operations of the United States Government." *Military Order* § 1(c), 66 Fed. Reg. 57,833-34 (Nov. 16, 2001).

Given the obvious and overriding concern about impending future attacks, and the ongoing threats by al Qaeda to strike at America and its citizens again, both here and abroad, the President authorized the National Security Agency ("NSA") to "intercept *international* communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations." DOJ Memo, *supra* note 2, at 5 (emphasis added). Amicus henceforth will refer to this activity, further described below, as the "NSA Program."

In order to intercept international communications under the NSA Program, the government must have "a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda." *Id.* at 5. The purpose of the NSA Program is exclusively to "detect and prevent another catastrophic terrorist attack on the United States" and it is intended for situations in which the government has to "move very, very quickly. FISA, by contrast, is better suited for `long term monitoring.'" *Id.* (internal citations omitted)

The NSA Program has been, and continues to be, "reviewed for legality by the Department of Justice and . . . monitored by the General Counsel and Inspector General of the NSA to ensure that civil liberties are being protected," as well as being "carefully reviewed approximately every 45 days to ensure that [it is] being used properly." *Id.* Finally, Congressional leaders in both political parties, as of January 2006, had "been briefed more than a dozen times on the" NSA Program, and continue to be briefed. *Id.* Plaintiffs have

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00247 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.194

launched a legal attack against the NSA Program, claiming that it violates, *inter alia*, the Foreign Intelligence Surveillance Act (FISA), codified at 50 U.S.C. §§ 1801-62, the constitutional doctrine of separation of powers, the First Amendment, and the Fourth Amendment.

SUMMARY OF ARGUMENT

Under our Constitution, the President of the United States is uniquely charged with the responsibility of protecting our Nation and its people from attack, including attack from international terrorists like those who, on September 11, 2001, conducted the single deadliest attack against civilians on U.S. soil by a foreign enemy in our history. The Constitution vests the President with sufficient authority to carry out this grave, fundamental, and core constitutional responsibility, including through the conduct of foreign intelligence collection operations such as the NSA Program.

Any interpretation of the Foreign Intelligence Surveillance Act (FISA), as applied to the precise facts and circumstances of the NSA Program (which cannot be determined on the present record), that would impair the President's ability to carry out his constitutional responsibilities would render FISA itself unconstitutional under the separation-of-powers doctrine. FISA could not, under such circumstances, constitutionally prevent the President from carrying out the NSA Program to collect foreign intelligence to prevent future terrorist attacks on our country.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00248 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.195

ARGUMENT

I. TO THE EXTENT THAT FISA IMPAIRS THE PRESIDENT'S ABILITY TO CONDUCT ELECTRONIC SURVEILLANCE OF INTERNATIONAL COMMUNICATIONS FROM SUSPECTED TERRORISTS TO OR FROM THE UNITED STATES TO PROTECT THE COUNTRY FROM ATTACK, IT VIOLATES THE SEPARATION OF POWERS

In Part III of their Memorandum, Plaintiffs argue that, because the NSA allegedly is engaged in electronic surveillance activities that Congress intended to foreclose when it enacted FISA in 1978, the NSA Program violates the separation of powers. Pl. Mem. at 21-32. The Plaintiffs have it exactly backwards. To the extent that FISA is interpreted as impairing the President's ability to gather timely intelligence, specifically, international electronic communications to or from suspected al Qaeda members, in order to carry out his constitutional responsibilities to protect the United States and its citizens from attack, FISA itself violates the separation of powers by encroaching on the President's well-established constitutional responsibilities and authorities.

As amicus will demonstrate, under Article II of the Constitution, the President has substantial and plenary authorities in foreign affairs and, particularly, in gathering foreign and military intelligence. Those substantial powers are further enhanced by the President's related Commander-in-Chief powers that he possesses in both peace and wartime. All of these powers must, and are, currently being exercised in our ongoing war with al Qaeda, a deadly enemy against whom Congress has authorized the President to use "all necessary and appropriate force." AUMF § 2(a).

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00249 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.196

A. The Supreme Court Has Consistently Recognized the President's "Plenary" Authority in Foreign Affairs

Over the last 150 years, the Supreme Court has had numerous opportunities to expound on the scope and nature of the President's inherent and exclusive powers, under Article II of the Constitution, to conduct foreign affairs. In 1852, for example, the Court referred to the executive branch as "that department of our government *exclusively* which is charged with our foreign relations." *Kennett v. Chambers*, 55 U.S. 38, 51 (1852) (emphasis added). In *United States v. Curtiss-Wright Export Co.*, 299 U.S. 304 (1936), the Court emphatically recognized:

> [the] *delicate, plenary and exclusive power* of the President as the sole organ of the federal government in the field of international relations--*a power which does not require as a basis for its exercise an act of Congress*, but which, of course, like every other governmental power, must be exercised in subordination to the applicable provisions of the Constitution.

Id. at 320 (emphasis added). As Justice Sutherland further explained:

> It will contribute to the elucidation of the question if we first consider the differences between the powers of the federal government in respect of foreign or external affairs and those in respect of domestic or internal affairs. That there are differences between them, and that these differences are fundamental, may not be doubted.
>
> * * * *
>
> [Congress] must often accord to the President a degree of discretion and freedom of statutory restriction which would not be admissible were domestic affairs alone involved.

Id. at 315, 320. A year later, the Court again recognized that the Executive "had the authority to speak as the sole organ of [the] Government." *United States v. Belmont*, 301 U.S. 324, 330 (1937).

Even Justice Robert Jackson, writing for the Court in *Johnson v. Eistentrager*, 339 U.S. 763 (1950), acknowledged that the President was "exclusively responsible" for the "conduct of

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00250 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.197

diplomatic and foreign affairs." *Id.* at 789. And in the so-called Pentagon Papers case, Justice Stewart, in his concurring opinion joined by Justice White, noted that:

> In the governmental structure created by our Constitution, the Executive is endowed with enormous power in the two related areas of national defense and international relations. This power, *largely unchecked by the Legislative and Judicial branches*, has been pressed to the very hilt since the advent of the nuclear missile age. For better or for worse, the simple fact is that *a President of the United States possesses vastly greater constitutional independence in these two vital areas of power than does, say, a prime minister of a country with a parliamentary form of government.*

New York Times Co. v. United States, 403 U.S. 713, 727-28 (1971) (footnotes omitted) (emphasis added). *See also id.* at 741 (Marshall, J., concurring) ("[I]t is beyond cavil that the President has broad powers by virtue of his primary responsibility for the conduct of our foreign affairs and his position as Commander in Chief."); *id.* at 756, (Blackmun, J., dissenting) ("It is plain . . . that the scope of the judicial function in passing upon the activities of the Executive Branch of the Government in the field of foreign affairs is very narrowly restricted. This view is, I think, dictated by the concept of separation of powers upon which our constitutional system rests."). Finally, in *Dep't of the Navy v. Egan,* 484 U.S. 518 (1988), Justice Blackmun, writing for the majority, reiterated that the "Court has also recognized 'the generally accepted view that foreign policy was the province and responsibility of the Executive.'" *Id.* at 529.

While it is true that the Congress has certain enumerated powers, under Article I, to declare war, to raise and support the Army, provide for a Navy, and the like, it is the President who -- in addition to his express powers to make treaties, appoint and receive ambassadors, and serve as Commander-in-Chief -- has the plenary and exclusive power to conduct foreign

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00251 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.198

affairs, as intended by the Founders.[4] Accordingly, contrary to the Plaintiffs' arguments, it is the President, not the Congress, who has constitutional primacy over foreign affairs.

B. Foreign Intelligence Collection Operations Lie at the "Core" of the President's Plenary Foreign Affairs Powers

As firmly established is the President's plenary constitutional position in foreign affairs generally, it is even stronger in the conduct of foreign and military intelligence operations.[5]

---

[4] For an excellent historical discussion of the Framers' view supporting the President's central responsibility for the conduct of foreign affairs over the power of Congress, see H. Jefferson Powell, *The Founders and the President's Authority Over Foreign Affairs*, 40 Wm. & Mary L. Rev. 1471 (1999). Moreover, the Vesting Clause provides that "[t]he executive Power shall be vested in a President of the United States of America." U.S. Const. art. II, § 1. In sharp contrast, Article I, Section I states only that: "All legislative Powers *herein granted* shall be vested in a Congress of the United States, which shall consist of a Senate and House of Representatives." (emphasis added) The Supreme Court has found this difference important:

> The difference between the grant of legislative power under article 1 to Congress which is limited to powers therein enumerated, and the more general grant of the executive power to the President under article 2, is significant. . . .[T]he executive power is given in general terms strengthened by specific terms where emphasis is appropriate, and limited by direct expressions where limitation is needed. . . .
> * * * *
> [A]rticle 2 grants to the President the executive power of the government . . . [and] the provisions of the second section of article 2, which blend action by the legislative branch, or by part of it, in the work of the executive, are limitations to be strictly construed, and not to be extended by implication. . . .

Myers v. United States, 272 U.S. 52, 128, 163-64 (1926).

[5] As the Congress recognized in the preamble to the AUMF, "the President has authority under the Constitution to deter and prevent acts of international terrorism against the United States." AUMF pmbl. Clearly, in order to deter and prevent such acts effectively, that authority must necessarily include the timely collection of foreign and military intelligence, particularly during wartime. The Supreme Court apparently agrees:

> We begin the inquiry by noting that the President of the United States has the fundamental duty under Art. II, §1, of the Constitution, to "preserve, protect, and defend the Constitution of the United States." Implicit in that duty is the power to protect our government against those who would subvert or overthrow it by unlawful means.

(continued...)

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00252 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.199

Our courts have strongly and repeatedly linked the President's inherent foreign affairs power, his duty and power to protect national security, and his Commander-in-Chief power, to his authority over foreign and military intelligence collection operations, including electronic surveillance for foreign intelligence purposes.

In the Civil War-era *Prize Cases*, the Court held that the President had the power, if not the duty, to use force to resist an attack against the United States, even in the absence of authorizing legislation. 67 U.S. 635, 688 (1862). The Supreme Court later held that President Lincoln "was undoubtedly authorized during the war, as commander-in-chief of the armies of the United States, *to employ secret agents* to enter the rebel lines *and obtain information respecting the strength, resources, and movements of the enemy*." *Totten v. United States*, 92 U.S. 105, 106 (1875) (emphasis added). No authorizing legislation by the Congress was required to enable the President to spy on the "enemy" -- inside the United States -- who had taken up arms against the Union.

The Supreme Court later recognized the inextricable link between the President's foreign affairs and foreign intelligence powers, and the strong link between those powers and the President's Commander-in-Chief power. In *Chicago & Southern Air Lines v. Waterman S.S. Corp.*, 333 U.S. 103 (1948), for example, the Court stated:

> [t]he President, both as Commander-in-Chief and as the Nation's organ for foreign affairs, has available intelligence services whose reports are not and ought not to be published to the world. It would be intolerable that courts, without the relevant information, should review and perhaps nullify actions of the Executive taken on information properly held secret.

---

[5](...continued)
United States v. United States District Court (Keith), 407 U.S. 297, 310 (1972) (emphasis added).

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00253 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.200

Id. at 111. In *Haig v. Agee*, 453 U.S. 280 (1981), the Court recognized that:

> [i]t is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation. Protection of the foreign policy of the United States is a governmental interest of great importance, since foreign policy and national security considerations cannot neatly be compartmentalized. Measures to protect the secrecy of our Government's foreign intelligence operations plainly serve these interests.

Id. at 307 (citations omitted). As Justice O'Connor stated in 1988: "The functions performed by the Central Intelligence Agency and the Director of Central Intelligence lie at the *core* of 'the very delicate, plenary and exclusive power of the President as the sole organ of the federal government in the field of international relations.'" *Webster v. Doe*, 486 U.S. 592, 605-06 (1988) (O'Connor, J., concurring in part, dissenting in part) (emphasis added).

Many federal appeals courts which have ruled on the President's authority to conduct foreign intelligence electronic surveillance operations similarly have recognized the President's considerable constitutional powers to collect foreign intelligence to protect our national security. Notably, those courts have stressed the fundamental difference between *purely* domestic cases and those involving the collection of intelligence regarding foreign threats to our nation's security (such as the instant case), and have looked with disfavor on legislative restrictions on the latter.

Twenty years after *Youngstown Sheet & Tube v. Sawyer,* 343 U.S. 579 (1952), the court in *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973), upheld the President's inherent constitutional authority to authorize warrantless wiretaps for foreign intelligence purposes. The Fifth Circuit explained its holding as follows:

> [B]ecause of the President's constitutional duty to act for the United States in the field of foreign relations, and his inherent power to protect national security in the context of foreign affairs, *we reaffirm. . . that the President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence. Restrictions upon*

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00254 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.201

> *the President's power which are appropriate in cases of domestic security become artificial in the context of the international sphere.* Our holding . . . is buttressed by a thread which runs through the Federalist Papers: that the President must take care to safeguard the nation from possible foreign encroachment, whether in its existence as a nation or in its intercourse with other nations. See e.g., The Federalist No. 64, at 434-36 (Jay); The Federalist No. 70, at 471 (Hamilton); The Federalist No. 74 at 500 (Hamilton) (J. Cooke ed. 1961).

Id. at 426 (emphasis added) (citations omitted).[6]

Similarly, in *United States v. Butenko*, 494 F.2d 593 (3d Cir. 1974), the Court noted that while the "Constitution contains no express provision authorizing the President to conduct surveillance . . . it would appear that such power is . . . implied from his duty to conduct the nation's foreign affairs." *Id.* at 603. In reaffirming the legality of warrantless foreign intelligence electronic surveillance, the *Butenko* court further noted:

> [F]oreign intelligence gathering is a clandestine and highly unstructured activity, and the need for electronic surveillance often cannot be anticipated in advance. Certainly occasions arise when officers, acting under the President's authority, are seeking foreign intelligence information, *where exigent circumstances would excuse a warrant.* To demand that such officers be so sensitive to the nuances of complex situations that they must interrupt their activities and rush to the nearest available magistrate to seek a warrant would seriously fetter the Executive in the performance of his foreign affairs duties.

Id. at 605 (emphasis added).

Perhaps most directly relevant to the instant case is the Fourth Circuit's decision in *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980). Although adjudicating a pre-FISA fact pattern, the *Truong* court was well aware of FISA's passage as it discussed the important policy considerations in deciding separation-of-powers questions regarding congressional restrictions on the President's foreign intelligence gathering powers.

---

[6] The passage of FISA, and the nearly 30 years since, in no way undermines the reasoning of the *Brown* court, and other authorities cited herein, as to the constitutional and practical reasons for Presidential primacy in this area.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00255 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.202

> For several reasons, the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would, following *Keith,* [*United States v. U.S. Dist. Ct.*, 407 U.S. 297 (1972)] "unduly frustrate" the President in carrying out his foreign affairs responsibilities. First of all, attempts to counter foreign threats to the national security require the utmost stealth, speed, and secrecy. A [uniform] warrant requirement would add a procedural hurdle that would reduce the flexibility of executive foreign intelligence initiatives, [and] in some cases delay executive response to foreign intelligence threats. . . .
>
> * * * *
>
> Perhaps most crucially, the executive branch not only has superior expertise in the area of foreign intelligence, it is also constitutionally designated as the pre-eminent authority in foreign affairs . . . . Just as the separation of powers in *Keith* forced the executive to recognize a judicial role when the President conducts domestic surveillance, so the separation of powers requires us to acknowledge the *principal responsibility of the President for foreign affairs and concomitantly for foreign intelligence surveillance.*

Id. at 913-14 (emphasis added) (citations omitted).[7]

Finally, it is instructive that the special Foreign Intelligence Court of Review recognized in a post-FISA, and post-September 11, case, that:

> [t]he *Truong* court, as did all the other courts to have decided the issue, held that the President did have the 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, No. 02-001, 310 F.3d 717, 745 (FISA Ct. Rev. 2002) (emphasis added). In rejecting a Fourth Amendment argument made by the ACLU as amicus in that case, the Court of Review held that FISA, as amended by the PATRIOT Act, was constitutional, "*[e]ven*

---

[7] As Plaintiffs acknowledge, the Supreme Court in *Keith*, referred to in *Truong*, emphasized that the case "involve[d] only the domestic aspects of national security. We have not addressed, *and express no opinion* as to the issues which may be involved with respect to activities of foreign powers or their agents." 407 U.S. at 321-22 (footnote omitted, citing to authority for the proposition that "warrantless surveillance, though impermissible in domestic security cases, may be constitutional where foreign powers are involved.") (emphasis added).

