AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 109–341

USA PATRIOT ACT

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

USA PATRIOT ACT

APRIL 19, 2005

APRIL 27, 2005

MAY 24, 2005

Printed for the use of the Select Committee on Intelligence

Available via the World Wide Web: http://www.access.gpo.gov/congress/senate

U.S. GOVERNMENT PRINTING OFFICE

24-983 PDF WASHINGTON : 2006

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

SELECT COMMITTEE ON INTELLIGENCE

[Established by S. Res. 400, 94th Cong., 2d Sess.]

PAT ROBERTS, Kansas, *Chairman*
JOHN D. ROCKEFELLER IV, West Virginia, *Chairman*

ORRIN G. HATCH, Utah
MIKE DeWINE, Ohio
CHRISTOPHER S. BOND, Missouri
TRENT LOTT, Mississippi
OLYMPIA J. SNOWE, Maine
CHUCK HAGEL, Nebraska
SAXBY CHAMBLISS, Georgia
JOHN W. WARNER, Virginia

CARL LEVIN, Michigan
DIANNE FEINSTEIN, California
RON WYDEN, Oregon
RICHARD J. DURBIN, Illinois
EVAN BAYH, Indiana
JOHN EDWARDS, North Carolina
BARBARA A. MIKULSKI, Maryland

BILL FRIST, Tennessee, *Ex Officio*
HARRY REID, Nevada, *Ex Officio*

BILL DUHNKE, *Staff Director*
ANDREW W. JOHNSON, *Minority Staff Director*
KATHLEEN P. MCGHEE, *Chief Clerk*

CONTENTS

DAY ONE

Hearing held in Washington, DC:
April 19, 2005 1

Statements of :
Roberts, Hon. Pat, a U.S. Senator from the State of Kansas 1
Prepared statement 2
Rockefeller, Hon. John D. IV, a U.S. Senator from the State of West Virginia, prepared statement 29
Nojeim, Gregory T., Associate Director and Chief Legislative Counsel, ACLU, prepared statement 29
Dempsey, James X., Executive Director, Center for Democracy & Technology, prepared statement 45
MacDonald, Heather, Senior Fellow at the Manhattan Institute for Policy Research, prepared statement 57

Supplemental Materials:
Testimony on the USA PATRIOT Act by Bob Barr 4
Letter from Edwin Meese III and Paul Rosenzweig 10
Testimony of Orin S. Kerr 23
Statement for the Record by Kate Martin 26
Chart on the USA PATRIOT Act 42

DAY TWO

Hearing held in Washington, DC:
April 27, 2005 87

Statements of:
Gonzales, Hon. Alberto R., Attorney General, Department of Justice 97
Prepared statement 90
Mueller, Hon. Robert S. III, Director, Federal Bureau of Investigation 100
Goss, Hon. Porter J., Director, Central Intelligence Agency 104
Prepared statement 102

Supplemental Materials:
April 4, 2005 Letter from William E. Moschella, Assistant Attorney General to Senator Arlen Specter 130
April 26, 2005 Letter from William E. Moschella, Assistant Attorney General to Senator Dianne Feinstein 137

DAY THREE

Hearing held in Washington, DC:
May 24, 2005 153

Statements of:
Caproni, Ms. Valerie, General Counsel, Federal Bureau of Investigation .. 168
Prepared statement 166
Feinstein, Hon. Dianne, a U.S. Senator from the State of California, prepared statement 176
Kris, David S., former Associate Deputy Attorney General, U.S. Department of Justice, prepared statement 188

Page

—Continued

Onek, Joseph, Senior Policy Analyst, Open Society Institute, prepared statement 208

Collins, Daniel P., former Associate Deputy Attorney General, U.S. Department of Justice, prepared statement 212

Dempsey, James X., Executive Director, Center for Democracy and Technology, prepared statement 221

Supplemental Materials:

May 23, 2005 Letter from Richard A. Seamon, University of Idaho 155

THE USA PATRIOT ACT OF 2001

DAY ONE

TUESDAY, APRIL 19, 2005

UNITED STATES SENATE,
SENATE SELECT COMMITTEE ON INTELLIGENCE,
Washington, DC.

The Committee met, pursuant to notice, at 3:05 p.m., in room SH–216, Hart Senate Office Building, Hon. Pat Roberts (Chairman of the Committee) presiding.

Committee Members Present: Senators Roberts, Bond, Lott, Snowe, Chambliss, Warner, Rockefeller, Feinstein, Wyden, and Corzine.

OPENING STATEMENT OF HON. PAT ROBERTS

Chairman ROBERTS. The Committee will come to order.

I would like to apologize to our witnesses for the 40-minute delay due to the procedural votes that we had on the floor of the Senate. I guess the good news is that, at least for the time being, we have completed those votes. The challenge that we face is that at 5 o'clock we will have additional votes. We're down already to 1 hour and 45 minutes.

Now I have a marvelous opening statement that deals with the PATRIOT Act and all of the varied concerns and positives that are involved with that Act and your concerns as well. But, I am going to simply submit that for the record in an attempt to hear from you.

Can we keep the applause down a little bit?

[Laughter.]

Chairman ROBERTS. I think the Vice Chairman is going to do likewise, although he will seek his own counsel.

We've invited a panel of outside experts to provide their views of the USA PATRIOT Act and their opinions on those provisions of the Act which will expire later this year.

Our witnesses are Mr. Gregory T. Nojeim, the Associate Director and Chief Legislative Counsel for the American Civil Liberties Union; Mr. Jim Dempsey, Executive Director of the Center for Democracy and Technology; and Ms. Heather MacDonald, a John M. Olen fellow at the Manhattan Institute. The Committee thanks all of our witnesses for being here today.

[The prepared statement of Chairman Roberts follows:]

PREPARED STATEMENT OF HON. PAT ROBERTS

The Committee will come to order.

On September 11, 2001, 19 terrorists hijacked four flights over the United States. We all remember the events of that day. The images of the collapse of the World Trade Center, the burning Pentagon, and the crash site of United Flight 93 in Shanksville, Pennsylvania should never be forgotten.

But, the story of that day was written well before September 11th, and it was written by the terrorists that lived and trained within the United States. They rented apartments, bought cars, made telephone calls, sent e-mails, surfed the Internet, received wire transfers, and attended flight schools.

The terrorists hid in the open—their sinister plans and intentions camouflaged by millions of innocent, lawful transactions that occur every day in the United States.

The activities of the hijackers went largely unnoticed by our intelligence and law enforcement agencies. As this Committee and the 9/11 Commission have pointed out, systemic flaws in our national security agencies prevented full cooperation that might have stopped these attacks.

But, in addition to these systemic flaws, our national security agencies were operating under obsolete authorities. Their hands were tied by inaccurate interpretations of existing law that restricted common-sense sharing of intelligence information.

The USA PATRIOT Act was the first legislative effort by Congress and the President to reform our national security apparatus in response to the attacks of September 11th. The Act brought intelligence tools into the information age. Collection authorities that had been enacted during the era of the rotary phone had not kept pace with the new world of e-mail, the Internet, and mobile phones. The Act also tore down "walls" erected by overly cautious lawyers that had prevented information sharing and coordination between law enforcement and intelligence officials.

The USA PATRIOT Act was drafted and passed by overwhelming majorities in both the Senate and the House and signed by the President on October 26, 2001. But, to describe the Act as a rash response to a horrific attack would be a mistake. Many of the provisions in the Act had been the subject of deliberation for years. The provisions were enacted with an acute awareness of rights guaranteed by the Constitution and applicable judicial precedents. The USA PATRIOT Act reflected a careful balancing of national security and the privacy rights of U.S. persons.

Nonetheless, some of the more important provisions in the Act were passed subject to a "sunset" provision. Sixteen provisions in the Act—and the recently enacted "lone wolf" amendment to the Foreign Intelligence Surveillance Act—will expire on December 31, 2005.

The danger posed by terrorism and other national security threats, however, will not expire on that date.

Today, the Senate Select Committee on Intelligence continues its on-going oversight of the USA PATRIOT Act. This open hearing will be the first in a series of three hearings designed to educate Members and the public as the Senate considers the repeal of the "sunset" provision and modifications to other intelligence authorities. On Thursday, the Committee will hold a closed hearing on operational matters relating to the Act. Next Wednesday, we will hear from the Attorney General, Director of the Federal Bureau of Investigation, and the Director of Central Intelligence.

This is not the Committee's first review of the USA PATRIOT Act or the Foreign Intelligence Surveillance Act, also known as FISA. The Committee regularly holds hearings, conducts briefings, and receives information regarding the activities of the Intelligence Community. The Committee conducted a closed hearing on the USA PATRIOT Act during the last Congress. We receive detailed reports from the Department of Justice every 6 months regarding FISA collection and annual reports on the use of other surveillance tools.

The Committee is also in the final stages of completing its second audit of the procedures, practices, and use of FISA. This comprehensive, classified analysis will represent one of the most thorough reviews of Executive branch activities under FISA since the USA PATRIOT Act was enacted.

Today, we have invited a panel of outside experts to provide their views of the USA PATRIOT Act and their opinions on those provisions of the Act that will expire later this year.