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00256 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.203

without taking into account the President's inherent constitutional authority to conduct warrantless foreign intelligence surveillance." Id. at 746 (emphasis added).

Accordingly, amicus submits that the President's constitutional authority to conduct foreign intelligence surveillance under the NSA Program is well established.

C. Plaintiffs' Reliance on Justice Jackson's Concurring Opinion in *Youngstown* as Trumping the President's Power to Collect Foreign Intelligence under the NSA Program is Misplaced

Plaintiffs rely heavily on Justice Jackson's concurring opinion in *Youngstown Sheet & Tube*, 343 U.S. 579, 592 (1952) (Jackson, J., concurring), to support their argument that the NSA Program violates the separation of powers by allegedly violating FISA's requirements. Pl. Mem. at 22-25. Assuming, *arguendo*, that the terms of FISA apply to the NSA Program,[8] amicus submits that Plaintiffs' reliance on *Youngstown* is misplaced and, in any event, not dispositive of the instant case.

1. Plaintiffs' Interpretation of Justice Jackson's *Youngstown* Concurrence is Fatally Flawed

Plaintiffs' argument goes essentially as follows: Congress has certain substantial constitutional authorities under Article I, including those relating to war powers, foreign affairs, and foreign intelligence gathering, and enacted FISA allegedly pursuant to those authorities. Congress intended the procedures of FISA to be the "exclusive means" governing all government electronic surveillance for foreign intelligence collection purposes. Therefore,

---

[8] *See McCarthy Monograph*, *supra* note 2, at 54-60 (concluding that FISA need not be invalidated in order to uphold the NSA Program, inasmuch as a careful parsing of the FISA provisions themselves -- both with respect to who is covered and what electronic communications are covered -- reveal that they are rather narrow, particularly those provisions that incorporate a "reasonable expectation of privacy" standard, since, arguably, it is not "reasonable" to expect international electronic communications to be private).

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00257 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.204

despite the President's "core" powers under Article II in this area, he has "violated the law" because he authorized electronic surveillance of international communications with suspected al Qaeda agents without obtaining a FISA order, which, although not technically a warrant, is functionally equivalent to one.

To support this flawed syllogism (even assuming the dubious proposition that Congress has substantial foreign intelligence authorities), Plaintiffs principally rely on Justice Jackson's oft-cited concurring opinion in *Youngstown Sheet & Tube v. Sawyer,* 343 U.S. 579 (1952), where the Court was faced with a challenge to President Truman's order to have the federal government take possession and control of the Nation's steel mills during the Korean conflict. In his attempt to ensure a reliable supply of steel for the war effort in light of a looming labor strike, President Truman chose not to invoke certain statutes that dealt with seizure of property and the settlement of labor disputes. *Id.* at 582-83.

Justice Jackson assayed the constitutional powers of the President as follows: In the so-called "Zone 1," where a President acts pursuant to an express or implied authorization by Congress, the President's power is at its "zenith" because he exercises not only his own constitutional powers, but "all that Congress can delegate." *Id.* at 635. In "Zone 2," where Congress has not spoken in a particular area, the President is in a "zone of twilight" and must rely upon his constitutional powers alone. *Id.* at 637. Finally, in "Zone 3," where the President's actions are "incompatible with the express or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter." *Id.*

Plaintiffs assert that the NSA Program must fall into Zone 3, based on (1) their reading

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00258 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.205

of FISA's exclusivity provision, and (2) their rejection of any argument that the AUMF *is* a statutory augmentation of the President's own constitutional powers in the area of foreign intelligence electronic surveillance. Even if the NSA Program falls under Zone 3, the President's authority in this case must be sustained based upon a proper application of the *Youngstown* opinion and subsequent separation-of-powers cases.

2. Even if the President's Constitutional Authority is in Zone 3, It is Not Extinguished

Even if the President is exercising powers that are incompatible with "the expressed or implied will of Congress," that does not mean he has acted unlawfully. According to Justice Jackson, the President may still rely "upon his own constitutional powers minus any constitutional powers of Congress over the matter." *Id.* This statement would make no sense unless Justice Jackson contemplated circumstances in which powers that are exercised, even at this "lowest ebb," were still sufficiently robust to sustain the constitutionality of the President's action in the teeth of contrary legislation.

More importantly, even if Congress had some constitutional powers with respect to the general subject matter under scrutiny, a proper balancing of those interests by a court would recognize the primacy of presidential power over congressional power in the area of foreign affairs and, particularly, foreign intelligence collection. If it were otherwise, then the Congress could, for example: by virtue of its power to ratify treaties, control negotiations with foreign governments;[9] by virtue of its authority to declare war, prevent a President from using military

[9] *See, e.g.*, *Earth Island Inst. v. Christopher*, 6 F.3d 648, 652 (9th Cir. 1993) ("The district court correctly ruled that the section 609(a) claims relate to 'the foreign affairs function, which rests within the exclusive province of the Executive Branch under Article II, section 2 of the United States Constitution.' The statute's requirement that the Executive initiate discussions with foreign nations (continued...)

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00259 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.206

force to respond to an overseas attack on Americans;[10] or, by virtue of its authority to make rules for the Army and Navy, prohibit the President, as Commander-in-Chief, from holding courts martial for military personnel.[11] In each of these circumstances, the judiciary and/or executive branch legal opinions have wisely rejected, as unconstitutional, exercises of Congress's power that impair the President's ability to carry out his constitutionally assigned responsibilities, even though Congress clearly had some articulable constitutional authority in the areas at issue. So too is the case here.

Taken to its logical extreme, the Plaintiffs' position, if adopted, would fundamentally alter the system of separation of powers and checks and balances created by our Constitution, transforming our governmental system into one in which Congress alone reigns supreme in virtually all spheres of the exercise of governmental power.

3. *Youngstown* is Further Distinguishable Because It was Principally a Domestic Case, Whereas the NSA Program is Principally a Foreign Affairs Activity

Plaintiffs' attempt to apply Justice Jackson's analysis to a case that primarily involves foreign affairs and foreign intelligence, as does the case at bar, is even further off the mark. A cursory reading of *Youngstown* makes clear that, although the executive/congressional conflict

---

[9](...continued)
violates the separation of powers, and this court cannot enforce it").

[10] With respect to the War Powers Resolution, 50 U.S.C. § 1541(c), the Executive Branch under both parties has taken the position that "the President's power to deploy armed forces into situations of actual or indicated hostilities is not restricted to the three categories specifically marked out by the [War Powers] Resolution." Proposed Deployment of United States Armed Forces Into Bosnia, 19 Op. Off. Legal Counsel OLC 327 (1995) (citing Overview of the War Powers Resolution, 8 Op. Off. Legal Counsel 271, 274-75 (1984)).

[11] *United States v. Eliason*, 41 U.S. 291, 301 (1842) ("The power of the executive to establish rules and regulations for the government of the army, is undoubted.")

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00260 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.207

at issue in that case unfolded against the backdrop of the Korean War, the legal and factual issues at stake were far more "domestic" in nature than those raised by the NSA Program.

As noted, *Youngstown* involved President Truman's order to seize and control private U.S. steel mills after the failure of the industry and unions to reach a collective bargaining agreement. 343 U.S. at 582-84. In striking down President Truman's attempted seizure of the steel mills by executive order, rather than following legislation dealing with emergencies, the *Youngstown* Court described the powers of Congress as follows: "It can authorize the taking of private property for public use. It can make laws regulating the relationships between employers and employees, prescribing rules designed to settle labor disputes, and fixing wages and working conditions in certain fields of our economy." *Id.* at 588. Even Justice Jackson recognized the primarily "domestic" nature of the case, when he cautioned:

> We should not use this occasion to circumscribe, much less to contract, the lawful role of the President as Commander-in-Chief. *I should indulge the widest latitude of interpretation to sustain his exclusive function to command the instruments of national force, at least when turned against the outside world* for the security of our society. But, when it is turned inward, not because of rebellion *but because of a lawful economic struggle between industry and labor*, it should have no such indulgence.

Id. at 645 (emphasis added).[12]

---

[12] Unlike the relatively long time delay involved in the production of steel before it can be put to military use, such as manufacturing a military vehicle or ship, the interception of vital and useful foreign intelligence to detect and prevent a terrorist attack often requires rapid and immediate action. Indeed, in a post September 11 world, the action required may be more rapid and immediate than FISA can accommodate. It is impossible for this or any court to determine, in the absence of specific facts and circumstances, whether FISA, as applied to the NSA Program, unconstitutionally impairs the President's ability to carry out of his constitutional responsibilities. One example, however, of how FISA could impair the collection of timely intelligence is the obvious impossibility of gathering sufficient information about a one-time, in-progress, short-duration terrorism warning phone call, and preparing it for submission to, and approval by, the FISA Court (or, for emergency authorization, the Attorney General) in time to intercept the contents of the call.

More generally, since the NSA Program was disclosed, experts have given other explanations

(continued...)

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00261 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.208

Accordingly, courts have long recognized — both before and after *Youngstown* -- that separation-of-powers conflicts between the Congress and the President raising primarily foreign affairs and national security issues must be analyzed differently than cases like *Youngstown*, which principally involved a domestic issue, but having only indirect or incidental implications for the exercise of the President's foreign affairs and Commander-in-Chief powers. As one court cautioned:

> Several important factors must be considered in order to understand the impact of [*Youngstown*]. . . . [A]lthough the executive had argued that the seizures were related to the war power, in essence the President was obtruding into the field of labor relations, an area traditionally assigned to the Congress. Even though the nationalization and the Court's injunction of the President's action might have had some, although indirect, effect on the foreign relations of this country, such import, if any, would have been clearly minimal compared to the drastic change which nationalization by the President would otherwise have brought about in the free enterprise system. Contrasting...[*Youngstown*] with *Curtiss-Wright*, for example, clearly reveals the different set of considerations raised by foreign relations cases.

Atlee v. Laird, 347 F.Supp. 689, 701-02 (E.D. Pa. 1972), *aff'd*, 411 U.S. 911 (1973) (emphasis added) (footnotes omitted).

As previously noted, in *United States v. Brown*, the Fifth Circuit, in upholding the

---

[12](...continued)
for the incompatibility of FISA's procedural strictures with the reality of the post-September 11, 2001 world. *See, e.g.*, K. A. Taipale, *Whispering Wires and Warrantless Wiretaps: Data Mining and Foreign Intelligence,* N.Y.U. Rev. of L. & Sec., No. VII Suppl. Bull. on L. & Sec. (Spring 2006) (forthcoming, currently available at http://whisperingwires.info/) (FISA is "inadequate to address recent technology developments, including: the transition from circuit-based to packet-based communications; the globalization of communications infrastructure; and the development of automated monitoring techniques, including data mining and traffic analysis.") *citing* Richard A. Posner, *Commentary: A New Surveillance Act*, Wall St. J. A16 (Feb. 15, 2006) (FISA is "hopeless as a framework for detecting terrorists. [FISA] requires that surveillance be conducted pursuant to warrants based on probable cause to believe that the target of surveillance is a terrorist, when the desperate need is to find out who is a terrorist."). In short, in order "to connect the dots," one must first collect the dots, a task extremely difficult or impossible today under all the 1978 procedures of FISA.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00262 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.209

President's inherent constitutional authority to order warrantless foreign intelligence wiretaps, recognized that "[r]estrictions upon the President's power which are appropriate in cases of domestic security become artificial in the context of the international sphere." 484 F.2d 418, 426 (5th Cir. 1973). Furthermore, as Chief Justice Warren Burger noted in *Goldwater v. Carter*, 444 U.S. 996 (1979):

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

Id. at 1004-05 (Burger, C.J., concurring) (emphasis added) (citations omitted).

In primarily foreign affairs/national security cases, such as the instant one, greater deference must be given the President's constitutional authority vis-a-vis the expression of congressional will on the subject. This fundamental difference between the powers asserted in *Youngstown* and the NSA Program eviscerates the Plaintiffs' separation-of-powers argument.[13]

---

[13] In addition to *Youngstown*, Plaintiffs cite *Little v. Barreme*, 6 U.S. 170 (1804) for the proposition that the Supreme Court has "rejected the President's power to act" where his actions (seizing boats sailing *from* French ports where Congress authorized only the seizure of boats sailing *to* French ports) were "unauthorized or prohibited by Congress." Pl. Mem. at 25. For at least three reasons, *Barreme* provides no support for Plaintiffs' position. First, it appears clear that the Executive Branch in *Barreme* was attempting to *comply with the Act*, but made a mistake by including supplemental instructions to seize ships sailing *to* French ports. 6 U.S. at 178. This is reinforced by the fact that "a copy of the act was transmitted by the secretary of the navy, to the captains of armed vessels, *who were ordered to consider* [the Act] *as a part of their instructions*." *Id.*

Second, much like the situation in *Youngstown*, the congressional limitations in *Barreme* dealt with activities primarily committed to the Congress in the text of the Constitution itself. These include the powers to: "regulate commerce with foreign nations, and among the several states, and with the Indian tribes," Art. I, § 8, cl. 3; "define and punish piracies and felonies committed on the high seas, and offenses against the law of nations," Art. I, § 8, cl. 10; and "declare war, grant letters of marque and reprisal, and make rules concerning captures on land and water." Art. I, § 8, cl. 11. Plaintiffs do

(continued...)

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00263 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.210

D. FISA, if Applied to the NSA Program, Would Violate Separation of Powers by Encroaching on the President's Constitutional Authorities

Even if Congress has attempted to occupy the field for intercepting international communications through FISA as the "exclusive means," and the President's exercise of his constitutional authority in this area is at its "lowest ebb," FISA is unconstitutional as applied if FISA impermissibily interferes with the proper execution of the President's own authorities and responsibilities as Chief Executive, Commander-in-Chief, and "sole organ" of international relations (an issue this Court likely cannot resolve as a factual matter due to the invocation of the state and military secrets privilege). Rather than the simplistic bright-line approach urged by Plaintiffs to decide separation-of-powers cases, the Court, post-*Youngstown*, has repeatedly made clear that a balancing-of-powers approach must be used.[14]

In *Nixon v. Adm'r of General Services*, 433 U.S. 425 (1977), for example, the Court held that "in determining whether [a legislative] Act disrupts the proper balance [of power] between the coordinate branches, the proper inquiry focuses on the extent to which it prevents the executive from accomplishing its constitutionally assigned functions." *Id.* at 443. In *Public Citizen v. United States*, 491 U.S. 440 (1989), the Supreme Court was faced with the issue of whether the Federal Advisory Committee Act (FACA), which established procedures by which

---

[13](...continued)
not, as they cannot, assert any such explicit constitutional authorities for Congress in the realm of foreign intelligence collection.

Finally, the fact that there are *exceptions* to the President's general constitutional primacy in foreign affairs -- which are explicitly spelled out in the Constitution itself and are to be narrowly construed -- only proves the rule of the President's general primacy. Thus, *Barreme* is irrelevant to a separation-of-powers assessment of the NSA Program which amicus have demonstrated lies at the "core" of the President's constitutional authorities, and not within the authorities of Congress.

[14] Indeed, even Justice Jackson admitted that his own tripartite categorization of presidential powers was "somewhat oversimplified." *Youngstown*, 343 U.S. at 635.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00264 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.211

the Executive branch utilizes private advisory committees, was constitutional *as applied* to a putative private advisory committee formed by the American Bar Association (ABA) that advised the President on the qualifications of potential federal judicial nominees. Under Article II, the President has the power to appoint judges, but the Senate also has a clear and important advise and consent power. At first blush, the legislative branch would seem to have constitutional authority over that shared power, in addition to the Necessary and Proper Clause, to require minimum open government procedures in the manner in which the advisory committee provides advice to the President on the qualification of judicial candidates under consideration for nomination by the President. The majority in *Public Citizen* recognized that applying FACA in this context, however, raised serious separation-of-powers questions, and, invoking the constitutional avoidance doctrine, ruled that Congress intended to have FACA apply only to advisory committees that were established or controlled by the Executive. *Id.* at 461. Accordingly, because the ABA committee was not established or controlled by the Executive, FACA did not apply in that case.

Justice Kennedy, however, joined by then-Chief Justice Rehnquist and Justice O'Connor, all concurring in the result,[15] found it necessary to reach the constitutional question, and stated that applying FACA to the manner in which the President obtains advice on potential nominees would violate the separation of powers:

> In some of our more recent cases involving the powers and prerogatives of the President, we have employed something of a balancing approach, asking whether the statute at issue prevents the President 'from accomplishing [his] constitutionally assigned functions' . . . . and whether the extent of the intrusion on the President's

[15] Justice Scalia recused himself from the case, apparently because he previously opined on the matter years earlier as Assistant Attorney for the Office of Legal Counsel, concluding that FACA, as applied to the ABA committee, did violate the separation of powers.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00265 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.212

> powers "is justified by an overriding need to promote objectives within the constitutional authority of Congress."

Id. at 484 (1989) (citing *Nixon v. Adm'r of General Services*). Applying FACA to the appointments process surely would not prevent the President from nominating whomever he chose to be a federal judge. Nevertheless, Justice Kennedy recognized that FACA's impairment of the exercise of even a small part of that presidential power -- namely, the ability to receive unfettered advice from the private sector in the aid of his appointment power -- was sufficient to disable the legislative branch from regulating the exercise of the President's power. *Id.* at 482-88. In the instant case, it cannot be seriously doubted that applying FISA to preclude the NSA Program would impair the execution of a core constitutional duty of the President to a much greater degree than would be the case of applying FACA to the ABA advisory committee.

Finally, in *Clinton v. Jones*, 520 U.S. 681 (1997), the Supreme Court reiterated that a violation of the separation of powers is measured by determining whether the action rises "to the level of constitutionally forbidden impairment of the Executive's ability to perform its constitutionally mandated functions." *Id.* at 702.

The constitutional power of the President to gather and share intelligence information also has been recognized by the prior Administration with regard to a statutory preclusion on the sharing of intelligence information gleaned from a criminal wiretap set up under Title III.[16] As aptly summarized in an Office of Legal Counsel Opinion:

> In extraordinary circumstances electronic surveillance conducted pursuant to Title III

[16] Precisely like FISA, Title III prescribes criminal penalties for violating its provisions. 18 U.S.C. § 2511.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00266 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.213

> may yield information of such importance to national security or foreign relations that the President's constitutional powers will permit disclosure of the information to the intelligence community notwithstanding the restrictions of Title III. . . . [T]he Constitution vests the President with responsibility over all matters within the executive branch that bear on national defense and foreign affairs, including, where necessary, the collection and dissemination of national security information. Because "[i]t is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation, ". . . the President has a powerful claim, under the Constitution, to receive information critical to the national security or foreign relations and to authorize its disclosure to the intelligence community. *Where the President's authority concerning national security or foreign relations is in tension with a statutory rather than a constitutional rule, the statute cannot displace the President's constitutional authority and should be read to be "subject to an implied exception in deference to such presidential powers." Rainbow Navigation, Inc. v. Department of the Navy*, 783 F.2d 1072, 1078 (D.C. Cir. 1986) (Scalia, J.). We believe that, if Title III limited the access of the President and his aides to information critical to national security or foreign relations, *it would be unconstitutional as applied in those circumstances.*

Sharing Title III Electronic Surveillance Material With the Intelligence Community, Op. Off. Legal Counsel, 2000 WL 33716983 at 9 (Oct. 17, 2000) (emphasis added) (internal citations omitted). And even the legislative history of FISA indicates that Congress recognized that its "exclusive" procedural mechanism for foreign electronic surveillance "does not foreclose a different decision by the Supreme Court." H.R. Conf. Rep. No. 95-1720, at 35, reprinted in U.S.C.C.A.N. 4048, 4064.

FISA, as Plaintiffs would have it apply, would severely impair the Executive "from accomplishing its constitutionally assigned function." Accordingly, amicus submits that, even if the merits of this case can be reached, it is FISA, as applied, and not the NSA Program, which violates the separation of powers.

CONCLUSION

While it is true, as Plaintiffs claim, that a "state of war is not a blank check for the President," *Hamdi v. Rumsfeld*, 542 U.S. 507, 536 (2004) (plurality op.), it is also true, as

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00267 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.214

Justice Jackson warned, that the courts should not "convert the constitutional Bill of Rights into a suicide pact." *Terminiello v. Chicago*, 337 U.S. 1, 36 (1949) (Jackson, J., dissenting). From the limited information available about the NSA Program, WLF submits that it is well within the President's constitutional authorities to carry out such limited electronic surveillance of suspected terrorists who would attack this Nation and kill its citizens. In any event, this Court cannot grant the Plaintiffs' Motion for Partial Summary Judgment without knowing the facts and circumstances of the NSA Program.

Respectfully submitted,

H. Bryan Cunningham
MORGAN & CUNNINGHAM LLC
Two Tamarac Center, Suite 425
7535 East Hampden Avenue
Denver, CO 80231
(303) 743-0003

Daniel J. Popeo
Paul D. Kamenar
WASHINGTON LEGAL FOUNDATION
2009 Massachusetts Ave., NW
Washington, DC 20046
(202) 588-0302

/s/
Timothy A. Valliere [TV 1198]
BUSHELL & VALLIERE LLP
60 E. 42d Street
Suite 2925
New York, NY 10165
(212) 949-4700
(Local Counsel)

Counsel for Amicus Curiae Washington Legal Foundation

Date: June 6, 2006

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00268 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.215

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

before the

Senate Judiciary Committee

"Modernization of the Foreign Intelligence Surveillance Act"

July 26, 2006

Chairman Specter, Ranking Member Leahy, Members of the Committee, 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 modernized already several times since 9/11, most notably in the recently reauthorized PATRIOT Act, and providers of digital communications services in the US have for some years been modifying their network to accommodate government surveillance.

The Chairman's bill as it stands today is not a modernizing bill. Rather, it would turn back the clock to an era of unchecked Presidential power, warrantless domestic surveillance, and constitutional uncertainty.

We commend Chairman Specter for his tireless leadership in seeking to ensure judicial review of this President's warrantless surveillance program. From the outset, the Chairman has criticized the Administration's disregard for FISA's express requirements. He has vigorously sought more information about the program, and he has held repeated hearings. The Chairman has worked across the aisle to draft legislation with Senator Feinstein. Now, through intense negotiations, the Chairman has secured the promise of the President to submit his current program to court review. With profound respect, we must conclude that the price the Chairman paid for that simple concession is far too high.

---

[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.

43453.216

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

Prior to this hearing, the Administration has made no showing on the public record that FISA is in need of further amendment, with the sole exception of the Attorney General's explanation of problems involving FISA's emergency exception, problems due in part to the paperwork burdens created by the Executive Branch and perpetuated by this Administration.

Perhaps at this hearing, the Administration's witnesses will describe further specific defects in FISA. If they do, we will endeavor to respond to them in our oral remarks, but, surely, any issues the Administration raises at this hearing will require further careful study. Certainly, if the Administration identifies any problems at this hearing (on Wednesday), it is too soon to expect that suitable responses to them can be drafted and understood by the next day (Thursday), when this Committee may again take up FISA-related legislation, or even by next week.

Congress can best modernize FISA – if it needs modernizing -- only after further hearings, building on public testimony 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.

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 Chairman's New Legislation Would Not Modernize FISA – It 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 Chairman's Bill Would Not Guarantee Judicial Review of Future Surveillance Programs Affecting Americans

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

First, it is not clear that any legislation is necessary to get the President's program reviewed, since the program is already the subject of 30 pending cases. In the lead case, the district court last week turned aside a government effort to dismiss the case and is headed towards consideration of the merits.[2]

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 the Chairman's bill might fail to give the FISA court jurisdiction to review the President's program:

---

[2] More than thirty cases challenging the Administration's warrantless surveillance program are now pending, including challenges filed by criminal defendants who may have been targeted. Several federal judges have already heard arguments about the legality of the surveillance. (Many of the cases are stayed in order to resolve issues associated with "multi-district litigation.") These cases cover not only the Administration's limited admissions about the program, but also evidence that the Administration, aided by AT&T and likely other telecommunications companies, has been conducting wholesale surveillance on the communications and communications records of millions of Americans for four years.

Indeed, three U.S. district court judges have already considered the Administration's national security arguments, complete with secret evidence: Judge Vaughn Walker in San Francisco; Judge Anna Diggs Taylor in Detroit; and Judge Matthew Kennelly in Chicago. Judge Walker recently rejected the government's assertion of the "state secrets privilege," setting up that case for further proceedings on the merits.

- The President has said that his program only allows short term monitoring, but the Chairman'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 the Chairman's bill applies *only* when it is not possible to specify who is being targeted.

Even assuming that the Chairman's bill would allow the FISA court to review the President's program, in other key ways the bill undermines judicial review by forcing transfer to the Foreign Intelligence Surveillance Court of Review (FISCR) of any case initiated by a citizen challenging a communications intelligence activity of the government. In these cases, the government would have the benefit not only of all its normal procedural grounds for seeking dismissal of a case but also of the largely ex parte and in camera processes of the FISCR, making it virtually impossible for parties challenging the government program to overcome the evidentiary burdens they would face.

Finally, the Chairman's 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.

The Price Is Too High – Turning the Clock Back to an Era of Unchecked Presidential Power and Warrantless Domestic Surveillance

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 the Chairman's amendments, merely optional; the repeal 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 the Chairman'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, the Chairman'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 the Chairman'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, the substitute 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 the Chairman's bill, the substitute does not require the Administration to submit the President's warrantless surveillance program or any future program for judicial review.

The Chairman'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 9 of the Chairman'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."[3]

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 standards tested over time and insulated from the pressures of the moment. . . .[4]

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.

Section 9 – Total Information Awareness on Steroids?

To cinch the deal with the White House, the Chairman has added to his bill a new Section 9, which would vastly expand the scope of warrantless surveillance that never has

---

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

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

to be submitted to a court and create a vast database of phone calls and other information reminiscent of the Total Information Awareness program, which the Administration could data mine at will, outside any judicial or congressional oversight.

Probably 30% of the meaning of FISA is buried in its definitions, especially its definition of "electronic surveillance" and "minimization procedures." Sugar-coated as "conforming amendments," the changes made by Section 9 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.

The "cut and bite" amendments of Section 9 are very hard to parse, but so far, we have identified the following remarkable provisions:

- The bill makes major changes to FISA's 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 outside the definition of electronic surveillance, then it is not covered by the Act, and can be carried on without a warrant. Therefore, narrowing the definition of electronic surveillance places more activity outside the oversight of the Act. Section 9 makes major changes to the definition of electronic surveillance, permitting the NSA's vacuum cleaners to be turned on any international calls involving US citizens.

- In what may be the most far-reaching provision, Section 9 amends section 102 of FISA (50 USC 1802) to allow the "Attorney General" to authorize warrantless surveillance if it is "solely directed at the acquisition of the communications of a foreign power or agent of a foreign power." Under this amendment, so long as the surveillance is "directed at" a foreign power or non-US person suspected of being an agent of a foreign power, the government can intercept the purely domestic calls of US citizens without court order.

- Under the bill, if he chooses, the Attorney General can designate anyone – his secretary, the janitor, an official of the department of Defense, a local police officer, as "Attorney General", thereby authorized to approve warrantless surveillance under section 102, to issue certifications to communications companies and others, and to carry out all the other duties assigned to the Attorney General under the Act.

- The bill amends the definition of a non-US person agent of a foreign power to include someone who "possesses or is expected to transmit or receiving foreign intelligence while in the" US.

The Specter- Feinstein Bill Is the Correct 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;
- 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.

Despite the lack of any publicly articulated rationale, the bill the Chairman negotiated with the Administration would cast aside all five of these principles.

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.[5]

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 Modernized

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.[6]

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:

---

[5] 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.

[6] 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 ... .[7]

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.

---

[7] 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.

Technology Can Support Particularity

It has been suggested that it is difficult or impossible for the government to isolate the communications of specific targets in networks using packet switching rather than circuit switching technology. However, partly as a result of the Communications Assistance for Law Enforcement Act of 1994 (CALEA), a number of companies are offering technology to isolate packet communications for government surveillance. One company, for example, notes that its surveillance technology for broadband Internet service providers and ISPs "is highly flexible, utilizing either passive probes or active software functionality within the network nodes to filter out traffic of interest."[8] Cisco recently released its "Service Independent Intercept Architecture," which uses existing network elements and offers an "integrated approach that limits the intercept activity to the router or gateway that is handling the target's IP traffic and only activates an intercept when the target is accessing the network." http://www.cisco.com/technologies/SII/SII.pdf VeriSign is another company offering comprehensive services for interception:

> VeriSign operates as a Trusted Third Party (TTP) assisting service providers in meeting the legal, technical and operational requirements for lawful assistance and legal interception as required by the Communications Assistance for Law Enforcement Act (CALEA). VeriSign NetDiscovery Service is a managed service provides a reliable, end-to-end solution that can help accomplish compliance quickly on traditional and packet-based network deployments.[9]

CALEA, it should be noted, requires service providers in the United States to have the technological ability to isolate the communications of a surveillance target to the exclusion of the communications of all other users of the network. It must be emphasized

---

[8] VERINT Systems, Inc., STAR-GATE for Broadband Data and ISP, http://www.verint.com/lawful_interception/gen_ar2a_view.cfm?article_level2_category_id=7&article_level2a_id=59

[9] http://www.verisign.com/products-services/communications-services/connectivity-and-interoperability-services/calea-compliance/index.html

that FISA only applies to surveillance inside the United States, where the intelligence agencies have the willing and court-ordered cooperation of service providers. The vacuum cleaner approach is sometimes necessary overseas because the intelligence agencies do not have the cooperation of local service providers. The vacuum cleaner, let alone being unconstitutional, is not necessary inside the US. It is also noteworthy that the FBI reports that it does not have to use its notorious Carnivore, or DCS 1000, which was intended to isolate targeted IP communications, because commercially available software is able to do the job. [10]

Technology is not a substitute for sound policy. In this case, however, the trend of technology seems to favor, not excuse, particularity.

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 Committee, we urge you to look on this as a process that will take some care. The Administration should engage in a debate on the public record, and 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.

[10] http://www.epic.org/privacy/carnivore/2003_report.pdf.