Our witnesses are: Mr. Gregory T. Nojeim, Associate Director and Chief Legislative Counsel for the American Civil Liberties Union; Mr. Jim Dempsey, Executive Director of the Center for Democracy and Technology; and Ms. Heather Mac Donald, a John M. Olin fellow at the Manhattan Institute. The Committee thanks all of our witnesses for being here today.

We have also received testimony and submissions for the record from: The Honorable Bob Barr, former Congressman from Georgia; Former Attorney General Edwin Meese III, and Paul Rosenszweig (RO-zen-swayg) of the Heritage Foundation; Associate Professor Orin S. Kerr of the George Washington University Law School; and Ms. Kate Martin, Director of the Center for National Security Studies.

Without objection, the submissions from these commentators will be entered into the record.

Before I recognize the Vice Chairman, I want to set out some fundamental principles that will inform my consideration of the USA PATRIOT Act reauthorization and any other modifications to law or policy governing intelligence activities.

First, our intelligence agencies need flexible authorities to confront terrorists, spies, proliferators, and other national security threats.

Second, as we seek to protect national security, we must also ensure that civil liberties and privacy are not sacrificed in the process. This is not a zero-sum game, however. As former Supreme Court Justice Arthur Goldberg noted, "While the Constitution protects against invasions of individual rights, it is not a suicide pact."

Third, these are not matters of "first impression." Interpreting the Constitution and the President's responsibility to protect national security, Federal courts have wrestled with many of these issues before. They have recognized the authority of the President to conduct warrantless electronic surveillance of foreign powers and their agents. Well-established judicial precedents also make clear that certain records—even of the most private information—lose their Constitutional protection when voluntarily exposed publicly or to a business or other third party.

Finally, I will support reasonable modifications to USA PATRIOT Act provisions or other authorities that clarify legal uncertainties, but I will oppose modifications that place *unnecessary* hurdles in the path of lawful intelligence investigations.

I would like to note one particular example of an authority that has been questioned by some in the context of the USA PATRIOT Act.

Everyday, we expose our personal information to businesses—when we buy milk from the grocery store with a credit card; when we open an e-mail account over the Internet; when we apply for a mortgage. This information we have voluntarily exposed to others is no longer private. Federal courts have clearly established that this record trail is not "protected" by the warrant requirement of the Fourth Amendment.

I have said before, that the 9/11 hijackers conducted numerous transactions while living within the United States. It should not be surprising that the records of these transactions would have been useful to the Intelligence Community before the attacks. Records from flight schools, cell phone companies, rental car dealers, or internet service providers might have revealed crucial information about the activities of these terrorists.

To gain access to these types of transactional records, the FBI uses a FISA "business records" order. A FISA "business records" order allows the FBI to access records for investigations of international terrorists and spies.

Before the USA PATRIOT Act, the authority to access "business records" under FISA was limited to certain types of business—like storage facilities, rental car companies, airlines, hotels, and the like. Section 215 of the USA PATRIOT Act expanded the types of entities that were subject to a FISA "business records" order and the types of items that could be sought with such an order.

Armed with a FISA "business records" order, the FBI can now go to a flight school to ask for records about a student they believe to be a terrorist. They can ask an internet service provider for the subscriber information of a possible spy. They can ask for transactional records from a fertilizer company, a chemical company, and a car dealership if those records will support an investigation to stop a car bomb attack by al Qaeda.

Libraries, booksellers, and others have raised great concern about this provision.

In law enforcement investigations, the government can obtain the *same types of records*—from all types of businesses, including libraries and bookstores—with a grand jury subpoena. These subpoenas are issued *without* a court order and are subject to judicial review only *after* they are issued.

A FISA "business records" order—on the other hand—can be issued *only upon the approval of a Federal Judge* serving on the Foreign Intelligence Surveillance Court. The judge can direct the FBI to modify the scope of the order. No similar preissuance review exists in the context of grand jury subpoenas.

Still, there is concern that the provision infringes privacy interests.

A FISA "business records" order also CANNOT be sought if the investigation is based solely on activities protected by the First Amendment. This prohibition dovetails with existing restrictions in Executive Order 12333 on the collection of foreign intelligence concerning the domestic activities of U.S. persons.

Finally, I note that the FISA "business records" provision is a relatively non-intrusive means of collecting intelligence for a national security investigation. Analysis of these business records can help solidify investigative leads or clear innocent names before more intrusive FISA techniques such as electronic surveillance or physical search are ever employed.

And, there are limitations in the USA PATRIOT Act, along with requirements for judicial review, the Congressional reporting obligations, and the prohibitions in Executive Order 12333.

While I recognize that some clarifying modifications to Section 215 may be necessary, I will oppose modifications that increase the standard for an order above "relevance" or place unreasonable barriers between these business records and intelligence officials.

Section 215 is just one example of the numerous tools that the USA PATRIOT Act provided to the men and women protecting us from further attack. These tools are currently helping our intelligence agencies identify terrorists, track their movements, and disrupt their plots. The provisions are subject to review by courts and the oversight of Congress.

Those provisions of the USA PATRIOT Act subject to expiration at the end of the year must be reauthorized. The alternative is a return to failed, outdated, and illogical limits on national security investigations that tied our hands prior to the 9/11 attacks. The dangers are real, and we should give our people every Constitutional tool available to fight and defeat terrorism.

I now recognize the Vice Chairman for any remarks he might wish to make.

Chairman ROBERTS. We also received testimony and submissions for the record from the Honorable Bob Barr, the former Congressman from Georgia; former Attorney General Ed Meese and Paul Rosenzweig of the Heritage Foundation; Associate Professor Orin S. Kerr of the George Washington University Law School; and Ms. Kate Martin, the Director of the Center for National Security Studies.

Without objection, the submissions from these commentators will be entered into the record.

[The prepared statements referred to follow:]

PREPARED STATEMENT OF BOB BARR

Chairman Roberts, Ranking Member Rockefeller, distinguished members of the Select Committee, I thank you for the invitation to present my views in this written statement on the debate over the PATRIOT Act "sunset" provisions, and I applaud your oversight on this crucial matter.

My name is Bob Barr. From 1995 to 2003, I had the honor to represent Georgia's Seventh District in the U.S. House of Representatives, serving that entire period on the House Judiciary Committee. From 1986 to 1990, I served as the United States Attorney for the Northern District of Georgia after being nominated by President Ronald Reagan, and was thereafter the president of the Southeastern Legal Foundation. For much of the 1970's, I was an official with the CIA.

I currently serve as CEO and President of Liberty Strategies, LLC, and *Of Counsel* with the Law Offices of Edwin Marger. I also hold the 21st Century Liberties Chair for Freedom and Privacy at the American Conservative Union, consult on privacy issues with the American Civil Liberties Union, and am a board member of the National Rifle Association.

Finally, I am the Chairman of a new network of primarily conservative organizations called Patriots to Restore Checks and Balances, which includes the American Conservative Union, Eagle Forum, Americans for Tax Reform, the American Civil Liberties Union, Gun Owners of America, the Second Amendment Foundation, the Libertarian Party, the Association of American Physicians and Surgeons, and the Free Congress Foundation.

We strongly urge Congress to resist calls to summarily remove the sunset provisions in the PATRIOT Act. This reflects our philosophy in support of all necessary and constitutional powers with which to fight acts of terrorism, but against the centralization of undue authority in any one aim or agency of government.

As I have said many times before, I believe the current struggle to properly integrate our shared constitutional heritage into our efforts to provide for the common defense, is the defining debate of our time. If we fail to strike the appropriate balance, we will do irreparable harm to our most elemental principles as a nation.

To that end, I urge this Committee to carefully examine the current language of the 2001 USA PATRIOT Act, and to make modest modifications to a handful of its provisions. In particular, I strongly urge individual members to co-sponsor Senator Larry Craig's Security and Freedom Enhancement Act of 2005, known as the SAFE Act. Although in many respects, this legislation does not address all of our concerns with the USA PATRIOT Act, it is an essential first step.

Even though I voted for the USA PATRIOT Act in October 2001, as did many of my colleagues, I did so with the understanding it was an extraordinary measure for an extraordinary threat; that it would be used exclusively, or at least primarily, in the context of important antiterrorism cases; and that the Department of Justice would be cautious in its implementation and forthcoming in providing information on its use to the Congress and the American people.

I have become skeptical on all of these fronts.

First, the Justice Department has been quite frank in its use and desire to use the USA PATRIOT Act in *non-terrorism* contexts. Second, the administration has repeatedly stated its intention to expand the USA PATRIOT Act, and has floated various pieces of legislation that would do so.

And, third, although this Committee would be in the best position to judge, the Justice Department has not produced any compelling evidence that the USA PATRIOT Act has been essential in preventing al Qaeda-style terrorist plots. Although I grant we have not suffered another major terrorist attack since 9/11, as Homeland Security Secretary Michael Chertoff put it, "[i]t's like sprinkling powder to keep away elephants. If no elephants show up, how do you prove it's because of the powder, rather than because there were never any elephants?" [1]

Before I specifically discuss those provisions of the USA PATRIOT Act most pertinent to this Committee's jurisdiction, I would like to bring two new developments in the "sunsets" debate to the Committee's attention. Namely, we learned earlier this month that both the USA PATRIOT Act appears to have been used in the Brandon Mayfield affair, and that the Administration is increasingly turning to it for its surveillance needs.