Testimony of Mary B. DeRosa

Senior Fellow, Center for Strategic and International Studies

Before the

Committee on the Judiciary, United States Senate

July 26, 2006

Mr. Chairman, Senator Leahy, and members of the Committee, thank you for the opportunity to testify on the subject of the Foreign Intelligence Surveillance Act (FISA) in the 21st Century.

I am a Senior Fellow at the Center for Strategic and International Studies (CSIS). Before coming to CSIS, I was the Legal Adviser at the National Security Council and, earlier, I was a lawyer in the General Counsel's office of the Department of Defense. Through both of those experiences I came to appreciate not only the great value of electronic surveillance for national security, but also the need for flexible tools and authorities for conducting surveillance. Particularly with the threat from terrorists who operate all over the world, including within our borders, national security professionals must be able to act nimbly and to leverage the most advanced technological tools to collect intelligence.

Electronic surveillance – intercepting people's private communications – is also one of the most invasive tools that the government can use. When the government conducts this surveillance within our borders it must be done in a manner that protects civil liberties and, critically, in a way that the public accepts as legitimate. The experts in the Executive Branch and Congress who crafted FISA in the late 1970s concluded that the critical mechanism for ensuring public acceptance of national security electronic surveillance at home was to create a process that ensured careful court oversight of surveillance decisions, and to make that process exclusive. That was an extraordinarily wise judgment. The government can act most effectively to protect national security when it has all of us behind it in this critical task; this is harder if it is lurching from controversy to controversy, trying to explain and defend its actions. Court oversight of surveillance decisions enhances public trust and it must remain at the core of any discussion of FISA in the 21st Century.

I have two other observations before discussing in greater detail some possible updates to FISA and existing legislative proposals. First, FISA is actually more flexible than many people give it credit for. It is certainly not a model of clarity – its language is dense almost to the point of being unreadable (an area where improvement would be welcome, as I will discuss). But those who have interpreted and applied FISA through the years know it has been flexible enough to adapt to many changes in technology and threat. In

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00282 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.229

addition, the showing required to receive a surveillance order – probable cause that a person is an agent of a foreign power or terrorist group – is not particularly rigorous and a number of tools exist – pen registers, trap and trace devices, and National Security Letters, for example – that permit those seeking a warrant to develop the evidence they need to meet the probable cause requirement. The FBI has not found itself "paralyzed" in attempting to pursue possible connections to terrorism, as some have suggested. Many of the hurdles that national security professionals do encounter in seeking FISA warrants are due to burdensome administration, misunderstanding, or conflicting interpretations of the law. This is a problem, surely, and FISA is far from perfect, but it is important to clear away the hyperbole and misunderstanding and look at what truly needs fixing.

A related observation is that to make informed revisions to FISA, Congress must hear from the Executive Branch about the ways in which FISA is inadequate or overly burdensome. Congress can not be expected to guess at what about FISA is broken; the consequences of making a mistake are too high. Certainly with an issue this important Congress can not be expected simply to accept the Executive Branch's proposals for change, without an explanation of why they are needed. Congress must be able to evaluate itself the need for change and to balance competing priorities.

With the remainder of my testimony I will first discuss some ways in which FISA might be improved. Finally, I will comment specifically on some aspects of the current draft of S.2453, which the Chairman has introduced in this Committee.

Improving FISA

I discuss here a number of potential areas for improvement to FISA. For some of these areas, there is sufficient information already from the Executive Branch about the problems that exist to craft informed legislation. For others, more information from the Executive Branch would be necessary before any useful legislation is possible.

Streamline FISA Procedures

The most consistent complaint about FISA from those who must use it is that the administrative requirements for seeking a warrant make the process unduly difficult and time-consuming. People speak of burdensome paperwork and significant delays in the Justice Department approval process. Applications can be put on a fast track if they are urgent, but this is an ad hoc and unsatisfactory process. In addition, FISA's emergency provision permits the conduct of surveillance for 72 hours before seeking a warrant, but procedures within the Executive Branch for exercising this option are also burdensome. In any event, it is bad governance at best if the government must invoke an emergency procedure because its own bureaucracy is too stifling.

It is not clear that these bureaucratic problems are due to the language of FISA itself; many can be attributed to Executive Branch procedures that have developed over time. The Executive Branch has the responsibility to improve its own procedures if it finds

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00283 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.230

them to be an impediment to national security. But in this case, where there is plenty of evidence of a problem, Congress can and should act to improve the situation.

Several pieces of proposed legislation would address this problem. S.3001, introduced in this Committee, would streamline the approval process by, among other things, requiring development of a secure electronic system for submitting and approving applications, and authorizes adding personnel at the Justice Department Office of Intelligence Policy and Review (OIPR), the office responsible for shepherding the FISA approval process. The draft legislation also would add flexibility to FISA's emergency procedures. In the House, H.R.5371, the LISTEN Act, would also authorize increased resources to process FISA applications to ensure more timely and efficient processing. Of the provisions in these drafts, the requirement to develop a secure electronic system for submitting applications is the most promising because it would force the Executive Branch to refine and modernize its approval process. By all accounts the current process needs thorough reform, not just more resources.

Reaffirm FISA's Exclusivity

National security surveillance decisions must receive disciplined, transparent oversight from a court. Public acceptance of domestic electronic surveillance requires clarity about the manner in which that surveillance is authorized and overseen. Oversight by the judicial branch, although not always easy, is a critical check on the Executive Branch when it employs such an intrusive tool. The language and legislative history of FISA leave no doubt that it was intended to be the exclusive avenue for conducting national security electronic surveillance of domestic communications (that is, at least one party is located within the United States). The Bush Administration's conduct and legal defense of the controversial NSA surveillance program – which targets communications in which one party is located in the United States – has challenged that exclusivity. The Administration concedes that the program involves communications that FISA's terms cover, but says it may proceed outside of the FISA scheme because of the President's authority as Commander in Chief. If Congress does not act to reaffirm FISA's exclusivity, there is a danger that this and later administrations will assert that Congress has acquiesced in the Administration's legal theory. There might then be many surveillance programs that do not receive oversight by the Foreign Intelligence Surveillance Court (FISC) or any other court.

To say judicial oversight is critical does not mean that the Executive Branch and its employees are untrustworthy. In fact, the people carrying out national security electronic surveillance, on the whole, care a great deal about protecting privacy and have absolutely no interest in violating civil liberties. The problem is human nature: because protecting national security is potentially in tension with protecting individual liberties, it is unrealistic to ask one person to balance both goals and check their own behavior. The national security agencies and their employees are charged with protecting the United States from harm. When faced with a decision about whether to take a step that invades liberties they will not always be able to judge whether it is the only way or the best way to address a problem – or whether it is simply the easiest way. If they fear that failure to

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00284 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.231

take action might cause people to die, their instinct will be to push as far as they can push. We want them to have this instinct, but when it comes to something as intrusive as electronic surveillance, we also need someone else to balance other interests and draw clear lines. With national security electronic surveillance, FISA provides those lines, and FISC oversight enforces them. If there are no lines and there is no FISC oversight, the instinct of national security employees to push to the line in order to protect becomes a threat to our nation, rather than the comfort that it should be.

That is the reason FISA's drafters determined that its mechanism, including oversight by the FISC, should be the exclusive route for the exercise of the President's authority to conduct electronic surveillance. Congress has this power. The President has authority in the national security area to conduct electronic surveillance without a criminal warrant, but that authority is not exclusive. Congress has constitutional authorities in the national security area and it may pass laws that regulate the exercise of the President's powers. Congress did this with FISA – it permitted the President to exercise his authority, but provided the exclusive mechanism for him to use. In the face of the Bush Administration's legal arguments, Congress should reaffirm that the FISA scheme is exclusive so there can be no question that the carefully constructed oversight scheme is the only route available for electronic surveillance programs that FISA, by its terms, covers.

Some proposed legislation would reaffirm FISA's exclusivity. S.3001 and the LISTEN Act (H.R.5371) reiterate the exclusivity provisions of FISA. S.3001 also would prohibit the use of funds for electronic surveillance except in accordance with FISA or the criminal wiretap provisions. As I will discuss in greater detail later, S.2453, in its most recent form, would move in the opposite direction; it not only fails to reaffirm exclusivity, but in fact explicitly rejects it.

Clarify Certain FISA Provisions

As I have mentioned, FISA is a very dense and often confusing piece of legislation. Clarifying some aspects of the law would be helpful to the Executive Branch in carrying out its responsibilities. For example, there appears to be some confusion about whether a communication that is entirely foreign – that is, made between parties all of whom are located overseas – may still become subject to FISA's requirements if it passes through a communications node located in the United States. It is my understanding that intercepting this type of communication would not be "electronic surveillance" subject to FISA's provisions because it does not involve targeting a communication to or from at least one person who is located in the United States. If there is confusion about this point that causes the Executive Branch difficulty in carrying out its surveillance activities, the legislation should be clarified.

Similarly, FISA could be clearer about the treatment of "metadata." There is an important difference in the degree of intrusiveness between interception of the actual content – spoken or written words – of a communication and interception of the "metadata" or descriptive information about that communication. Metadata might

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00285 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.232

include information like identity or location of the parties and the time and duration of the call. Most laws reflect the difference in intrusiveness by placing less stringent controls on government access to metadata. Treatment of metadata under FISA, however, is somewhat confused. FISA contains sections on the use of "pen registers" and "trap and trace" devices – which collect "to" and "from" information about communications – that permits use of these tools with fewer controls than the collection of content. FISA's definition of "contents" of a communication, however, includes not only the "substance, purport, or meaning" but also the "identity of the parties to" or "the existence" of that communication. These latter categories are usually considered metadata, not content. This definition could be read to apply to a fairly broad range of metadata – even information like a phone number can be used to identify a party. Metadata about communications can have very significant intelligence value and is becoming increasingly important with the growing sophistication of tools to analyze communications "traffic." FISA should be as clear as possible about the distinction between content and metadata and the protections afforded each type of data. S.2453 would clarify this matter.

There may be other areas where confusion about legal direction runs the risk of interfering with effective action pursuant to FISA. If so, the Executive Branch should identify problems to Congress so that it can act to correct them.

Consider Adaptations to Address Changing Technology, Including Programmatic Approvals

In the almost 30 years since FISA became law, communications technology has changed radically. Perhaps the most significant change for purposes of electronic surveillance is the move from circuit-based to packet-based communications technology. Increasingly, interception of communications does not involve "tapping" a dedicated line as it did when FISA was drafted, but instead requires sifting through and connecting discrete packets of information that together make up an electronic or voice communication. As I mentioned earlier, FISA's provisions actually have been far more flexible than many would suggest. FISA is adequate to the current task of electronic surveillance, but it almost certainly is not optimal. A careful review by Congress of FISA's definitions and requirements, informed by Administration input, could result in useful changes to make FISA even more adaptable.

One particular change to adapt to technology that has been proposed is a move to permit FISC approval of programs of surveillance in addition to individual warrants. I believe this is an area where revisions might well be appropriate. On this subject, however, far more information is needed from Executive Branch operators about what they need and why before Congress can legislate responsibly.

FISA's procedures were designed generally to authorize electronic surveillance on individual targets that have been identified through other means as foreign powers, terrorists, or their agents. But increasingly, analysts seek to use transactional data involving large numbers of people, including communications metadata or even content,

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00286 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.233

to help with the job of identifying the terrorists in the first place. Using automated programs that employ algorithms (often referred to as "data mining"), analysts will seek to detect links between subjects or patterns of activity that will help unmask terrorists who might then be the subject of individual surveillance. Although the current FISA procedures are flexible, it is fair to say that they were not designed for this use of surveillance. This issue has been raised in discussions of the NSA domestic surveillance program, although it is not clear from public descriptions of that program what type of analysis it involves.

One thing that is crucial in any discussion of programmatic approvals under FISA is how the FISC would authorize and oversee those programs. The need for careful Court oversight is at least as great with this type of surveillance. I believe any authority for advance approval of programs must provide a standard for review that is something akin to probable cause and require the FISC to evaluate the purpose of the program and the basis for concluding that it will collect foreign intelligence. The court should take into consideration in its review what type of analysis will be used, how intrusive it is and its level of accuracy; what data is involved; procedures that will be used to protect privacy, such as the use of anonymization or other technology; procedures for dissemination and use of the information obtained; and what auditing and other techniques will be employed to assure compliance with guidelines. The authority would also have to provide for regular court oversight of the programs.

Comments on S.2453

The legislation that the Chairman has introduced after discussions with the White House is an attempt to create a route for obtaining judicial review of the controversial NSA surveillance program, while permitting FISC approval of surveillance programs and addressing some of the Administration's concerns about FISA as it is currently written. I agree that judicial review of the NSA program is a high priority, but I have some serious concerns with this proposed legislation.

Would Make the FISA Process Optional

As I have said, it is my view that FISA's carefully constructed oversight scheme must be the only route available for the national security electronic surveillance that FISA addresses. Therefore, my most significant concern with S.2453 is that it would make FISA optional. Section 9 of S.2453 reads: "Nothing in the Act shall be construed to limit the constitutional authority of the President to collect intelligence with respect to foreign powers and agents of foreign powers." That section also repeals the provisions that now make FISA exclusive. This is a dramatic rejection of the judgment of FISA's drafters that FISC oversight is crucial to protection of civil liberties and maintenance of public trust in the conduct of electronic surveillance for national security.

Congress has the authority to make FISA the exclusive process for conducting national security electronic surveillance in the United States, even if the President has

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00287 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.234

constitutional authority in this area. A long line of separation of powers analysis, beginning with Justice Jackson's concurrence in *Youngstown Sheet & Tube Co. v. Sawyer*, makes it clear that Congress may limit or regulate the President's exercise of his constitutional authority. In Youngstown, Justice Jackson stated:

> When the President takes measures incompatible with the express or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter. Courts can sustain exclusive executive Presidential control in such case only by disabling the Congress from acting upon the subject.

As recently as last month, in the *Hamden v. Rumsfeld* case, the Supreme Court has reaffirmed this line of analysis. In *Hamden*'s footnote 23 the Court cites *Youngstown* and explains:

> 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.* (Emphasis added.)

There is little question that Congress has its own powers in this area. Indeed, the "Findings" section of S.2453, Section 2(9), lists and describes those powers. Therefore, by regulating the President's exercise of surveillance power with FISA and directing that the process be exclusive, Congress placed the President's independent authority at its "lowest ebb." The provision in S.2453 that recognizes and specifically declines to limit the President's authority lifts those powers from their "lowest ebb" and provides the President the option to choose avenues for national security electronic surveillance at home that will not involve any court oversight.

Would Limit, and Distort the Outcome of, Judicial Review

A second problem with S.2453 concerns the quality of the judicial review it would provide. Although I agree that it is important to obtain a judicial determination of the constitutionality of the controversial NSA surveillance program that has been disclosed publicly, this legislation would actually cut off several promising avenues for that review. The proposal gives the FISC authority to review and approve an "electronic surveillance program," which presumably would include the NSA program in question. It does not require the Executive Branch to submit any program for approval. The White House has committed to submit the current NSA program to the FISC, but for other programs created under the authority of this legislation, review would be optional. While providing this optional avenue, the bill would cut off review by other federal courts requiring a transfer of any such cases to the Foreign Intelligence Surveillance Court of Review if the Executive Branch requests it. This would affect the several cases currently under consideration in federal district courts. Moreover, the Foreign Intelligence Surveillance

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00288 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.235

Court of Review, or any other federal court hearing such a case, is permitted to dismiss a legal challenge to a surveillance program "for any reason."

The Legislation also would increase significantly the Administration's chances of prevailing in any review that does occur by changing the relative positions of the Executive and Legislative Branches in a separation of powers analysis. For the reasons discussed in the previous section, the provision in S.2453 recognizing and specifically declining to limit the President's authority would be read by a court as an expression by Congress that it supports, or at the least is silent on, the President's pursuit of this program outside of the FISA scheme. The exclusivity provisions of FISA as currently written, on the other hand, would be seen specifically to prohibit this independent route. The expression of Congress's will is a critical aspect of separation of powers analysis under *Youngstown* and its progeny.

Would Allow for Program Approvals with Little Review or Oversight

Sections 5 and 6 of S.2453 would permit applications for and approval of electronic surveillance programs. Although, as I stated earlier, I believe permitting programmatic approvals could be a useful innovation, these sections as written would not provide the kinds of protections that would be essential with this type of change. First, Congress must have more information from the Executive Branch before it can legislate in this area. In the absence of a clear understanding of what the operators feel they need and why, Congress is left to guess, or simply to accept general statements from the Administration about the authority it believes it needs. Neither is acceptable in an area this sensitive. Programs of surveillance have the potential to be extraordinarily intrusive and Congress has a responsibility to consider carefully and balance the benefit to security and the potential for harm. Second, the provisions are overly general, allowing approvals based only on a showing that the program is "reasonably designed" to lead to a broad category of communications. Finally, the legislation does not provide for the kind of careful oversight by the FISC of the ongoing conduct of the program that I believe is essential.

Would Loosen Many Existing Protections in FISA

Other aspects of S.2453 would create exceptions, change definitions, and lower standards in a way that, taken together, would significantly reduce the protections that FISA affords. Although I have not had the opportunity to do a thorough analysis of the proposal's many provisions, I will mention a few about which I have particular concerns. The expansion of the definition of non-U.S. person agent of a foreign power (section 10(b)(1)) to include an individual who "otherwise possesses or is expected to transmit or receive foreign intelligence information while in the United States" could permit surveillance of a considerably broader range of individuals under FISA than is now possible. The redraft of FISA's section 102, which permits surveillance without application to the FISC, would increase the types of communications that are exempted from court review under this authority. And the expansion of the time limit for all

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00289 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.236

surveillance orders to 1 year would reduce FISC participation and could allow surveillance well past when it is providing useful intelligence.

Conclusion

I am grateful to the Committee for giving me the opportunity to provide my views on FISA and efforts to modernize that legislation to meet 21st Century requirements.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00290 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.237

Testimony to the Judiciary Committee of the US Senate
By General Michael V. Hayden,
Director, CIA

26 July 2006

Mister Chairman, Senator Leahy, thank you for the opportunity to speak before your committee today. The work that you and we have before us is truly important: how do we best balance our security and our liberty in the pursuit of legitimate foreign intelligence. Let me congratulate the Committee for taking on the task of examining and—where appropriate—amending the Foreign Intelligence Surveillance Act.

This task of balancing liberty and security is one that those of us in the intelligence community take very seriously and one to which we constantly turn our attention.

I recall that within days of the 9-11 attacks I addressed the NSA workforce to lay out our mission in a new environment. It was a short video talk beamed throughout our headquarters at Fort Meade and globally. Most of what I said was what anyone would expect. I tried to inspire. Our work was important and the Nation was relying on us. I tried to comfort. Look on the bright side: right now a quarter billion Americans wished they had your job. I ended the talk by trying to give perspective. All free peoples have had to balance the demands of liberty with the demands of security. Historically we Americans had planted our flag well down the spectrum toward liberty. Here was our challenge. "We were going to keep America free," I said, "by making Americans feel safe again."

This was not an easy challenge. The Joint Inquiry Commission (comprised of the House and Senate Intelligence Committees) would summarize our shortcomings in the months and years leading to the September 11th attacks. The Commission harshly criticized our ability to link things happening in the United States with things that were happening elsewhere.

Let me note some of JIC's Systemic Findings (Joint HPSCI-SSCI, from abridged findings and conclusions)

43453.238

"...NSA's cautious approach to any collection of intelligence relating to activities in the United States" (finding 7)

"There were also gaps in NSA's coverage of foreign communications and the FBI's coverage of domestic communications" (Finding 1, p 36, tab 4)

"...NSA did not want to be perceived as targeting individuals in the United States." (Finding 1, p 36, tab 4)

"[in talking about one end US conversations]...there was insufficient focus on what many would have thought was among the most critically important kinds of terrorist related communications, at least in terms of protecting the homeland." (Finding 1, p. 36, tab 4)

For NSA the challenge was especially acute. NSA intercepts communications and it does so for only one purpose: to protect the lives, the liberties and the well being of the citizens of the United States from those who would do us harm. By the late 1990s, that job was becoming very difficult. The explosion of modern communications in terms of its volume, variety and velocity threatened to overwhelm the Agency.

The September 11th attacks exposed an even more critical fault line. The laws of the United States do (and should) distinguish between the information space that is America and the rest of the planet.

But modern telecommunications do not so cleanly respect that geographic distinction. We exist on a unitary, integrated, global telecommunications grid in which geography is an increasingly irrelevant factor. What does "place" mean when one is traversing the World Wide Web? There are no area codes on the Internet.

And if modern telecommunications muted the distinctions of geography, our enemy seemed to want to end the distinction altogether. After all, he killed 3000 of our countrymen from within the homeland.

In terms of both technology and the character of our enemy, "in" America and "of" America no longer were synonymous.

43453.239

I testified about this challenge in open session to the House Intelligence Committee in April of the year 2000. At the time I created some looks of disbelief when I said that if Usama bin Ladin crossed the bridge from Niagara Falls, Ontario to Niagara Falls, New York, there were provisions of US law that would kick in, offer him some protections and affect how NSA could now cover him. At the time I was just using this as a stark hypothetical. Seventeen months later this was about life and death.

The legal regime under which NSA was operating—the Foreign Intelligence Surveillance Act—had been crafted to protect American liberty and American security.

But the revolution in telecommunications technology has extended the actual impact of the FISA regime far beyond what Congress could ever have anticipated in 1978. And I don't think that anyone could make the claim that the FISA statute was optimized to deal with a 9/11 or to deal with a lethal enemy who likely already had combatants inside the United States.

Because of the wording of the statute, the government looks to four factors in assessing whether or not a court order was required before NSA can lawfully intercept a communication: who was the target, where was the target, how did we intercept the communication, and where did we intercept the communication.

The bill before the committee today effectively re-examines the relevance of each of these factors and the criteria we want to use with each.

Who is the target?

The FISA regime from 1978 onward focused on specific court orders, against individual targets, individually justified and individually documented. This was well suited to stable, foreign entities on which we wanted to focus for extended period of time for foreign intelligence purposes. It is less well suited to provide the agility to detect and prevent attacks against the homeland.

43453.240

In short, its careful, individualized processes exacted little cost when the goal was long term and exhaustive intelligence coverage against a known and recognizable agent of a foreign power. The costs were different when the objective was to detect and prevent attacks, when we are in *hot pursuit* of communications entering or leaving the United States involving *someone associated with al Qa'ida.*

In this regard, extending the period for emergency FISA's to seven days and allowing the Attorney General to delegate his authority to grant emergency orders is also very welcome and appropriate.

Where is the target?

As I said earlier, geography is becoming less relevant. In the age of the Internet and a global communications grid that routes communications by the cheapest available bandwidth available each nanosecond, should our statutes presume that all communications that touch America should be equally protected?

As the Chairman noted earlier this week, we do not limit our liberties by exempting from FISA's jurisdiction communications between two persons overseas that gets routed through US facilities.

Our limited government resources should focus on protecting US persons, not those entities who get covered as a result of technological changes that extend the impact—and protection—of FISA far beyond what its drafters intended.

I know that Senator DeWine among others has been very concerned about allocations of these resources and FISA backlogs. As Director of CIA I share his concerns in allocating my resources and hope that this legislation will help properly focus resources on protecting the legitimate privacy rights of US persons.

How did we intercept the communication?

For reasons that seemed sound at the time, current statute makes a distinction between collection "on a wire" and collection out of the air. When the law was passed, almost all local calls were on a wire and

43453.241

almost all long haul communications were in the air. In an age of cell phones and fiber optic cables, that has been reversed...with powerful and unintended consequences for how NSA can lawful acquire a signal. Legislators in1978 should not have been expected to predict the future of global telecommunications. Neither should you. The statute should be technology neutral.

Where we intercept the communication?

A single communication can transit the world even if the communicants are only a few miles apart. And in that transit NSA may have multiple opportunities to intercept it as it moves and changes medium. As long as a communication is otherwise lawfully targeted, we should be indifferent to where the intercept is achieved. Signals intelligence is a difficult art and science, especially in today's telecommunication universe. Intercept of a particular communication—one that would help protect the homeland, for example—is always probabilistic, not deterministic. No coverage is guaranteed. We need to be able to use all the technological tools we have.

In that light, there are no communications more important to the safety of the Homeland than those affiliated with al Qa'ida with one end in the United States. And so why should our laws make it more difficult to target the al Qa'ida communications that are most important to us—those entering or leaving the United States!

Because of the nature of global communications, we are playing with a tremendous home field advantage and we need to exploit this edge. We also need to protect this edge and those who provide it. The legislative language requiring compulsory compliance from carriers is an important step in this regard.

After 9/11, patriotic Americans assisted the Intelligence Community in ensuring that we have not had another attack on our soil since that awful day. And prior to 9/11, we received critical assistance across the IC from private entities. As Director of NSA, Deputy DNI, and now Director of the CIA, I understand that government cannot do everything. At times, we need assistance from outside the government.

43453.242

Whatever legal differences and debates may occur about separation of powers, Article 2, and so on, those people who provide help to protect America should not suffer as a part of this debate. I would urge the committee to recognize the importance of the efforts of these Americans and provide appropriate protection.

One final—and very important—point. Many of the steps contained in the proposed legislation will address the issue raised by the Congress' Joint Inquiry Commission: one end US conversations, communications that the JIC characterized as "among the most critically important kinds of terrorist related communications, at least in terms of protecting the homeland."

That means NSA will bump up against information to, from or about US persons. Let me stress that NSA routinely deals with this challenge and knows how to do this while protecting US privacy. The draft bill contains quite a bit of language about minimization—the process NSA uses to protect US identities. The same rules of minimization that NSA uses globally, rules approved by the Attorney General and thoroughly briefed to Congress, will be used.

Let me close by saying that we have a great opportunity here today. We can meet the original intent of the FISA Act to protect our liberty and our security by making the legislation relevant to both the technologies and the enemies we face.

Thank you.

43453.243

from the office of

Senator Edward M. Kennedy

of Massachusetts

FOR IMMEDIATE RELEASE
July 26, 2006

CONTACT: Laura Capps/Melissa Wagoner
(202) 224-2633

STATEMENT BY SENATOR EDWARD M. KENNEDY ON FISA MODERNIZATION

(AS PREPARED FOR DELIVERY BEFORE JUDICIARY COMMITTEE)

I regret that the Committee is now moving forward on legislation -- when we continue to tip toe around a serious investigation of the Administration's massive electronic surveillance program being conducted by the National Security Agency. Only four Members of the Judiciary Committee sit on the Intelligence Committee. Perhaps they know more, but the rest of us are legislating in the dark.

When it comes to national security, our country is far stronger when all of us stand united. Across party lines, we all agree on the need for law enforcement and intelligence officers to have strong powers to investigate terrorism, to prevent future attacks, and improve information-sharing between federal, state and local law enforcement. Cooperation between the Administration and Congress is fundamental to our national security, and we should all come together to meet our obligations to protect the safety and security of the United States.

There is a way to fight terrorism within the framework of the Constitution. Thirty years ago, when the Cold War still threatened us, a Republican Administration and a Democratic Congress worked together to enact the Foreign Intelligence Surveillance Act, giving broad authority to the government in cases involving national security.

Then, as now, the debate was driven by public disclosures of widespread surveillance by the National Security Agency. Then, as now, there was discussion over the proper scope of the President's authority.

But then, unlike now, the President decided to work with Congress to obtain clear authority for a wiretapping program. Since the enactment of that law in 1978, the rules have been clear. The conference report states plainly that Congress was setting forth a standard for all future Presidents to follow. It established the "exclusive means" by which, such surveillance could be conducted on U.S. soil.

The law's purpose has always been clear – to put an end to unsupervised wiretapping under the blanket claim of "national security." The Act was also intended to ensure that the

43453.244

Executive Branch – under any President – would not ignore basic civil liberties of the American people by claiming an unchecked "inherent power" to eavesdrop on conversations on U.S. soil.

The Authorization for Use of Military Force passed by Congress after September 11th did not authorize domestic electronic surveillance, and certainly did not authorize domestic electronic surveillance of American citizens without a judicially approved warrant. Congress has never authorized and never approved domestic electronic surveillance of United States citizens without a warrant.

Like the Intelligence Committee, the Judiciary Committee has its own important oversight role. When we began drafting the Foreign Intelligence Surveillance Act in 1976, both Committees held hearings and we had ongoing discussions with the Administration, and the legislation enacted in 1978 has been a success by any standard.

For the past 26 years, the Foreign Intelligence Surveillance Act has provided the "exclusive means" for domestic surveillance by the Administration. Yet the Chairman's bill would repeal the existing statutory scheme – and give the President an unprecedented "blank check." The White House is thumbing its nose at the role of Congress – and ignoring the recent clear rebukes by the Supreme Court.

Section 8 of this proposal states categorically that, "Nothing in this Act shall be construed to limit the constitutional authority of the President to collect intelligence with respect to foreign powers and agents of foreign powers." This section has only one purpose – to codify the breathtakingly broad and erroneous view of executive power asserted by the Bush Administration and rejected by the Supreme Court. The bill that we have is labeled "Discussion Draft," but the Chairman has already announced that the White House does not want any discussion – much less any changes to this so-called compromise.

This sham proposal allows the President alone to decide whether he will permit a court to review the legality of his electronic surveillance activities. For the first time, these sweeping programs of domestic surveillance would be subject to court review only if the President agrees voluntarily to have a court conduct such a review. The bill also allows the President to authorize entire programs of surveillance – not just applications for individual warrants.

The American Bar Association minces no words. It calls this White House bill an "enormous and unwarranted departure" from existing law! It ignores the requirements of the Fourth Amendment – which require probable cause and individualized suspicion before the government can monitor communications. It even allows the government to transfer any case challenging the legality of its surveillance program to the secret FISA court, where the government can then seek dismissal of the case for any reason. Under this proposal, the President can go to a court that permits only government lawyers to appear before it, and obtain a secret -- blanket -- endorsement of his surveillance program.

It's obvious our Congressional oversight so far hasn't been effective in guaranteeing that the constitutional checks and balances on executive power are working. All we've received are

43453.245

after-the-fact legal rationalizations for the program. If the Committee stops having hearings an stops carrying out its investigative and oversight functions, then we are abandoning our own oa to protect and defend the Constitution. Instead of fulfilling our long-standing role as a constitutional watch-dog, we become a presidential lap-dog.

Americans deserve national security laws that protect both our security and our constitutional rights. The 9/11 Commissioners got it right. Our goal should be to adopt governmental powers that genuinely enhance our national security while maintaining adequate oversight over their use. If our current national security laws are inadequate, the Administratio should work with both Republicans and Democrats Members in Congress to update our laws with due regard for our Constitution, treaties, and the laws of war. The Bush Administration, however, is asking us not only to write legislation – it wants us to override the constitutional checks and balances that are at the core of our democracy, and we should not yield to that arrogant request.

The Administration has made blunder after blunder in waging the war on terrorism. Congress should not aid and abet them in committing another one.