The Mayfield revelation is particularly disturbing. Mayfield—the Oregon lawyer turned prime suspect in the Madrid bombing investigation because of faulty fingerprint analysis at the FBI—was subjected to a highly intrusive Federal investigation and then detained as a "material witness" for 2 weeks before finally being exonerated.

According to Attorney General Gonzales, the FBI used the USA PATRIOT Act when it executed a covert search of Mayfield's home. Specifically, the attorney general said that Section 207 was used to extend the duration of Mayfield's surveillance, and that "in some sense" Section 218, which made it easier to use intelligence authorities in criminal contexts, was used.

We all fully understand the FBI is not perfect and generally support the bureau even when it makes honest mistakes.

However, the Mayfield case shows how the USA PATRIOT Act, by lessening meaningful judicial oversight, reduces the ability of the FBI and Justice Department to avoid such mistakes. In particular, it shows how—through the increased use of classified and less exacting foreign intelligence surveillance authority in place of traditional criminal warrants based on probable cause and executed in the open—the USA PATRIOT Act can compound mistakes and amplify them into serious deprivations of an innocent person's personal liberty.

In Mayfield's case, not only was a U.S. citizen detained, but his home was subjected to a "black bag" intelligence search even though the Justice Departillent was arguably conducting this search primarily for criminal purposes; in other words, in order to apprehend a suspect in a terrorist bombing that had already taken place. Such a foreign intelligence search is even more intrusive than the criminal "sneak and peek" search warrants available under section 213 of the USA PATRIOT Act, because notice is not simply delayed, it is never provided. The *Washington Post* reported that in a March 24th letter to Mayfield, the Justice Department acknowledged that during a covert search of his home, agents copied computer and paper files, took 355 digital photographs, seized six cigarette butts for DNA analysis, and used cotton swabs to obtain other DNA evidence.

In short, the Mayfield case should serve as a cautionary tale of how the USA PATRIOT Act can seriously exacerbate any "broken telephone" effect in an ongoing investigation.

I would also say, especially to Senators Hatch and Feinstein, that this is the type of problem that supporters of increased checks and balances refer to when discussing so-called "PATRIOT Act abuses." No one is of the mind that the FBI would

[1] Stephen Brill, After: How America Confronted the September 12 Era 348 (2003).

deliberately seek to infringe on the rights of loyal, law-abiding Americans. But there need be no malice aforethought for something to constitute an "abuse." The fact is, procedural deficiencies in the law's implementation likely led to Mayfield's predicament, and Mayfield was an innocent man.

Put another way, sometimes the road to abuse is paved with good intentions. Take, for instance, the Racketeer Influenced and Corrupt Organizations, or RICO, Act, which was passed to provide tools to fight organized crime, but was then used against pro-life groups. Overbroad laws are necessarily subject to overbroad application, if not now, then under future administrations, including those with less regard for civil liberties. That in itself can be deemed "abusive."

The second consideration—that the USA PATRIOT Act is becoming an ever more popular tool for the Justice Department—should be of particular concern to limited government conservatives like myself. As with taxes, unduly expanded government authority is next to impossible to retract.

As an illustration, I would point the Committee to the Attorney General's statement that, to date, Section 215 of the USA PATRIOT Act has been used 35 times. Note, however, that former Attorney General John Ashcroft declassified a memorandum to FBI Director Robert Mueller in September 2003 saying that Section 215 had *never* been used, meaning that those 35 court orders have all been issued in just the last year-and-a-half.

Granted, three dozen court orders may be considered by some to be a drop in the ocean of foreign intelligence document-production orders. Clearly, however, the trend is toward increased, not decreased, use of the USA PATRIOT Act; and, given the reach of the statute, the increased enthusiasm for its use ought to sound alarms.

Similarly, on the eve of the recent, April 6th Senate Judiciary Committee hearing, the Justice Department released statistics disclosing the use to date of Section 213 of the PATRIOT Act—the so-called "sneak and peek" provision that grants statutory authorization for the indefinite delay of criminal search warrant notification.

Apparently, the department sought and received the authority to delay notice 108 times between April 2003 and January 2005, a period of approximately 22 months. By contrast, it sought and received this authority 47 times between November 2001, when the PATRIOT Act was enacted, and April 2003, a period of about 17 months. The 5-month difference in timeframe aside, these numbers clearly reveal a substantial increase in use.

Moreover, Senator Arlen Specter at the April 6th Judiciary Committee hearing also revealed that 92—or approximately 60 percent—of those 155 requests were granted under the broad justification that notice would have the result of "seriously jeopardizing an investigation," rather than under the more specific criteria that notice would endanger a person's life, imperil evidence, induce flight from prosecution or lead to witness tampering.

While I understand the jurisdiction of this Committee is concerned primarily with foreign intelligence authorities, not with criminal "sneak and peek" warrants, I respectfully submit that you should be concerned when criminal investigative powers are made so broad that they come to resemble powers associated with foreign intelligence investigations. As Attorney General Gonzales informed Representative Flake at an April 7th hearing of the House Judiciary Committee, six criminal delayed-notice warrants under section 213 of the PATRIOT Act were approved with an *indefinite* delay (just as we had feared), and one had a delay that lasted fully half a year.

Lengthy, secret surveillance, including secret "black bag" jobs (all undertaken, since 1978, with the proper approval of the Foreign Intelligence Surveillance Court, of course) have long been the hallmark of a specialized, but crucial, type of investigation—the foreign intelligence investigation of suspected spies and international terrorists—the members of this Committee understand better than anyone. When these intrusive powers, such as the power to enter a home without notifying the owner, become more common in criminal or other types of investigations, the American people become alarmed. The resulting furor risks more draconian limits on all such secret surveillance powers—even in the investigations where they may actually be needed.

Although I acknowledge the Justice Departtnent's argument that Section 213 and 215 searches and surveillance represent only a fraction of the searches and surveillance conducted by the FBI and other security agencies, I remain concerned. These are extraordinary authorities and they are being used more frequently, and more and more outside their proper context of foreign intelligence and terrorism investigations. Any hint of such a trend should be very worrisome.

Furthermore, I would point the committee's attention to an April 1, 2005 Associated Press story on a recent report to Congress by the Assistant Attorney General for Legislative Affairs, William E. Moschella, disclosing the record number of For-

eign Intelligence Surveillance Act, or FISA, wiretaps in 2004. The department requested and won approval of 1,754 FISA wiretaps in 2004, up from 1,724 in 2003.

Although the marginal increase between 2003 and 2004 is small, the numbers still represent a 70 percent jump over the number obtained in 2000. In 2003, moreover, the use of intelligence wiretaps outstripped that of normal criminal wiretaps for the first time in history. One can only presume that the same trend continued in 2004.

The USA PATRIOT Act is directly relevant to the increased use of these intelligence wiretaps, as a number of provisions in the law made these wiretaps more intrusive and much easier to obtain outside of terrorism or espionage investigations. Section 218, for instance, which is set to sunset this year, now requires the investigation of foreign intelligence or terrorism to be a "significant purpose," rather than the primary purpose, of the intelligence wiretap.

Bearing these two new developments—the Mayfield revelations and the increased use of the PATRIOT Act—in mind, I urge the Intelligence Committee to look at three provisions that are of particular importance to your oversight mandate.

These are Sections 206, 215 and 505, which, respectively, created "roving wiretap" authority under FISA, expanded the government's ability to seize personal records and other materials under foreign intelligence authorities, and finally removed the required "nexus" to foreign powers for the specific targets of FBI "National Security letter" subpoenas.

First, when Congress created foreign intelligence roving wiretap authority in the USA PATRIOT Act, it failed to include the checks against abuse present in the analogous criminal statute. This is troubling because, as roving wiretaps attach to the target of the surveillance and not to the individual communications device, they provide a far more extensive and intrusive record of a person's communications.

Accordingly, criminal roving wiretaps require agents to "ascertain" that the target, rather than a third-party, is in fact using the telephone before they begin recording. They also require that, if the FBI does not actually know the identity (or an alias) of the target, but knows that he or she will be using a particular phone, the wiretap can attach to a single phone and all its users.

In creating roving wiretap authority under FISA, the USA PATRIOT Act did away with this ascertainment requirement. Then, shortly thereafter, the intelligence authorization bill for FY 2002 took away the requirement that the applicant specify either the identity of the target *or* the particular communications device.

The result, today, is a "John Doe" general warrant, issued secretly under FISA, that permits electronic surveillance irrespective of the communications device being tapped or the person being eavesdropped on.

The Justice Department has defended the open-ended nature of these "John Doe" wiretaps, by pointing to the requirement that they provide the FISA court with a physical description of the target if it cannot identify the communications device or target. Critics question how much of a safeguard this description requirement is in practice, given the paucity of identifying information it requires. In recognition of the oversight authority and security clearance of this Committee, I would urge its members to inquire on this point at length.

In addition, I would urge the Committee to tighten the roving wiretap authority to prevent anonymous or dragnet wiretapping, and to use the internal safeguards in the criminal roving wiretap statute as a model. At the very least, a judge authorizing a roving wiretap should have some assurance that (a) an innocent bystander's sensitive communications are protected, and (b) the court order is not an effective *general warrant* to be filled in later.

To that end, Senator Craig's SAFE Act would restore the ascertainment requirement and mandate that an FBI applicant for a national security roving wiretap specify *either* the actual target (or an alias) or the communications device to be tapped. This would, I believe, reserve for the government power that is more than sufficiently flexible to meet the demands of modern anti-terrorism and other anti-criminal investigations, over and above that of pre-PATRIOT Act authorities.

Next, I would urge the committee to carefully review the use and utility of Section 215, the USA PATRIOT Act's amendment to what was special authority under FISA to seize rental car, self-storage and airline records for national security investigations.

Prior to the USA PATRIOT Act, the underlying statute applied to only a limited subset of businesses, and it required a showing of "specific and articulable facts" that the target was an agent of a foreign power. The 2001 Act removed both these limitations, thereby greatly expanding the power of the government to reach to all "tangible things" (including books, records, papers, documents and other items), and lowering the evidentiary standard below that of standard, grand jury subpoenas which are pegged to at least some showing of relevance to criminal action by a *par-*

ticular person in an ongoing international terrorism or foreign intelligence investigation. .

Some have questioned why the section 215 power has become known as the "library provision," when libraries were not mentioned and given that it covers so much beyond library records or other information maintained by libraries. The answer is simple. Prior to the USA PATRIOT Act, library and bookseller records were not covered by this power, which then only permitted an order for the records of certain business. Now, library records *are* covered—as are all *other* records and tangible items, including membership lists of political organizations, gun purchase records, medical records, genetic information, and the list goes on.

Section 215 also comes with a sweeping gag order, without any explicit provision for a recipient to even consult with counsel; and if certification is made that the records are sought for any intelligence or terrorism inquiry, the judge has *no* power under the law to challenge that certification. Finally, and crucially, this is not like a grand jury subpoena, because a recipient has no explicit right to move to have it quashed in court, and failure to comply with a 215 order is presumably a serious offense.

Accordingly, critics of this section rightly charge that its open-ended scope and lack of meaningful judicial review open the door to abuses, and I agree. At the very least, Congress must restore the particularity requirement for the target of a Section 215 order, and should institute additional reporting requirements (subject, of course, to appropriate classification measures). Here again, such a modest limitation, consistent with traditional Fourth Amendment principles, would pose no significant hardship to Federal agents. Federal judges would, as they have for ages past, continue to approve virtually all such applications properly supported and applied for by government agents.

The SAFE Act, among other new procedural safeguards, would restore the specific and articulable facts standard and provide a recipient with at least some outlet to challenge an unreasonable order. It would also require notice before any information seized pursuant to Section 215 of the USA PATRIOT Act is introduced as evidence in any subsequent proceeding. These are "burdens" the government has always been able to meet and which have never been seen as any real impediment to the government's ability to secure necessary evidence.

I welcome the Attorney General's recent statements, agreeing to some changes to Section 215 that would make explicit a recipient's right to challenge the order and the secrecy provision, and would make explicit a recipient's right to consult an attorney. The Attorney General is certainly right to agree to changes in this poorly drafted provision, but, unfortunately, it remains unclear that the Administration will agree to a standard for a Section 215 order (individual suspicion) that will truly protect privacy. I strongly urge you to adopt the SAFE Act's standard in this regard.

Finally, I would urge the Committee to review Section 505 of the USA PATRIOT Act, which removed the requirement that the FBI self-certify that it has "specific and articulable facts" that the individual target of an administrative subpoena or "national security letter" (NSL), is an agent of a foreign power.

Prior to the USA PATRIOT Act, the FBI could use NSLs, which serve as non-judicial subpoenas issued at the sole discretion of the FBI, to demand business, Internet, credit and telephony records, among other things. Before doing so, agents had to at least certify internally that the NSL pertained to a particular individual, who was acting on behalf of a foreign power.

The USA PATRIOT Act effectively allows the FBI to issue NSLs for certain financial, transactional, electronic communications and credit records without *any* individualized suspicion. It changed the standard again to relevance to any investigation. The SAFE Act treats NSLs much like it does Section 215 orders—it maintains the expansive scope of the law, but includes the appropriate, minimal standard of individual suspicion; provides an explicit right to challenge the order; and retains the secrecy requirement, all of which take into account the sensitivity of national security investigations without taking away any necessary government powers.

In short, the SAFE Act simply modifies the powers expanded by the USA PATRIOT Act, by making the government's exercise thereof subject to the basic Fourth Amendment notion that before the government "pierces" an individual's right to privacy of information that can be used as evidence against them, it must have a reasonable suspicion that the person has either violated the law or is serving as an agent of a foreign power. The government has not shown any reason why it cannot meet such a nominal burden, and the Fourth Amendment requires it do so.

I believe, especially given that NSLs currently have no judge in the picture at all, that the SAFE Act's approach is entirely appropriate.

The committee should also note that Section 505(a) of the USA PATRIOT Act has been at the center of an ongoing bit of confusion about a 2004 court decision dealing

with NSLs and whether that court decision involved the 2001 Act or some other law. If I may, I would like to take this opportunity to make sure the record is accurate.

In September 2004, Judge Victor Marrero of the United States District Court for the Southern District of New York issued a 50-page ruling in the case of *Doe* v. *Ashcroft*, 334 F.Supp.2d 471 (S.D.N.Y. 2004). In it, he struck down 18 U.S.C. § 2709, the statute permitting the issuance of NSLs for customer records from Internet, telephone and other electronic service providers.

The judge struck the provision in its entirety, including the amendments made by Section 505(a) of the PATRIOT Act. Accordingly, the judge's decision struck down all of Section 505(a) of the PATRIOT Act, but also struck down the rest of the NSL statute with it.[2]

The judge ruled on two primary grounds—that the Section 2709 NSL is unreviewable, and that the attached gag order forever barred a recipient from telling anyone anything about the NSL. As the judge noted repeatedly in his opinion, the USA PATRIOT Act did remove the requirement of individual suspicion from the statute. For instance, he rests a large part of his First Amendment findings on the FBI's post-PATRIOT Act ability to suppress anonymous speech using an NSL.

Judge Marrero proffers two hypotheticals on that score, neither of which would have been possible prior to the USA PATRIOT Act unless the FBI had specific facts that the individual target was an agent of a foreign power. The FBI could use an NSL, the judge notes, to disclose the identity of an anonymous "blogger" critical of the government, or to discover the identity of everyone who has an e-mail account through a political campaign.

A number of lawmakers and other interested parties continue to claim, however, that *Doe* v. *Ashcroft* did not strike down a provision of the USA PATRIOT Act because Section 2709, prior to the Act, did not contain a right to challenge and contained a gag order. This is simply not true. First, whenever a statute is struck down in its entirety any then-operative amendments are also rendered unconstitutional. It is hard to see how a decision that strikes down every word of one section of a law can be said not to "involve" that law. Second, the USA PATRIOT Act is the 800-pound gorilla in the Marrero opinion, and clearly factored into his reasoning.

In sum, then, I urge the Committee to take into account the recent developments in the USA PATRIOT Act debate, most notably the Mayfield revelations and the indications that the Justice Department is turning to the PATRIOT Act more and more.

I also respectfully ask that the Committee look closely at the three most contentious PATRIOT Act amendments to foreign intelligence law—Sections 206, 215 and 505—and urge individual members to co-sponsor S. 737, the Security and Freedom Enhancement Act of 2005, which already enjoys bipartisan support.

As evidenced by the circumstances surrounding the founding of this very Committee, foreign intelligence law, especially as it applies domestically, poses serious risks to basic constitutional freedoms. While some hail the provisions in the USA PATRIOT Act as breaking down an artificial "wall" or a "technicality" between the gathering and use of evidence in criminal cases—matters necessarily subject to the Bill of Rights—and the gathering of foreign intelligence—appropriately not subject in its gathering to the limitations in the Bill of Rights—the fact is the artificial "wall" that applied different standards to the gathering and use of each category of information, is neither artificial nor a technicality: it is the Constitution of the United States of America. In treating them as one and the same in the name of fighting "terrorism" or any other threat posed to the good order and safety of our society, we show disdain for the fundamental underpinning of our constitutional form of government and the freedoms it enshrines.

Doing otherwise will result in an historical pattern where such laws are made ever more secret, ever more unchecked and ever more susceptible to abuse; and each subsequent national "crisis" forces the shades drawn tighter. It is a slippery slope, down which this Committee, this year in consideration of whether to sunset certain provisions in the USA PATRIOT Act and in deciding whether to place very modest and limited—but fundamentally important—restraints on some of the law's provisions, can help avoid.

Thank you again for this opportunity to comment on the vitally important deliberations of this Committee. I remain available to provide whatever further information the Committee might request.

---

[2] Judge Marrero's decision did not affect the rest of Section 505, which amended a number of different statutes that permit the FBI to issue NSLs for the production of other kinds of records.

THE HERITAGE FOUNDATION,
Washington, DC, April 18, 2005.