###

43453.246

U.S. SENATOR PATRICK LEAHY

CONTACT: David Carle, 202-224-3693 VERMONT

STATEMENT OF SENATOR PATRICK LEAHY,
RANKING MEMBER, JUDICIARY COMMITTEE
HEARING ON "FISA FOR THE 21ST CENTURY"
WEDNESDAY, JULY 26, 2006

I thank the Chairman for convening this hearing. We are especially glad to welcome General Hayden to his first appearance before this Committee since he assumed his new duties. The CIA has been in desperate need of the professionalism that he brings to this difficult job. Independence and competence were the two watchwords that led me to believe that he would serve well as Director of the CIA, and we need straight talk today in navigating the issues that we will be discussing at this hearing.

There are two sets of issues relating to the Foreign Intelligence Surveillance Act that are now before this Committee. First, what is the extent of the Administration's warrantless wiretapping in violation of FISA, and how should we in Congress react? After seven months and four hearings, we remain largely in the dark about what the Administration has been doing and continues to do, because the Administration has stonewalled this Committee's bipartisan efforts at oversight. But the answer is clear: we must demand and ensure that this Administration, and future Administrations, follow the law.

Second, does the FISA law itself need to be revised? Although it has been amended six times at this Administration's request in the five years since 9/11, the Administration is now telling us that it needs "modernization." The call for "modernization" is the focus of today's hearing. I appreciate Chairman Specter's agreement to the request that I and my fellow Democratic members of the Committee made to hold this hearing on the so-called modernization provisions contained in Section 9 of the Chairman's bill. Those proposals make substantial changes that require careful review.

It is important to emphasize at the outset that the issues of compliance and modernization are entirely separate. Whether or not FISA is in need of fine-tuning is a legitimate consideration, but FISA's possible imperfections provide no excuse for the Administration's flouting of existing law. By the same token, the Bush-Cheney Administration's outrageous disregard for existing law does not mean that we in Congress should shirk our responsibility to improve the law if there is room for improvement.

SECTION 9 "MODERNIZATION" PROVISIONS

So I am ready to consider Section 9 of the Chairman's bill on its merits. But I see serious grounds for skepticism, and I have some serious questions about those provisions, to which I think we need some candid answers.

senator_leahy@leahy.senate.gov
http://leahy.senate.gov/

43453.247

First, if Section 9's provisions are, as claimed, needed to bring FISA up-to-date with 21st Century technology, why haven't we heard about them until now? Not only have we amended FISA six times in the past five years. In July 2002, former Attorney General Ashcroft testified that the 2001 PATRIOT Act had "modernized our surveillance tools to keep pace with technological changes." In March of this year, in the Reauthorization of the PATRIOT Act, Congress made all the amendments to FISA that the Administration requested, and the President took credit for updating the law further.

If FISA as amended is too "quaint" to meet the challenges of the 21st Century, the Bush-Cheney Administration owes the Congress and the American people an explanation for its failure to speak up before now. This Administration is not shy about seeking expansions of Executive power, so I am naturally skeptical of a supposed need for modernization that it has been so slow to discover.

Second, FISA is a very complex and finely calibrated statute. In order to evaluate the merits of technical-sounding proposed changes and definitional provisions, we need to understand their purpose and likely practical effect – not just take the Administration's word that they make sense. We need to know what obstacles to the government's ability to protect the nation's security the proposed amendments would remove, and what dangers to Americans' liberties and privacy they would present.

To the extent that I have been able to figure out the highly complex language of Section 9 of the Chairman's bill, it seems to me to permit vast new amounts of warrantless surveillance of telephone calls involving American citizens. It would appear to authorize unrestricted, unregulated government surveillance of American citizens talking to relatives, colleagues and trading partners overseas, without any showing that that surveillance is likely to protect our national security. It would also allow limitless delegation of the Attorney General's authority, down to the lowest-level government employee. But to the extent that the Administration's witnesses can explain to us today, in practical and concrete terms, why they make sense, I will listen.

OTHER PROVISIONS

I will have some hard questions about Section 9. But let me turn for a minute to the rest of the Chairman's bill. It has been called a compromise. This Vermonter does not believe that we should ever compromise on requiring the Executive to submit to the rule of law. I am sad to say that I see this bill as less of a compromise and more a concession. It would abandon our oversight role and confine oversight to a single judge on a secret court, whose decision on the one program the Bush-Cheney Administration has agreed to submit for review is appealable only by the Government. And even that oversight would not be required by the bill itself. I expect that Senator Specter got the best deal that he thought he could. The President, Vice President and their legions can be hard-headed rather than flexible bargainers to be sure. I make these observations respectfully, not to criticize Senator Specter, who has reached his own judgment about how he is wiling to

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00301 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.248

proceed, but to express my reluctance to compromise FISA and the minimal protections it provides for Americans.

Section 8 would repeal FISA's "exclusivity" provision and affirmatively embrace the President's claim of sweeping inherent authority. The result is to make FISA optional. The President may use it or not, at his discretion.

It is astounding to me that we are considering this proposal. FISA was never intended to give Presidents choices; it was enacted to prevent abuses of Executive power and protect Americans' liberties by prohibiting the Government from spying on its citizens without court approval. The Bush-Cheney Administration has chosen to simply ignore it. Are we now going to reward its flouting of the rule of law by saying, in effect, "Oh, please excuse us for passing that law, we didn't mean it and we won't do it again."

Defenders of the bill have argued that Section 8 is meaningless because the President has whatever constitutional authority the Constitution says, and Congress cannot limit that authority through legislation. If the best thing we can say on behalf of proposed legislation is that it is a waste of ink, we should not be enacting it. But I do not for one minute believe that, when it goes before the secret FISA court, the Administration will adhere to the position that Section 8 is meaningless. The Administration is insisting on it for a reason.

As the Supreme Court recently explained in its *Hamdan* decision, the constitutional scope of presidential power depends on the legislation that Congress has enacted, even in times of war. The Constitution grants Congress the express power to set rules for the military, and the express power "To make all laws which shall be necessary and proper for carrying into execution" all the powers vested by the Constitution in the federal government, including those of the President.

In the absence of congressional action, the President may well have some measure of unilateral authority to gather intelligence, including through electronic surveillance. That is what the precedents the Administration always cites suggest. But once Congress has acted, as it did in FISA, the President is no longer free to do whatever he wants. As the Court explained in *Hamdan,* "Whether or not the President has independent power, absent congressional authorization," Congress may, "in proper exercise of its own . . . powers," place limitations on the President's powers.

That was the whole point of FISA: to limit the President's power to spy on ordinary Americans by making FISA the sole means by which foreign intelligence wiretaps may be conducted in the United States. Waiving FISA's exclusivity provision would not be meaningless; it would completely gut FISA and give the President a blank check to carry out warrantless wiretapping whenever he chooses. I could not in good conscience acquiesce in such a sweeping signing away of Americans' liberties in any circumstances. I certainly shall not do so at the behest of an Administration that has repeatedly broken the law.

#####

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00302 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.249

Copyright 2006 Los Angeles Times
All Rights Reserved
Los Angeles Times

July 16, 2006 Sunday
Home Edition

SECTION: CURRENT; Editorial Pages Desk; Part M; Pg. 4

LENGTH: 524 words

HEADLINE: License to wiretap

BODY:

ARLEN SPECTER WAS one of the first members of Congress to raise questions about the National Security Agency's warrantless wiretapping of Americans. So Americans who value their privacy should welcome his agreement with the Bush administration to bring NSA spying under judicial oversight, right?

Wrong. There is less to this "breakthrough" than meets the eye. Yes, the legislation proposed by Specter, the Pennsylvania Republican who is chairman of the Senate Judiciary Committee, has been approved by the White House and would bring the administration's program under the purview of a special federal court that approves wiretaps of U.S. citizens suspected of being an agent of a foreign power. But it would do so at the cost of undermining that court's responsibility to scrutinize individual requests for electronic surveillance.

That court, known as the Foreign Intelligence Surveillance Act court for the law that created it, was the watchdog that didn't bark in the NSA controversy. To his credit, Specter was among those in Congress who called for bringing the NSA into the FISA framework. In addition to offering his own bill, Specter endorsed one by Sen. Dianne Feinstein (D-Calif.) reaffirming the role of the FISA system.

Unfortunately, that is not the bill Specter has sold to the Bush administration.

Instead, President Bush and Atty. Gen. Alberto R. Gonzales have signed on to a different Specter proposal under which the FISA court would not authorize individual wiretaps or e-mail intercepts, but rather would rule on whether an entire program was constitutional and "reasonably designed to ensure" that intercepted communications had a terrorist connection. By definition, this "program-wide" review would pay less attention to the privacy rights of individuals whose calls might be monitored.

Assigning this broader role to FISA opens up a can of legal and constitutional worms. For example, if the FISA court -- and its appellate division -- ruled that a proposed surveillance program was unconstitutional, the government apparently could petition the Supreme Court for review. But the high court would be ruling not on a specific case or controversy but on the legality of the program as a whole, which is hard to square with its long-standing refusal to issue "advisory **opinions.**"

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00303 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.250

The Specter compromise has other weaknesses, traceable to the desire to win White House support. For example, the bill does not require that the president seek FISA court review of electronic surveillance programs, though Bush apparently has agreed to do so. Specter said he was deferring to Bush's desire not to bind his successors, but in a piece of legislation designed to reinforce the rule of law, it is incongruous to make presidential compliance voluntary.

Specter is right that the wiretapping should be tethered to FISA. But the way to do that is to require the government to secure the FISA court's approval for individual NSA surveillance operations. Specter deserves credit for demanding that the administration obey the law when it spies on Americans. But his compromise solution is too much of a compromise and not enough of a solution.

LOAD-DATE: July 16, 2006

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00304 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.251

The New York Times
nytimes.com

PRINTER-FRIENDLY FORMAT SPONSORED BY

June 15, 2006

EDITORIAL

A Leap of Faith, Off a Cliff

On Monday, the Bush administration told a judge in Detroit that the president's warrantless domestic spying is legal and constitutional, but refused to say why. The judge should just take his word for it, the lawyer said, because merely talking about it would endanger America. Today, Senator Arlen Specter wants his Judiciary Committee to take an even more outlandish leap of faith for an administration that has shown it does not deserve it.

Mr. Specter wants the committee to approve a bill he drafted that tinkers dangerously with the rules on wiretapping, even though the president has said the law doesn't apply to him anyway, and even though Mr. Specter and most of the panel are just as much in the dark as that judge in Detroit. The bill could well diminish the power of the Foreign Intelligence Surveillance Act, known as FISA, which was passed in 1978 to prevent just the sort of abuse that Mr. Bush's program represents.

The committee is considering four bills. Only one even remotely makes sense now: it would give legal standing to groups that want to challenge the spying in court. The rest vary from highly premature (Senator Dianne Feinstein's proposed changes to FISA) to the stamp of approval for Mr. Bush's claims of unlimited power that Senator Mike DeWine drafted.

Mr. Specter's bill is not that bad, but it is fatally flawed and should not go to the Senate floor. He is trying to change the system for judicial approval of government wiretaps in a way that suggests Congress is facing a technical problem with a legislative solution, when in fact it is a constitutional showdown.

There is also a practical problem: a bill on the floor of this Senate becomes the property of the Republican leadership, which will rewrite it to the specifications of Vice President Dick Cheney, the man in charge of this particular show of imperial power. Mr. Specter, of all people, should have no doubt of that, having been forced to watch in embarrassment last week as Mr. Cheney seized control of the committee's deliberations on the spying issue.

Mr. Specter says his bill would impose judicial review on domestic spying by giving the special court created by FISA power to rule on the constitutionality of the one program that Mr. Bush has acknowledged. But the review would be optional. Mr. Specter's bill would eliminate the vital principle that FISA's rules are the only legal way to eavesdrop on Americans' telephone calls and e-mail. It would give the president power to conduct surveillance under FISA "or under the constitutional authority of the executive." That merely reinforces Mr. Bush's claim that he is the sole judge of what powers he has, and how he exercises them.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00305 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.252

Mr. Specter's lawyers have arguments for many of these criticisms, and say the bill is being improved. But the main problem with the bill, like most of the others, is that it exists at all. This is not a time to offer the administration a chance to steamroll Congress into endorsing its decision to ignore the 1978 intelligence act and shred constitutional principles on warrants and on the separation of powers. This is a time for Congress to finally hold Mr. Bush accountable for his extralegal behavior and stop it.

Copyright 2006 The New York Times Company

Privacy Policy | Search | Corrections | XML | Help | Contact Us | Work for Us | Site Map

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00306 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.253

4 of 128 DOCUMENTS

Copyright 2006 The New York Times Company
The New York Times

July 16, 2006 Sunday
Late Edition - Final

SECTION: Section 4; Column 1; Editorial Desk; Pg. 11

LENGTH: 1456 words

HEADLINE: The Real Agenda

BODY:

It is only now, nearly five years after Sept. 11, that the full picture of the Bush administration's response to the terror attacks is becoming clear. Much of it, we can see now, had far less to do with fighting Osama bin Laden than with expanding presidential power.

Over and over again, the same pattern emerges: Given a choice between following the rules or carving out some unprecedented executive power, the White House always shrugged off the legal constraints. Even when the only challenge was to get required approval from an ever-cooperative Congress, the president and his staff preferred to go it alone. While no one questions the determination of the White House to fight terrorism, the methods this administration has used to do it have been shaped by another, perverse determination: never to consult, never to ask and always to fight against any constraint on the executive branch.

One result has been a frayed democratic fabric in a country founded on a constitutional system of checks and balances. Another has been a less effective war on terror.

The Guantanamo Bay Prison

This whole sorry story has been on vivid display since the Supreme Court ruled that the Geneva Conventions and United States law both applied to the Guantanamo Bay detention camp. For one brief, shining moment, it appeared that the administration realized it had met a check that it could not simply ignore. The White House sent out signals that the president was ready to work with Congress in creating a proper procedure for trying the hundreds of men who have spent years now locked up as suspected terrorists without any hope of due process.

But by week's end it was clear that the president's idea of cooperation was purely cosmetic. At hearings last week, the administration made it clear that it merely wanted Congress to legalize President Bush's illegal actions -- to amend the law to negate the court's ruling instead of creating a system of justice within the law. As for the Geneva Conventions, administration witnesses and some of their more ideologically blinkered supporters in Congress want to scrap the international consensus that no prisoner may be robbed of basic human dignity.

The hearings were a bizarre spectacle in which the top military lawyers -- who had been elbowed aside when the procedures at Guantanamo were established -- endorsed the idea that the prisoners were covered by the Geneva Convention protections. Meanwhile, administration officials and obedient Republican lawmakers offered a lot of silly talk about not coddling the masterminds of terror.

The divide made it clear how little this all has to do with fighting terrorism. Undoing the Geneva Conventions would further endanger the life of every member of the American military who might ever be taken captive in the future. And if the prisoners scooped up in Afghanistan and sent to Guantanamo had been properly processed first -- as military lawyers wanted to do -- many would never have been kept in custody, a continuing reproach to the country that is holding them. Others would actually have been able to be tried under a fair system that would give the world a less

perverse vision of American justice. The recent disbanding of the C.I.A. unit charged with finding Osama bin Laden is a reminder that the American people may never see anyone brought to trial for the terrible crimes of 9/11.

The hearings were supposed to produce a hopeful vision of a newly humbled and cooperative administration working with Congress to undo the mess it had created in stashing away hundreds of people, many with limited connections to terrorism at the most, without any plan for what to do with them over the long run. Instead, we saw an administration whose political core was still intent on hunkering down. The most embarrassing moment came when Bush loyalists argued that the United States could not follow the Geneva Conventions because Common Article Three, which has governed the treatment of wartime prisoners for more than half a century, was too vague. Which part of "civilized peoples," "judicial guarantees" or "humiliating and degrading treatment" do they find confusing?