Hon. PAT ROBERTS, *Chairman,*
Senate Select Committee on Intelligence,
Senate Hart Office Bldg.,
Washington, DC.

Hon. JOHN D. ROCKEFELLER IV, *Vice Chairman,*
Senate Select Committee on on Intelligence,
Senate Hart Office Bldg.,
Washington, DC.

DEAR CHAIRMAN ROBERTS AND VICE CHAIRMAN ROCKEFELLER: We understand that the Senate Select Committee on Intelligence will be conducting an oversight hearing on April 19th concerning the reauthorization of certain provisions of the Patriot Act. We write to provide you with our views concerning that question.

In general, our view is that too much of the debate has focused on the Act not as it truly is but as people perceive it to be. Most of the proposals for reform mistake the appearance of potential problems and abuse (the myth) with the reality of no abuse at all. To take but one example, the Inspector General for the Department of Justice has consistently reported that there have been no instances in which the Patriot Act has been invoked to infringe on civil rights or civil liberties. *See* Report to Congress on Implementation of Section 1001 of the USA Patriot Act (March 2005); *see also* "Report Finds No Abuses of Patriot Act," Wa. Post at A2 (Jan. 28, 2004).

Thus, while we acknowledge that any expansion of governmental power comes with the potential for abuse, that potential does not, in our judgment warrant hesitancy absent some evidence of real abuse. In short, the case for change has not been made.

The Heritage Foundation has conducted extensive research on the Patriot Act that provides greater detail on this subject. All of our research is summarized in a memorandum we published entitled "The Patriot Act and Related Provisions: The Heritage Foundation's Research" (*http://www.heritage.org/Research/HomelandDefense/wm612.cfm*).

Most saliently for the Committee's consideration we would respectfully call your attention to two separate publications that contain much of our substantive analysis (copies of which we enclose with this letter):

- Rosenzweig, Carafano & Kochems, eds. "The Patriot Act Reader," (also available at *http://www.heritage.org/Research/HomelandDefense/The-Patriot-Act-Reader.cfm)*
- Meese & Rosenzweig, "The SAFE Act Will Not Make Us Safer," (also available at *http://www.heritage.org/Research/HomelandDefense/lm10.cfm*)

We would ask that you make this letter and our publications a part of the record of the Committee's hearing. We thank you for the opportunity to share with you our views.

Sincerely yours,

EDWIN MEESE III,
Ronald Reagan Distinguished Fellow.

PAUL ROSENZWEIG,
Senior Legal Research Fellow.

Legal Memorandum

Published by The Heritage Foundation

No. 10
April 30, 2004

The SAFE Act Will Not Make Us Safer

Edwin Meese III and Paul Rosenzweig

The USA PATRIOT Act,[1] a law passed with overwhelming support in Congress immediately following the September 11 terrorist attacks, has been the subject of many recent attacks and criticisms.[2] Opponents argue that various provisions of the Patriot Act, and related laws and practices, have greatly infringed upon American liberties while failing to deal effectively with the threat of terrorism.

Criticism of the anti-terrorist campaign is not limited to the Patriot Act; many other aspects of the Bush Administration's domestic response to terrorism have come under fire. To some degree, the Patriot Act as conceived by the public is broader than its actual provisions. Its very name has come to serve as a symbol for all of the domestic anti-terrorist law enforcement actions. It has become a convenient shorthand formulation for all questions that have arisen since September 11 about the alleged conflict between civil liberty and national security.

But the Patriot Act is a real law, with real purposes and real provisions. Too much of the debate has focused on the Act not as it truly is but as people perceive it to be. Most of the proposals for reform mistake the appearance of potential problems and abuse (the myth) with the reality of no abuse at all[3]—and, thus, the case for change has not been made.

The Security and Freedom Ensured Act of 2003 (the "SAFE Act")[4] is emblematic of this trend. It purports to be based upon an assessment of the necessity for change, yet its major substantive provisions lack any factual basis for con-

Talking Points

- We cannot decide policy based upon an over-wrought sense of fear. Most of the steps proposed to combat terrorism were previously used to combat organized crime, and there is no evidence of any real abuse. No First Amendment liberties have been curtailed, no dissent or criticism suppressed.
- In reviewing our policies and planning for the future, we must be guided by the realization that this is not a zero-sum game. We can achieve both goals—liberty and security—to an appreciable degree.
- The key is empowering government to do the right things while exercising oversight to prevent the abuse of authority. So long as we keep a vigilant eye on police authority, so long as the federal courts remain open, and so long as the debate about governmental conduct is a vibrant part of the American dialogue, the risk of excessive encroachment on our fundamental liberties can be avoided.

This paper, in its entirety, can be found at:
www.heritage.org/research/homelanddefense/lm10.cfm

Produced by the Center for Legal and Judicial Studies

Published by The Heritage Foundation
214 Massachusetts Ave., NE
Washington, DC 20002–4999
(202) 546-4400 heritage.org

Nothing written here is to be construed as legal advice on any matter, as an attempt to create an attorney-client relationship, or as an attempt to aid or hinder the passage of any bill before Congress.

cluding that changes are necessary. Often the proposals rest on incomplete legal analysis and would make America's response to terrorism less effective. In the end, they appear to be little more than a political fig leaf, intended to allow politicians to assert that they have responded to the public will and "fixed" the Patriot Act.

But capitulating to hysteria is pandering, not leadership. The SAFE Act will not make America safer.

This paper addresses the three principal substantive provisions of the SAFE Act: Section 2, which would limit the use of roving wiretaps; Section 3, which would modify traditional authority to delay notification of a search; and Sections 4 and 5, which would limit the ability of law enforcement and intelligence authorities to secure business records relating to terrorist activity. Each of these proposed revisions is ill-conceived and ought, on the merits, to be rejected.[5]

Roving Wiretaps: a Useful Tool

Section 206 of the Patriot Act authorized the use of "roving wiretaps"—that is, wiretaps that follow an individual and are not tied to a specific telephone or location—in terrorism investigations. America's original electronic surveillance laws (the Foreign Intelligence Surveillance Act ("FISA") of 1978 and Title III of the Omnibus Crime Control Act of 1968)[6] stem from a time when phones were the only means of electronic communications and all phones were connected by hard wires to a single network.

Roving wiretaps have arisen over the past 20 years for use in the investigation of ordinary crimes (e.g., drug transactions or organized crime activities) because modern technologies (cell phones, BlackBerries, and Internet telephony) allow those seeking to evade detection the ability to change communications devices and locations at will. Section 2 of the SAFE Act would unwisely restrict the use of roving wiretaps in terrorism investigations.

Getting a FISA Warrant to Conduct Electronic Surveillance

To begin with, one must understand the general structure of laws governing when law enforcement or intelligence agents may secure authorization to conduct electronic surveillance relating to suspected foreign intelligence or terrorism activity. Title III (the statute governing electronic surveillance for domestic crime) allows a court to enter an order authorizing electronic surveillance if "there is probable cause for belief that an individ-

1. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107-56, 115 Stat. 272 (Oct. 26, 2001).

2. Typical of the public criticism was the recent resolution of the National League of Cites calling for repeal of various portions of the Patriot Act. *See* Audrey Hudson, "Cities in Revolt over Patriot Act," *Washington Times*, Jan. 5, 2004. A number of cities and municipalities have passed similar resolutions. *See, e.g.*, Jessica Garrison, "L.A. Takes Stand Against Patriot Act," L.A. Times at B4 (Jan. 22, 2004). Responding to these criticisms, President Bush has called for reauthorization of the Patriot Act. *See* State of the Union (Jan. 20, 2004) ("The terrorist threat will not expire on [a] schedule. Our law enforcement needs [the Patriot Act] to protect our citizens.").

3. The Inspector General for the Department of Justice has reported that there have been no instances in which the Patriot Act has been invoked to infringe on civil rights or civil liberties. *See* Report to Congress on Implementation of Section 1001 of the USA Patriot Act (Jan. 27, 2004); *see also* "Report Finds No Abuses of Patriot Act," *Washington Post* at A2 (Jan. 28, 2004). This is consistent with the conclusions of others. For example, at a Senate Judiciary Committee Hearing on the Patriot Act, Senator Joseph Biden (D-DE) said that "some measure of the criticism [of the Patriot Act] is both misinformed and overblown." His colleague, Senator Dianne Feinstein (D-CA) said: "I have never had a single abuse of the Patriot Act reported to me. My staff...asked [the ACLU] for instances of actual abuses. They...said they had none." Even the lone Senator to vote against the Patriot Act, Russ Feingold (D-WI), said that he "supported 90 percent of the Patriot Act" and that there is "too much confusion and misinformation" about the Act. *See* Senate Jud. Comm. Hrg. 108th Cong. 1st Sess. (Oct. 21, 2003). These views—from Senators outside the Administration and an internal watchdog—are at odds with the fears often expressed by the public.

4. *See* S. 1709 (108th Cong.). The SAFE Act is co-sponsored by Senators Craig (R-ID), Durbin (D-IL), Crapo (R-ID), Feingold (D-WI), Sununu (R-NH), Wyden (D-OR), and Bingaman (D-NM).

5. A more extensive version of portions of this paper will appear in Paul Rosenzweig, "Civil Liberty and the Response to Terrorism," 42 Duq. L. Rev. ___ (2004) (forthcoming). Material from the article is reprinted here with permission.

6. The FISA governs applications for electronic surveillance in matters relating to foreign intelligence, espionage, counterintelligence, and terrorism. Title III governs applications for electronic surveillance involving the investigation of domestic crimes.

ual is committing, has committed or is about to commit" one of a list of several specified crimes.[7]

FISA (the statute governing intelligence and terrorism surveillance) has a parallel requirement: A warrant may issue if there is probable cause to believe that the target of the surveillance is a foreign power or the agent of a foreign power.[8] FISA also requires that the government establish probable cause to believe that "each of the facilities or places at which the surveillance is directed is being used, or is about to be used" by the foreign power or the agent of the foreign power who is the target of surveillance.[9] FISA court warrants thus are issued by federal judges, upon a showing of probable cause, and describe the things to be seized with particularity—the traditional three-prong test for compliance with the warrant clause requirements of the Fourth Amendment.[10]

Thus, no one can argue that these FISA warrants violate the Constitution. To the contrary, as the Foreign Intelligence Surveillance Court of Review recently made clear, the FISA warrant structure is "a reasonable response based on a balance of the legitimate need of the government for foreign intelligence information to protect against national security threats with the protected rights of citizens."[11] This is so because, as the court recognized, there is a difference in the nature of "ordinary" criminal prosecution and that directed at foreign intelligence or terrorism crimes:

> The main purpose of ordinary criminal law is twofold: to punish the wrongdoer and to deter other persons in society from embarking on the same course. The government's concern with respect to foreign intelligence crimes, on the other hand, is overwhelmingly to stop or frustrate the immediate criminal activity.[12]

Roving Wiretaps and Section 206

Roving wiretaps (whether used in foreign intelligence or domestic criminal investigations) are, as noted, a response to changing technologies. Phones are no longer fixed in one place and can move across state borders at the speed of flight. Sophisticated terrorists and criminals can change phones and communications devices constantly in an attempt to thwart interception.

In response to these changes in technology, in 1986 Congress authorized a relaxation of the particularity requirement for the investigation of drug offenses.[13] Under the modified law, the authority to intercept an individual's electronic communication was tied only to the individual who was the suspect of criminal activity (and who was attempting to

7. *See* 18 U.S.C. §2518(3)(a). Thus, Title III wiretaps are not available at all for the investigation of many relatively trivial criminal offenses.

8. *See* 50 U.S.C. §1805(a)(3)(A). A "foreign power" includes both foreign governments and groups engaged in international terrorism. *See* 50 U.S.C. §1801(a)(1). The definition of an agent of a foreign power includes any person who "knowingly engages in clandestine intelligence gathering activities...which...involve or may involve a violation of the criminal statutes of the United States" or "knowingly engages in sabotage or international terrorism, or activities that are in preparation thereof." 50 U.S.C. §§1801(b)(2)(A), (C). International terrorism is, in turn, defined as "violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States...or that would be a criminal violation if committed within the jurisdiction of the United States." 50 U.S.C. §1801(c)(1). Thus, one of the great and enduring myths about FISA and the Patriot Act is that they allow electronic surveillance willy-nilly for non-criminal activity. For any non-espionage activity under investigation, connection to the violation of some underlying criminal law is required. The specter of unfettered investigation of political groups for non-criminal activity is a bogeyman argument unsupported by a realistic appraisal of the law.

9. *See* 50 U.S.C. §1805(a)(3)(B). Title III again has a parallel requirement: probable cause to believe that the facilities are being or will be used for the commission of a domestic criminal offense or are leased to, used by, or listed in the name of the individual suspected of committing the crime. *See* 18 U.S.C. §2518(3)(d).

10. For an articulation of this test, *see Dalia v. United States*, 441 U.S. 238, 255 (1979).

11. *In re Sealed Case*, 310 F.3d 717, 742 (Foreign Int. Surv. Ct. Rev. 2002).

12. *Id.* at 744.

13. In 1986, Congress added 18 U.S.C. §2518(11) to Title III, authorizing intercept without specification of the particular phone to be intercepted if the interceptee's actions "could have the effect of thwarting interception." *See* Pub. L. No. 99-508, §106(d)(3), 100 Stat 1851 (1986).

"thwart" surveillance) rather than to a particular communications device.[14]

Section 206 authorized the same techniques for foreign intelligence investigations. As the Department of Justice has noted:

> This provision has enhanced the government's ability to monitor sophisticated international terrorists and intelligence officers, who are trained to thwart surveillance by rapidly changing hotels, cell phones, and internet accounts, just before important meetings or communications.[15]

One important safeguard is that the FISA court may authorize such roving wiretaps only if it makes a finding as to the terrorist's actions—that "the actions of the target of the application may have the effect of thwarting the identification" of a terrorism suspect.[16]

The SAFE Act's Unnecessary Burden

The SAFE Act would modify the existing FISA requirements by, in effect, imposing an unreasonable and burdensome ascertainment requirement on law enforcement and intelligence agents. Under the Patriot Act, agents may seek authority for an interception even when the identity of the suspect is not known (so long as probable cause existed to believe the person involved was an agent of a foreign power). The SAFE Act would change that regime. If enacted, it would require agents seeking authority for a wiretap to specify the identity of the target and, if they were unable to do so, to describe with specificity the nature and location of the places where the interception would occur. In other words, in certain circumstances, intelligence agents would be unable to secure a warrant to conduct electronic surveillance because of the indefiniteness of their information.

The proposed modification of the Patriot Act misses the point completely—so much so that one doubts whether any of the authors is a serious student of either law enforcement or intelligence activity. To the extent the SAFE Act calls for specificity with respect to the precise location or facility where the communication is occurring, it is a *non sequitur*. Government agents use roving wiretaps *only* when the location or facility where the communication is occurring is not known with precision—for the simple reason that those under surveillance are attempting to thwart surveillance by constantly changing their location and means of communication. To call for specificity as to location imposes a higher burden on using roving wiretaps in terrorism investigations than in routine domestic criminal investigations.

The SAFE Act's proposal to require that the individual who is the subject of scrutiny be precisely identified is equally foolhardy. In a domestic investigation, the identity of the suspect under scrutiny may often be well-known, though drug dealers do, of course, use aliases. The problem becomes substantially more acute in the shadowy world of espionage and terrorism, where the identity of the investigative subject is often obscured behind a gauze of deceit.

Terrorists change their identity with frequency and often pose as other, real-world individuals. Often, the only description that the intelligence agency will be able to provide to identify the suspect is an alias (or several aliases). Sometimes the description of the terrorism suspect may be nothing more than a physical description. And, on still other occasions, it may consist only of a pattern of behavior (*i.e.*, the person who regularly uses this series of phones, in this order, every third day). To insist that intelligence and law enforcement agents precisely identify the individual under scrutiny or the facility he will be using is, in effect, to ban the use of roving wiretaps in terrorism investigations.

And that is the wrong answer—indeed, the SAFE Act reverses the proper analysis. It imposes a narrow law enforcement paradigm on the efforts to combat terrorism. That paradigm, however, no longer holds. Law enforcement efforts to combat terrorism are policing of a different form: preventative rather than reactive. There is little, if any, value in punishing terrorists after the fact, especially when, in some instances, they are willing to perish in the attack. Hewing to the traditional law enforcement paradigm

14. A number of courts have concluded that the particularity requirements of the Constitution are not violated when roving wiretaps are authorized. *See, e.g., United States v. Bianco*, 998 F.2d 1112 (2d Cir. 1993).

15. Department of Justice, *The USA Patriot Act: Myth vs. Reality* 3 (2003).

16. 50 U.S.C. §1805(c)(2)(B) (as amended by Section 206 of the Patriot Act).

of particularity in the context of terrorism investigations is a fundamental category mistake.

The traditional law enforcement model is highly protective of civil liberty in preference to physical security. All lawyers have heard one or another form of the maxim that "it is better that 10 guilty go free than that one innocent be mistakenly punished."[17] This embodies a fundamentally moral judgment that, when it comes to enforcing criminal law, American society, in effect, prefers to have many more Type II errors (false negatives) than it does Type I errors (false positives).[18] That preference arises, at least implicitly, from a comparative valuation of the social costs attending the two types of error. We value liberty sufficiently highly that we see a great cost in any Type I error. And, though we realize that Type II errors free the guilty to return to the general population, thereby imposing additional social costs on society, we have a common-sense understanding that those costs, while significant, are not so substantial that they threaten large numbers of citizens or core structural aspects of the American polity.

The post-September 11 world changes this calculus, principally by changing the cost of the Type II errors. Whatever the costs of freeing organized crime boss John Gotti or serial murderer John Mohammad might be, they are considered less than the potentially horrific costs of failing to stop the next al-Qaeda assault. Thus, the theoretical rights-protective construct under which our law enforcement system operates must, of necessity, be modified to meet the new reality. We simply cannot afford a rule that "better 10 terrorists be able to succeed in their attacks than that one innocent be mistakenly subject to surveillance."[19] The SAFE Act's proposal to impose a traditional law enforcement construct misses this point altogether.