Eavesdropping on Americans

The administration's intent to use the war on terror to buttress presidential power was never clearer than in the case of its wiretapping program. The president had legal means of listening in on the phone calls of suspected terrorists and checking their e-mail messages. A special court was established through a 1978 law to give the executive branch warrants for just this purpose, efficiently and in secrecy. And Republicans in Congress were all but begging for a chance to change the process in any way the president requested. Instead, of course, the administration did what it wanted without asking anyone. When the program became public, the administration ignored calls for it to comply with the rules. As usual, the president's most loyal supporters simply urged that Congress pass a law allowing him to go on doing whatever he wanted to do.

Senator Arlen Specter, chairman of the Senate Judiciary Committee, announced on Thursday that he had obtained a concession from Mr. Bush on how to handle this problem. Once again, the early perception that the president was going to bend to the rules turned out to be premature.

The bill the president has agreed to accept would allow him to go on ignoring the eavesdropping law. It does not require the president to obtain warrants for the one domestic spying program we know about -- or for any other program -- from the special intelligence surveillance court. It makes that an option and sets the precedent of giving blanket approval to programs, rather than insisting on the individual warrants required by the Constitution. Once again, the president has refused to acknowledge that there are rules he is required to follow.

And while the bill would establish new rules that Mr. Bush could voluntarily follow, it strips the federal courts of the right to hear legal challenges to the president's wiretapping authority. The Supreme Court made it clear in the Guantanamo Bay case that this sort of meddling is unconstitutional.

If Congress accepts this deal, Mr. Specter said, the president will promise to ask the surveillance court to assess the constitutionality of the domestic spying program he has acknowledged. Even if Mr. Bush had a record of keeping such bargains, that is not the right court to make the determination. In addition, Mr. Bush could appeal if the court ruled against him, but the measure provides no avenue of appeal if the surveillance court decides the spying program is constitutional.

The Cost of Executive Arrogance

The president's constant efforts to assert his power to act without consent or consultation has warped the war on terror. The unity and sense of national purpose that followed 9/11 is gone, replaced by suspicion and divisiveness that never needed to emerge. The president had no need to go it alone -- everyone wanted to go with him. Both parties in Congress were eager to show they were tough on terrorism. But the obsession with presidential prerogatives created fights where no fights needed to occur and made huge messes out of programs that could have functioned more efficiently within the rules.

Jane Mayer provided a close look at this effort to undermine the constitutional separation of powers in a chilling article in the July 3 issue of The New Yorker. She showed how it grew out of Vice President Dick Cheney's long and deeply held conviction that the real lesson of Watergate and the later Iran-contra debacle was that the president needed more power and that Congress and the courts should get out of the way.

To a disturbing degree, the horror of 9/11 became an excuse to take up this cause behind the shield of Americans' deep insecurity. The results have been devastating. Americans' civil liberties have been trampled. The nation's image as

a champion of human rights has been gravely harmed. Prisoners have been abused, tortured and even killed at the prisons we know about, while other prisons operate in secret. American agents "disappear" people, some entirely innocent, and send them off to torture chambers in distant lands. Hundreds of innocent men have been jailed at Guantanamo Bay without charges or rudimentary rights. And Congress has shirked its duty to correct this out of fear of being painted as pro-terrorist at election time.

We still hope Congress will respond to the Supreme Court's powerful and unequivocal ruling on Guantanamo Bay and also hold Mr. Bush to account for ignoring the law on wiretapping. Certainly, the president has made it clear that he is not giving an inch of ground.

URL: http://www.nytimes.com

LOAD-DATE: July 16, 2006

Patriots to restore Checks and Balances

July 20, 2006

The Honorable ***Patrick Leahy***
United States Senate
Washington, DC 20510

Dear Senator ***Leahy***,

On behalf of Patriots to Restore Checks and Balances and its network of conservative and libertarian individuals and organizations, I strongly urge you to reject the so-called "compromise" reached by Vice-President Dick Cheney and Senate Judiciary Committee Chairman Arlen Specter on legislation authorizing the president to wiretap Americans without individual warrants from courts. This deal will be introduced as an amendment to S.2453, the "National Security Surveillance Act of 2006," in the Senate Judiciary Committee this Thursday.

While the White House and Senator Specter tout this measure as a panacea to the NSA's lawless spying, in reality it fails to hold the administration accountable, lacks adequate oversight and weakens the Foreign Intelligence Surveillance Act (FISA) created to protect Americans against unreasonable and unnecessary wiretaps. The proposed legislation gives this and future presidents more than a blank check — it gives them a blank checkbook. Here's how:

- **The Specter-Cheney bill rewrites FISA to allow the president to wiretap without a court order, eliminating judicial review.** The proposed legislation would rewrite FISA to allow the president to wiretap without a court order. The Fourth Amendment requires a court to issue a warrant describing the person and thing to be searched and seized, and FISA echoes this by requiring court review of every wiretap of an American resident in national security investigations. Even though the current judicial review process does approve warrants when an American is conspiring with al Qaeda, the president still refuses to follow the law. If the Cheney-Specter bill passes, the law will no longer require the president to get a court order to wiretap Americans. Rather than restoring judicial review, the proposed legislation would eliminate judicial review in all but one instance in which the deck is stacked with judges handpicked to hear the case.

- **Neither Congress nor the courts would be informed of spying on innocent Americans.** Under the proposed legislation, neither Congress nor the FISA court would be informed of the number of Americans being wiretapped or the names of individuals under surveillance. Instead, it authorizes the court to approve a "program-wide" warrant that includes a broad sweep of conversations of Americans believed to have communicated or been associated with an agent of a foreign power. Any journalist, lawyer or hotel clerk who has ever been contacted by an individual being monitored by U.S. agents could have his or her phone conversations wiretapped indefinitely.

- **The Cheney-Specter bill forces all state and federal challenges of wiretapping or data mining into secret court proceedings.** The Cheney-Specter bill would require all state and federal cases challenging illegal wiretapping or data mining to be transferred to the FISA court, where proceedings are held in secret and cases can be dismissed for "any reason." In an unprecedented move, the White House also insisted that the court withhold secret information even from Americans entitled to it under federal law unless

1718 M Street, NW, Mailbox #232, Washington, DC 20036
Phone: 1-800-583-9122 **Web site**: www.checksbalances.org

07/20/2006 10:57AM

43453.257

they obtain special permission from the attorney general. After the secret FISA court rules, U.S. courts are directed to follow their orders.

- **The Cheney-Specter bill legalizes data mining.** In the wake of revelations about widespread data mining of Americans' personal records, the proposed legislation would change the definition of surveillance to exclude the NSA's collection of data about millions of innocent Americans. In addition, the Cheney-Specter bill would also compensate companies that cooperate with the NSA and give them immunity from liability.

- **The Cheney-Specter bill changes the rules on physical searches of homes and businesses.** The proposed legislation would give the government power to demand that landlords and other businesses make phones and computers secretly available under program warrants, which neither specify any individual by name nor are based on any evidence that the individual is conspiring with al Qaeda. In addition, the legislation would eliminate the requirement in FISA that an individual court warrant be issued before a home can be searched during times of war. This gives the administration blanket authority to secretly search Americans' homes and businesses in the name of national security during wartime without any evidence.

A thorough review of all facets of the administration's domestic surveillance programs must take place before Congress generously sanctions it. It is Congress' responsibility to hold hearings, investigate and serve as a robust check to the Executive Branch to ensure the protection of Americans civil liberties and privacy rights.

I urge you to restore constitutional checks and balances to the law by rejecting S. 2453. We are safer when the government focuses its resources on those conspiring with al Qaeda rather than wasting our tax dollars allowing innocent Americans' rights to be violated without any proof they are doing anything wrong

Sincerely,

Bob Barr
Member of Congress, 1995-2003
Chairman, Patriots to Restore Checks and Balances

1718 M Street, NW, Mailbox #232, Washington, DC 20036
Phone: 1-800-583-9122 **Web site**: www.checksbalances.org

07/20/2006 10:57AM

43453.258

**STATEMENT OF FORMER ASSOCIATE ATTORNEY GENERAL JOHN SCHMIDT
BEFORE THE SENATE JUDICIARY COMMITTEE
JULY 28, 2006**

My name is John Schmidt. I am now a partner in the law firm of Mayer, Brown, Rowe & Maw in Chicago. From 1994 to 1997, I served as the Associate Attorney General of the United States in the Justice Department under President Bill Clinton. Prior to going to the Justice Department I served from 1993 to 1994 as Ambassador and Chief United States Negotiator to the Uruguay Round under the General Agreement on Tariffs & Trade. I have a long history of active support for Democrats for local and national office, including serving as the first Chief of Staff for Mayor Richard M. Daley in Chicago and leadership positions in campaigns of Paul Simon, Adlai Stevenson, Barack Obama and others.

The question we should ask about possible changes in the Foreign Intelligence Surveillance Act is not who "wins" or "loses" between Congress and the President, as though the separation of powers were a sporting event between the branches. The question is what institutional structure will both protect our constitutional rights and achieve effective surveillance of Al Qaeda and other terrorist groups. Passage of the bill drafted by Senator Spector would be a constructive step toward both of these objectives.

The Specter bill would allow the President to submit to the Foreign Intelligence Surveillance Court for review of its constitutionality a program for electronic surveillance of terrorist groups that does not involve FISA court approval of individualized warrants identifying the specific surveillance targets. The President cannot do that under current law. The FISA court has been explicit that it is a court of limited statutory jurisdiction; for example, the court refused some years ago to consider an application for approval of a physical search to obtain foreign intelligence at a time when the statute was limited to the approval of electronic surveillance.

The surveillance program that President Bush authorized the National Security Agency to undertake after 9/11 involves decisions by NSA professionals in a 'real time' process that President Bush, General Hayden and others have all said could not be reconciled with the FISA statutory requirement for individualized approval of warrants. Based on everything we know about it, the NSA program nevertheless appears to most observers to be protective of constitutional rights, in light of the critical importance of the information to be obtained, in a way that would satisfy the requirement of reasonableness under the Fourth Amendment.

Outside observers, however, cannot know the specifics of what is, by its nature, a secret surveillance program. And outside observers do not have the institutional capacity and independence of federal judges in making constitutional judgments.

43453.259

A federal court determination of the constitutionality of the NSA program, which the Specter bill allows, would be good for everyone—for the President, Congress, NSA security professionals and the American people.*

It would be good for the President to find out whether a federal court agrees that the NSA program is constitutional. Such a judgment would allow the President to make changes if necessary to satisfy constitutional standards.

It would be good for Congress for a federal court to make that constitutional judgment. Congress lacks the institutional capacity to make a constitutional judgment of this nature. As a political branch, its members are susceptible, in appearance if not in fact, to the partisan pressures of subservience, by members of the President's party, or hostility, by members of the opposition. While Congress may make broad constitutional judgments in legislating, it has no mechanism for making judgments that require assessment of the details of a particular program. Congressional oversight, while it should continue, is misused when it is asked to bear the weight of such constitutional judgments.

It would be good for security professionals at the NSA and elsewhere to be given the confidence of a federal court judgment on the constitutionality of their actions. There is no reason to think the current NSA program is the last word when it comes to electronic surveillance of terrorist groups. We want the smartest and most creative people at the NSA and elsewhere in government working with the best communications professionals in the private sector to develop new and better surveillance methods than any we can currently imagine. Creative and aggressive efforts of this kind must be inhibited today by the prospect than any changes in the current program, or wholly new surveillance programs, will face confrontation and dispute over their legality. A procedure for court review, in contrast, allows security professionals to know that the constitutionality of future programs can be reviewed by a court before they are put into effect.

Finally, a federal court judgment on the constitutionality of a surveillance program would be good for the American people. Federal courts are far and away our most trusted institutional means to make constitutional judgments. Such a judgment will increase the confidence of all of us that our constitutional rights are being protected.

The Specter bill also contains an acknowledgement of the President's Article II authority as commander-in-chief, outside the statute, to order warrantless electronic surveillance of a foreign enemy that has attacked this country. This provision is consistent with judicial authority. Three federal Court of Appeals decisions have held that the President has power under Article II to order warrantless wiretapping for foreign intelligence purposes.** The only judicial decision that deals with Congressional authority

* The idea of giving the FISA court the authority to approve a surveillance program, in addition to individualized warrants, was actually suggested thirty years ago by Attorney General Edward Levi. See "A Historical Solution to the Bush Spying Issue," *Chicago Tribune* (February 12, 2006) (attached).

** United States v. Brown, 484 F.2d 418 (5th Cir. 1973); United States v. Butenko, 494 F.2d 593 (3d Cir. 1974); United States v. Truong Dinh Hung, 629 F.2d 908 (1980).

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00313 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.260

in the surveillance area says flatly that "Congress could not encroach on the President's constitutional power."* Thus, by including this recognition, Congress is simply acknowledging what the courts have said.

But even if Congress could constitutionally limit the President's surveillance authority to a specified statutory process, Congress should not want to do that. Edward Levi, the great Attorney General under President Ford who played a critical role in the development of the FISA statute, repeatedly said that it would be "dangerous" for Congress to enact a statute that did not explicitly acknowledge the President's Article II surveillance power. Although Levi was prepared to say that President Ford would use the FISA statutory process in all circumstances he could then anticipate, he emphasized that future foreign threats to this country were unpredictable and communications technologies could change in ways that made the statutory process inadequate to those future threats.

If there was any previous doubt, the events of 9/11 proved Levi unmistakably correct. No one anticipated a massive terrorist attack here in the United States creating a need for surveillance in this country on where and when that terrorist group might attack next. When the NSA told the President that it could potentially obtain information on such a future attack using surveillance technologies that were inconsistent with the requirements of the FISA statutory process, the President had to rely on his Article II power or deny us the added protection from that surveillance.

If those who assert that the FISA statutory process is "exclusive" were correct, then if General Hayden had called President Bush on the morning of 9/11 and said that the NSA wanted to go forward immediately with intercepts of calls at other airports where Al Qaeda was believed to be planning further attacks, the President's only lawful response would have been to tell the NSA to get in touch with the Attorney General and begin examining whether each of the proposed intercepts satisfied the FISA standard, with the prospect of obtaining authorization many hours, if not days, later. That is not the way any American President would understand his constitutional authority and I do not believe any court would reach that result.

One can debate the extent of the President's constitutional power to carry out surveillance on a foreign enemy outside the confines of a statute, but there can be no serious doubt that in some circumstances such power exists. The provision in the Specter bill does not purport to define the extent of the President's Article II power, but only to acknowledge its existence.

I would change the bill's procedures for judicial review of a terrorist surveillance program in three respects:

1. A surveillance program is more appropriately submitted for review directly to the Foreign Intelligence Surveillance Court of Review, consisting of 3 federal Court of Appeals Judges, instead of to the Foreign Intelligence Surveillance Court, which consists of District Court judges. Under the current bill, the constitutionality of a program would

* In re Sealed Case, 310 F. 3d 717, 742 (Foreign Intelligence Surveillance Court of Review 2002).

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00314 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.261

reach the appellate court level only if the lower court denied approval and the government appealed.

2. The statute should provide that the Court of Review will make public its decision on any surveillance program to the extent it can do so without compromising the secrecy of the program. While I believe the Court would take such action anyway, as it did when it made public its opinion on the required "wall" procedures after passage of the Patriot Act, it would be desirable to provide assurance to that effect.

3. The statute should direct the Court of Review to submit copies of any opinion on the legality of a surveillance program to the Supreme Court and allow the Supreme Court to review the decision on a writ of certiorari if it chooses to do so. This would provide assurance that decisions are consistent with the Supreme Court's view of constitutional requirements.