Nor is there any practical necessity for the SAFE Act's proposed revisions. Though Section 206 has been the law of the land for more than two years, there have be *no* reported instances of abuse of this authority.[20] Whatever else may be said about the Patriot Act, even its most ardent critics must admit that they are basing their legislative proposals on fear rather than reality. But fear is not a basis for policymaking.

Searches and Seizures: Delayed Notification

One section of the Patriot Act that has engendered great criticism is Section 213, which authorizes the issuance of delayed notification search warrants—which critics call "sneak and peek" warrants. Section 3 of the SAFE Act would modify Section 213 by limiting the circumstances in which delayed notification warrants could be issued and by requiring burdensome, repetitive recertification requirements. Section 3 would also sunset (that is terminate) the provisions of Section 213 altogether on December 31, 2005.

Traditional Rules of Search and Seizure

Traditionally, when the courts have issued search warrants authorizing the government's forcible entry into a citizen's home or office, they have required that the searching officers provide contemporaneous notification of the search to the individual whose home or office has been entered.[21] Prior to September 11, some courts permitted limited delays in notification to the owner, when immediate notification

17. *E.g.*, *Furman v. Georgia*, 408 U.S. 238, 367 n. 158 (1972) (Marshall, J., concurring). The aphorism has its source in 4 Blackstone, Commentaries, ch. 27 at 358 (Wait & Co. 1907).

18. "In a criminal case...we do not view the social disutility of convicting an innocent man as equivalent to the disutility of acquitting someone who is guilty.... [T]he reasonable doubt standard is bottomed on a fundamental value determination of our society that it is far worse to convict an innocent man than to let a guilty man go free." *In re: Winship*, 397 U.S. 357, 372 (1970) (Harlan, J., concurring).

19. The closely related point, of course, is that we must guard against "mission creep." Since the justification for altering the traditional assessment of comparative risks is in part based upon the altered nature of the terrorist threat, we cannot alter that assessment and then apply it in the traditional contexts. *See* Paul Rosenzweig & Michael Scardaville, "The Need to Protect Civil Liberties While Combating Terrorism: Legal Principles and the Total Information Awareness Program," at 10–11, Legal Memorandum No. 6, The Heritage Foundation (February 2003) (arguing for use of new technology only to combat terrorism); William Stuntz, "Local Policing After the Terror," 111 Yale L. J. 2137, 2183-84 (2002) (arguing for use of information sharing only to combat most serious offenses).

20. *See supra* n. 3.

would hinder the ongoing investigation. Section 213 codifies that common law tradition and extends it to terrorism investigations. Critics see this extension as an unwarranted expansion of authority—but here, too, the fears of abuse seem to outstrip reality.

Delayed notification warrants are a long-existing crime-fighting tool upheld by courts nationwide for decades in organized crime, drug cases, and child pornography. For example, Mafia Don Nicky Scarfo maintained the records of his various criminal activities on a personal computer, protected by a highly sophisticated encryption technology. Law enforcement knew where the information was—and thus had ample probable cause to seize the computer. But the seizure would have been useless without a way of breaking the encryption. So, on a delayed notification warrant, the FBI surreptitiously placed a keystroke logger on Scarfo's computer. The logger recorded Scarfo's password, which the FBI then used to examine all of Scarfo's records of his various drug deals and murders.[22] It would, of course, have been fruitless for the FBI to have secured a warrant to enter Scarfo's home and place a logger on his computer if, at the same time, it had been obliged to notify Scarfo that it had done so.[23]

The courts have approved this common law use of delayed notification. Over 20 years ago, the Supreme Court held that the Fourth Amendment does not require law enforcement to give immediate notice of the execution of a search warrant. The Court emphasized "that covert entries are constitutional in some circumstances, at least if they are made pursuant to a warrant." In fact, the Court stated that an argument to the contrary was "frivolous."[24] In an earlier case—the seminal case defining the scope of privacy in contemporary America—the Court said that "officers need not announce their purpose before conducting an otherwise [duly] authorized search if such an announcement would provoke the escape of the suspect or the destruction of critical evidence."[25]

Section 213 Adopts the Traditional Standard

Section 213 of the Patriot Act thus attempts to codify the common law authority given to law enforcement for decades. As summarized by the Department of Justice:

> Because of differences between jurisdictions, the law was a mix of inconsistent standards that varied across the country. This lack of uniformity hindered complex terrorism cases. Section 213 resolved the problem by establishing a uniform statutory standard.[26]

Now, under Section 213, courts can delay notice if there is "reasonable cause" to believe that immediate notification may have a specified adverse result. The "reasonable cause" standard is consistent with pre-Patriot Act case law for delayed notice of warrants.[27] And the law goes further, defining "reasonable cause" for the issuance of a court order narrowly. Courts are, under Section 213, authorized to delay notice only when immediate notification may result in death or physical harm to an individual, flight from prosecution, evidence tampering, witness intimidation, or otherwise seriously jeopardize an investigation.

In short, Section 213 is really no change at all; it merely clarifies that a single uniform standard applies and that terrorist offenses are included. Nor does Sec-

21. The requirement has a long-standing provenance in common law. As the King's Bench court said in 1603: "In all cases where the King is a party, the sheriff...may break the party's house, either to arrest him, or to do execution of the King's process, if otherwise he cannot enter. But before he breaks it, he ought to signify the cause of his coming, and to make request to open the doors." *Semanyne's Case*, 5 Co. Rep. 91a, 77 Eng. Rep. 194 (K.B. 1603).

22. *United States v. Scarfo*, 180 FSupp.2d 572 (D.N.J. 2001).

23. The same, of course, is true of any surreptitious use of listening devices. It would have done little good for the FBI to secure a warrant to enter John Gotti's eating club in Brooklyn to place a recording device in the facility if it had been obliged, at the same time, to politely let Gotti know that he needed to speak clearly into the chandelier, as that was where the bug had been placed.

24. *Dalia v. U.S.*, 441 U.S. 238 (1979).

25. *Katz v. U.S.*, 389 U.S. 347 (1967).

26. Department of Justice, *The USA Patriot Act: Myth vs. Reality* 11 (2003).

27. *See, e.g., United States v. Villegas*, 899 F.2d 1324, 1337 (2d Cir. 1990) (government must show "good reason" for delayed notice of warrants).

tion 213 promise great abuse. Here, as in the past under common law, the officer seeking authority for delayed entry must get authorization for that action from a federal judge or magistrate—under the exact same standards and procedures that apply in getting a warrant to enter a building in the first place. And the law makes clear that in all cases law enforcement must ultimately give notice that property has been searched or seized. The only difference from a traditional search warrant is the temporary delay in providing notification. Here, the presence of oversight rules seems strong—certainly strong enough to prevent the abuse that some critics fear.[28]

Section 213 Has Aided the Fight Against Terrorism

Nor can it be doubted that the delayed notification standards have performed a useful function and are a critical aspect of the strategy of prevention—detecting and incapacitating terrorists *before* they are able to strike.

One example of the use of delayed notification involves the indictment of Dr. Rafil Dhafir. A delayed notification warrant allowed the surreptitious search of an airmail envelope containing records of overseas bank accounts used to ship over $4 million to Iraq. Because Dhafir did not know of the search, he was unable to flee and he did not move the funds before they were seized.[29] In another instance, the Justice Department described a hypothetical situation (based upon an actual case) in which the FBI secured access to the hard drive of terrorists who had sent their computer for repair. In still another, they were able to plant a surveillance device in a building used by terrorists as a safe house.[30]

The SAFE Act Would Needlessly Limit the Use of Delayed Notification Authority

The SAFE Act would make two significant changes to Section 213. First, it would limit the circumstances under which delayed notification would be allowed. Second, it would impose upon the Department of Justice the burden of seeking reauthorization for the delay every seven days, regardless of whether circumstances had changed. Neither change is merited.

The change in standards—limiting the use of delayed notification—is particularly pernicious. Under Section 213 (just as with wiretap or other electronic surveillance) delayed notice is appropriate only when immediate notification may result in:

- Death or physical harm to an individual,
- Flight from prosecution,
- Evidence tampering,
- Witness intimidation, or
- Otherwise seriously jeopardize an investigation.

The SAFE Act would delete this final catchall phrase because it is perceived as too broad and as providing too much leeway for Executive action. But this concern is overly cautious: One can imagine few circumstances in which an investigation would be "seriously jeopardized" that would not also satisfy one of the more specific listings of potential adverse consequences. And nobody disputes that those other consequences (flight, risk of harm, etc.) are appropriate grounds for delay.

Even worse, though, are logical implications of what the SAFE Act would do. Those who would adopt the SAFE Act and delete the catchall phrase are implicitly saying that they are willing to accept the frustration of legitimate investigations. If you advocate changing Section 213, you are advocating the view that, even if an Article III federal judge finds that an investigation *would* be seriously jeopardized without a delay, you will not allow a delay in notification to occur.