I would also eliminate the provision of that bill that describes the specific nature of the communications that a surveillance program must target and instead simply require the court to determine that a program is consistent with the Constitution. While the more specific provisions seem reasonable and may fit the current NSA program, the statute is most likely to serve its purpose if the court has maximum flexibility to apply the Constitution to what may be wholly unanticipated future circumstances.

Congress and the President have the opportunity to get beyond the current confrontation over the NSA program and create an institutional mechanism that can avoid similar controversies in the future. Constitutional protection and terrorist surveillance will both be advanced by passage of the Specter bill.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00315 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.262

A historical solution to the Bush spying issue

by John Schmidt

This article originally appeared in the February 12, 2006 edition of the *Chicago Tribune*. Reprinted by permission.

Thirty years ago, Edward Levi, the most respected U.S. attorney general of the modern era, suggested a procedure that would resolve the dispute regarding President Bush and the National Security Agency wiretapping program.

In 1975 testimony to the Church Committee on U.S. intelligence activities, Levi suggested that court power to authorize foreign- intelligence wiretapping in the U.S. go beyond traditional warrants based on probable cause for surveillance of a particular individual. He said it should include power to approve a "program of surveillance" that is "designed to gather foreign-intelligence information essential to the security of the nation." Congress passed the Foreign Intelligence Surveillance Act in 1978, setting up a new court with authority to approve electronic surveillance on a case-by-case basis, but without Levi's suggested additional power.

Levi said a traditional warrant procedure works when surveillance "involves a particular target location or individual at a specific time." Foreign intelligence, however, may in some situations require "virtually continuous surveillance, which by its nature does not have specifically predetermined targets." In these situations, "the efficiency of a warrant requirement would be minimal."

In approving a surveillance plan, "judicial decision would take the form of an ex parte determination that the program of surveillance designed by the government strikes a reasonable balance between the government's need for the information and the protection of individuals' rights."

Had Levi's procedure been in place, President Bush could have submitted to a court an application setting out the elements of the proposed NSA surveillance program: the target; communications to be intercepted; screening methods; controls on information dissemination. Because FISA procedures are secret, a court application would not have compromised the program's secrecy. If Congress puts this procedure into the law, the president can submit the NSA program for approval now.

The court role would be limited to approving the "reasonableness" of the plan under the 4th Amendment, using a standard of review that recognizes the president's primary constitutional role in surveillance on foreign powers. The approving court might be the three-judge FISA court of review.

Based on everything we know, NSA's surveillance program would be approved. Even the president's critics generally acknowledge that, based upon what we know, the NSA program is "reasonable" in responding to the Al Qaeda threat.

Although Levi supported legislation in the foreign intelligence area, he rejected the position of Bush critics that the president's authority to order warrantless foreign intelligence surveillance can be limited by Congress to a statutory procedure. Levi told the Church Committee that the president has inherent constitutional authority to conduct such surveillance. Asked by Sen. Frank Church "if the constitutional powers in the area of foreign intelligence are exclusive to the executive or whether they are concurrent with the legislative branch," Levi replied:

"They are sufficiently concurrent so that legislation by the Congress would be influential . . . You are asking me

43453.263

whether I think there is presidential power beyond that, and my answer is 'Yes.'"

Levi was correct in predicting that, despite the president's inherent power, legislation by Congress in the foreign intelligence area would be "influential."

All presidents since FISA was passed have used the FISA court process to obtain surveillance authorization for particular individuals. Presidents would also use Levi's suggested procedure to obtain court approval of a surveillance program. President Bush has said he pressed his lawyers on whether the NSA program could be carried out through the existing FISA process, but the rapid time sequence and the need for security professionals to make quick decisions could not be reconciled with the FISA requirement to determine case-by-case probable cause in a manner that could satisfy the court.

Giving a court the power to approve a reasonable surveillance plan proposed by the president gives everyone--the president and those in the executive branch who carry out the surveillance, members of Congress who have oversight responsibility, and the American people--greater assurance that constitutional rights are being protected.

It made sense when Edward Levi suggested it 30 years ago and it makes sense today.

John R. Schmidt, a Chicago attorney, served from 1994 to 1997 as the associate attorney general in the Justice Department under President Bill Clinton.

43453.264

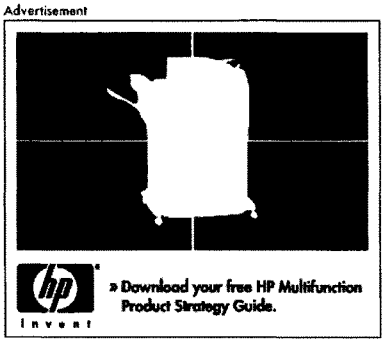
washingtonpost.com

Wiretap Surrender

Sen. Specter's bill on NSA surveillance is a capitulation to administration claims of executive power.

Saturday, July 15, 2006; A20

Advertisement



SENATE JUDICIARY Committee Chairman Arlen Specter (R-Pa.) has cast his agreement with the White House on legislation concerning the National Security Agency's warrantless surveillance as a compromise -- one in which President Bush accepts judicial review of the program. It isn't a compromise, except quite dramatically on the senator's part. Mr. Specter's bill began as a flawed but well-intentioned effort to get the program in front of the courts, but it has been turned into a green light for domestic spying. It must not pass.

The bill would, indeed, get the NSA's program in front of judges, in one of two ways. It would transfer lawsuits challenging the program from courts around the country to the super-secret court system that typically handles wiretap applications in national security cases. It would also permit -- but not require -- the administration to seek approval from this court system, created by the Foreign Intelligence Surveillance Act, for entire surveillance programs, thereby allowing judges to assess their legality.

But the cost of this judicial review would be ever so high. The bill's most dangerous language would effectively repeal FISA's current requirement that all domestic national security surveillance take place under its terms. The "compromise" bill would add to FISA: "Nothing in this Act shall be construed to limit the constitutional authority of the President to collect intelligence with respect to foreign powers and agents of foreign powers." It would also, in various places, insert Congress's acknowledgment that the president may have inherent constitutional authority to spy on Americans. Any reasonable court looking at this bill would understand it as withdrawing the nearly three-decade-old legal insistence that FISA is the exclusive legitimate means of spying on Americans. It would therefore legitimize whatever it is the NSA is doing -- and a whole lot more.

Allowing the administration to seek authorization from the courts for an "electronic surveillance program" is almost as dangerous. The FISA court today grants warrants for individual surveillance when the government shows evidence of espionage or terrorist ties. Under this bill, the government could get permission for long-term programs involving large numbers of innocent individuals with only a showing that the program is, in general, legal and that it is "reasonably designed" to capture the communications of "a person reasonably believed to have communication with" a foreign power or terrorist group.

The bill even makes a hash out of the generally reasonable idea of transferring existing litigation to the FISA court system. It inexplicably permits the FISA courts to "dismiss a challenge to the legality of an electronic surveillance program for *any* reason" -- such as, say, the eye color of one of the attorneys.

This bill is not a compromise but a full-fledged capitulation on the part of the legislative branch to executive claims of power. Mr. Specter has not been briefed on the NSA's program. Yet he's proposing revolutionary changes to the very fiber of the law of domestic surveillance -- changes not advocated by

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00318 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.265

key legislators who have detailed knowledge of the program. This week a remarkable congressional debate began on how terrorists should face trial, with Congress finally asserting its role in reining in overbroad assertions of presidential power. What a tragedy it would be if at the same time, it acceded to those powers on the fundamental rights of Americans.

© 2006 The Washington Post Company

Ads by Google

USA Patriot Act Solution
Complete tracking and reporting for Patriot Act Section 326. Free Trial
www.USAPatriotActCompliance.com

Identity Verification
OFAC Screening USA Patriot Act compliance
www.remitpro.com

Stop illegal NSA wiretaps
Demand a special counsel to investigate Bush's domestic spying!
www.americasdemocrats.org

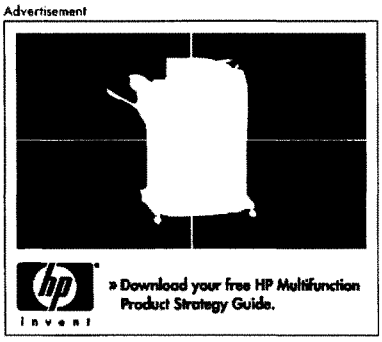
washingtonpost.com

Blank Check to Spy

Arlen Specter says his surveillance bill wouldn't give the administration unwarranted power. He's wrong.

Wednesday, July 26, 2006; A16

Advertisement



TODAY THE Senate Judiciary Committee will hold a hearing on modernizing the Foreign Intelligence Surveillance Act (FISA), the 1978 law that regulates domestic wiretapping and searches. The hearing is an effort on the part of committee Chairman Arlen Specter to move along his very dangerous bill -- negotiated with the White House -- to put the National Security Agency's domestic surveillance program before the federal courts. In an op-ed in these pages Monday, Mr. Specter described his proposal as a compromise with President Bush to ensure judicial review of the NSA program, which he called "a festering sore on our body politic." Yet his legislation would essentially respond to this festering sore by shooting the patient.

No matter how adamantly Mr. Specter denies that his bill would give Congress's blessing to domestic spying outside of FISA's strictures, it does so explicitly and unambiguously. It adds the following language to a statute that now provides the sole legal means for the government to spy on Americans in national security cases: "Nothing in this Act shall be construed to limit the constitutional authority of the President to collect intelligence with respect to foreign powers and agents of foreign powers." Mr. Specter argues that the bill doesn't accept the president's assertions of unilateral power but merely acknowledges them. But this is incorrect.

Under the Supreme Court's decades-old understanding, presidential power is at its lowest ebb when the president is acting contrary to the will of Congress, and at its zenith when he is using his own powers in concert with legislative authorization. Right now, to conduct warrantless surveillance domestically Mr. Bush must act at the very least in sharp tension with FISA. Under Mr. Specter's bill, however, the legislature would be explicitly acknowledging an alternative source of authority for snooping. It would thereby legitimize not only whatever the NSA may now be doing but lots of other surveillance it might dream up.

The bill would also allow -- but not require -- the administration to seek warrants for entire surveillance programs, based on the flimsiest evidence against a small subset of the population that would be subject to the surveillance. The result is that consistent with the bill, the administration could either ask or not ask judicial permission to monitor individuals or large groups of people, based on evidence or no evidence. Or it could simply act outside the law entirely.

In his op-ed piece, Mr. Specter challenged critics of his bill to present "a better idea for legislation that would resolve the program's legality." Ironically, several better ideas are already out there, from legislators who, unlike Mr. Specter, have actually been briefed on the NSA program. These proposals vary a lot, from more modest authorizations of the program to efforts to streamline FISA and provide resources so that authorities could get warrants more quickly. Remarkably, none of the legislators who have received detailed briefings has put forward a proposal as dramatic as Mr. Specter's. That should tell senators something.

VerDate Nov 24 2008 10:43 Apr 22, 2009 Jkt 043453 PO 00000 Frm 00320 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\43453.TXT SJUD1 PsN: CMORC

43453.267

Washington Post
Ashcroft Nostalgia

By Ruth Marcus
Wednesday, July 26, 2006; A17

Alberto Gonzales is achieving something remarkable, even miraculous, as attorney general: He is making John Ashcroft look good.

I was no fan of President Bush's first attorney general, who may be best remembered for holding prayer breakfasts with department brass, hiding the bare-breasted statue in the Great Hall of Justice behind an $8,000 set of drapes, and warning darkly that those who differed with administration policy were giving aid to terrorists.

But as I watched Gonzales testify before the Senate Judiciary Committee last week, it struck me: In terms of competence (the skill with which he handles the job) and character (willingness to stand up to the president), Gonzales is enough to make you yearn for the good old Ashcroft days.

Gonzales is an amiable man, not nearly so polarizing or ideological as his predecessor. If you were given the old desert-island choice between the two, he would be the better option -- more likely to share the rainwater, less likely to make you listen to him sing. (If you've ever heard Ashcroft's "Let the Eagle Soar," you know what I mean.)

Where Ashcroft was hard-edged and combative, Gonzales is pleasant and seemingly imperturbable. He's always reminded me a bit of the Pillsbury doughboy: No matter how hard he's poked, he springs back, smiling.

At the start of last week's hearing, Senate Judiciary Committee Chairman Arlen Specter (R-Pa.), sounding like an exasperated high school English teacher, chastised Gonzales for failing to turn in his prepared statement on time. The attorney general sat silent, then calmly delivered the tardy testimony.

The next three hours and 40 minutes illustrated just about everything that is wrong with Gonzales's Justice.

There is no polite way to put this: Gonzales doesn't seem to have an adequate grasp of what's happening in his own department or much influence in setting administration policy.

Asked about House-passed legislation that would bar Justice from enforcing a year-old law requiring trigger locks on newly sold handguns, Gonzales said he was "not aware of" the dispute. Asked about his department's prosecutions of corrupt Border Patrol agents (described in a front-page story in this newspaper), Gonzales said he would "have to get back to you."

And when Sen. Edward M. Kennedy (D-Mass.) inquired whether the administration supported reauthorization of the Voting Rights Act as passed by the House, Gonzales didn't seem empowered to give him a straight answer -- though the Judiciary Committee was set to

43453.288

take up the measure that afternoon. "I don't know if I'm in a position to state that as an administration we're going to support that," Gonzales said.

Gonzales as witness is a maddening exercise in jello-nailing. "I'm going to move on and accept your non-answer, because I don't think I'm going to get anything more on that subject, and perhaps nothing more on the next subject," Specter told Gonzales after a fruitless line of questioning about whether Justice was -- as the attorney general had said in May -- considering prosecuting journalists for publishing leaks.

Specter's bleak prediction proved accurate. When he asked Gonzales about the attorney general's previous assurance that the National Security Agency's electronic surveillance was the only program not subject to judicial authorization, this illuminating exchange ensued.

Gonzales: "I'm not sure that those are the words that I used, Mr. Chairman."

Specter: "Well, the substance of the words you used."

Gonzales: "Those are the substance of the words I used, but those are not the exact words that I used."

At which point Specter gave up and changed topics.

Sen. Patrick Leahy (D-Vt.) didn't fare any better on military tribunals. Leahy asked whether Congress should simply ratify the existing system, as an assistant attorney general had urged the previous week.

Gonzales: "That would certainly be one alternative that Congress could consider, Senator Leahy."

Leahy, trying again: "Is that the administration's position, yes or no?"

Gonzales: "I don't believe the administration has a position as to where Congress should begin its deliberations."

Well, that was informative.

The big news of the hearing -- that the president had in effect killed an internal Justice investigation into the domestic spying program by refusing to grant the necessary security clearances to department lawyers -- underscores the most disturbing aspect of Gonzales's tenure: his lack of independence from the president. If Gonzales disagreed with this move -- a bad call and an even worse precedent -- he offered no hint of it at the hearing.

This is not a surprise -- after all, Gonzales's entire public career is entwined with that of George W. Bush -- but it is a disappointment. Ashcroft at least clashed with the White House over detainee policy (he fought internally to give citizens detained as enemy combatants access to counsel) and warrantless surveillance (he refused when Gonzales came to his hospital room asking that he sign papers extending the program).

43453.269

To his credit, Gonzales did resist -- he supposedly threatened to quit -- when the president, pummeled by congressional Republicans over the search of a Democratic congressman's office, considered ordering Justice to return the documents. But Attorney General Gonzales doesn't seem to have any less zeal for unbridled presidential power -- or any less willingness to make outlandish arguments on its behalf -- than did White House Counsel Gonzales.

Which is precisely why he shouldn't be there in the first place -- and why I am experiencing intermittent twinges of a most unexpected emotion: Ashcroft nostalgia.

marcusr@washpost.com

© 2006 The Washington Post Company