In other words, critics value the process of notification more highly than the substance of an impaired investigation. This reverses the more rea-

28. The Department of Justice has reported to Congress that the most common period of delay has been seven days. Delays as short as one day or as long as 90 have been authorized. On occasion, courts have permitted delays for an unspecified period of time lasting until an indictment was unsealed. *See* Letter, Janice E. Brown, Act'g Asst. Atty. Gen., to Hon. James Sensenbrener, Chrmn. House Jud. Comm., Attachment at 10 (May 12, 2003)

29. *See* Letter, William E. Moscella, Asst. Atty. Gen., to Hon. Dennis Hastert, Speaker, at 3 (July 25, 2003); *see also* AP, "Four Indicted for Sending Funds to Iraq" (Feb. 26, 2003) (available at *http://www.chron.com/cs/CDA/printstory.hts/special/iraq/1796320)*.

30. *See* Moscella, Letter to Hastert, at 4.

sonable evaluation of the comparative values, especially when the result is validated by an independent federal judge.

Thus, proponents of the SAFE Act misunderstand the true nature of the issues at stake. The purpose of the notice requirement is twofold: (1) In typical searches, it allows a contemporaneous objection. The individual may say, in effect, "You've got the wrong house." (2) Following notification, it also allows for non-contemporaneous objections to be heard in court so that overzealous execution of the warrant, or a search beyond the scope authorized, may be challenged before a judge.

But in the context of a surreptitious entry and delayed notification, the first of those purposes can have no force. Except by accident, law enforcement or intelligence agents will not conduct a delayed-notice entry in a manner that affords contemporaneous notification—to do so would frustrate the precise purpose of the delayed notification. So the *only* way to effect the first of these two purposes is to prohibit delayed notification entry altogether—a rule that would have very significant costs. And it is equally clear that the second purpose—allowing subsequent challenge in court—is served so long as the law requires (as Section 213 does) eventual notification in all circumstances. The only real argument that critics can make is that Section 213 imposes costs by virtue of the time for which the notification is delayed—a true cost but a comparatively minor one when balanced against the substantial benefits that the process of delayed notification allows in appropriate cases.

The evident utility of the potential uses of Section 213, the provision for subsequent review in court, and the absolute absence of any evidence of abuse of this power suggest that several proposed repeals under congressional consideration are unwise.[31] At worst, they would completely eliminate a long-standing investigative tool for all crimes—both terrorist crimes and traditional common law crimes. At best, the rejection of Section 213 would re-institute a dichotomy between traditional crimes and terrorist investigations—again, a mistaken one that oddly provides greater authority to investigate less threatening common law criminal acts.

Increased Investigative Authority and Business Records

Perhaps no provision of the Patriot Act has excited greater controversy than has Section 215, the so-called angry librarians provision. The section allows the Foreign Intelligence Surveillance Court in a foreign intelligence investigation to issue an order directing the recipient to produce tangible things.

The revised statutory authority in Section 215 is not wholly new. FISA has had authority for securing some forms of business records since its inception. The new statute modifies FISA's original business-records authority in a two important respects:

First, it "expands the types of entities that can be compelled to disclose information. Under the old provision, the FISA court could order the production of records only from 'a common carrier, public accommodation facility, physical storage facility or vehicle rental facility.' The new provision contains no such restrictions."

Second, the new law "expanded the types of items that can be requested. Under the old authority, the FBI could only seek 'records.' Now, the FBI can seek 'any tangible things (including books, records, papers, documents, and other items).'"[32]

Thus, the modifications made by Section 215 do not explicitly authorize the production of library records; but by its terms, it authorizes orders to require the production of virtually any business record. That might include library records, though it would include as well airline manifests, international banking transaction records, and purchase records of all sorts.

Critics of the Patriot Act have decried this provision.[33] As a consequence, Section 4 of the SAFE Act would limit the authority to seek records to those situations where the government can provide "specific and articulable facts" demonstrating that the person to whom the records pertain is the agent of a

31. Besides the SAFE Act itself, repeal proposals are also included in S. 1552 (108th Cong.) (introduced by Sen. Murkowski (R-AK)) and H. Amdt 292 to H.R. 2799 (108th Cong.) (introduced by Rep. Otter (R-ID)) (proposing to prohibit funds to carry out Section 213).

32. Department of Justice, *The USA Patriot Act: Myth vs. Reality* 16 (2003).

foreign power. Section 5 would exempt library Internet services from surveillance that could be carried out on any other Internet system. The proposals are, again, an overreaction to the perception of a problem, mistaking the potential for abuse for the reality.

Section 215 Adopts Traditional Law Enforcement Practices

Section 215 mirrors, in the intelligence-gathering context, the scope of authority that already exists in traditional law enforcement investigations. Obtaining business records is a long-standing law enforcement tactic. Ordinary grand juries for years have issued subpoenas to all manner of businesses, including libraries and bookstores, for records relevant to criminal inquiries.

For example, in the 1997 Gianni Versace murder case, a Florida grand jury subpoenaed records from public libraries in Miami Beach. Likewise, in the 1990 Zodiac gunman investigation, a New York grand jury subpoenaed records from a public library in Manhattan. Investigators believed that the gunman was inspired by a Scottish occult poet, and wanted to learn who had checked out books by that poet.[34] In the Unabomber investigation, law enforcement officials sought the records of various libraries, hoping to identify the Unabomber as a former student with particular reading interests.[35]

Section 215 merely authorizes the FISA court to issue similar orders in national-security investigations. It contains a number of safeguards that protect civil liberties.

First, Section 215 requires FBI agents to get a court order. Agents cannot compel any entity to turn over its records unless judicial authority has been obtained. FISA orders are *unlike* grand jury subpoenas, which are requested without court supervision and are subject to challenge only *after* they have been issued.

Second, Section 215 has a narrow scope. It can be used only (1) "to obtain foreign intelligence information not concerning a United States person" or (2) "to protect against international terrorism or clandestine intelligence activities." It cannot be used to investigate ordinary crimes, or even domestic terrorism. Nor can it be used in any investigation premised solely on "activities protected by the first amendment to the Constitution."[36]

This is narrower than the scope of traditional law enforcement investigations. Under general criminal law, the grand jury may seek the production of any relevant business records. The only limitation is that the subpoena may be quashed if the subpoena recipient can demonstrate that "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation."[37] There is no necessity of showing a connection to foreign intelligence activity nor any limitation against investigation of United States persons. Thus, unlike under Section 215, the grand

33. "Many [people] are unaware that their library habits could become the target of government surveillance. In a free society, such monitoring is odious and unnecessary.... The secrecy that surrounds section 215 leads us to a society where the 'thought police' can target us for what we choose to read or what Websites we visit." See ACLU, "ACLU of New Mexico Seeks to Protect Individual Privacy," Torch, ACLU–New Mexico, July–August 2003. The false image created is, as one writer has characterized it, of "white-haired and apple-cheeked [librarians] resisting as best they can the terrible forces of McCarthyism, evangelical Christian book-burning, middle-class hypocrisy, and Big Brother government." Joseph Bottum, "The Library Lie," The Weekly Standard 7 (Jan. 26, 2004). While politically appealing, the image simply does not match reality.

34. *See* "Patriot Acting Out," Wall St. J. (Jan. 22, 2004). The original source for this information is: *Myth vs. Reality* at 14.

35. *See* James Richardson and Cynthia Hubert, "Unabomber used library at UC Davis?" Sac. Bee (April 10, 1996) (available at *http://www.unabombertrial.com/archive/1996/041096-1.html*) (reporting that UC Davis library provided book to FBI with markings relating to Unabomber manifesto); *cf.* Patrick Hoge, "Rural acquaintances say Kaczynski attracted little notice," Sac. Bee. (April 5, 1996) (available at *http://www.unabombertrial.com/archive/1996/040596-2.html*) (reporting on Kaczynski's reading habits at library in Montana). Some courts have interpreted their State constitutions to provide a First Amendment protection that does not exist in federal law. *See, e.g., Tattered Cover Inc. v. City of Thornton*, 44 P.3d 1044 (Colo. 2002).

36. 50 U.S.C. §1861(2)(B).

37. *United States v. R. Enterprises*, 498 U.S. 292, 301 (1991).

jury may inquire into potential violations of any federal crime with effectively limitless authority.[38]

Criticism of Section 215 Is Misguided

Critics make two particular criticisms of this provision: that the judicial review it provides for is a chimera, and that the provision of Section 215 imposing secrecy on the recipients of subpoenas issued pursuant to the section imposes a "gag rule" that prevents oversight of the use of the section's authority. Neither criticism, however, withstands close scrutiny.

Section 215 provides for judicial review of the application for a subpoena for business records. The language provides, however, that upon application, the court "shall" issue the requested subpoena. From the use of the word "shall," critics infer that the obligation to issue the requested subpoena is mandatory and, thus, that the issuing court has no discretion to reject an application. Of course, if this were true (which, as discussed below, it is not), then the absence of any judicial ability to reject an application would reduce the extent of judicial oversight.

But critics who make this argument (even if it were the case) miss the second-order effects of judicial review. It imposes obligations of veracity on those seeking the subpoenas, and to premise an objection on the lack of judicial review is to presuppose the mendacity of the subpoena affiants. It is also to presuppose the absence of any internal, administrative mechanisms in order to check potential misuse of the subpoena authority. And, most notably, it presupposes that the obligation to swear an oath of truthfulness, with attendant perjury penalties for falsity, has no deterrent effect on the misuse of authorities granted.[39]

But even more significantly, this criticism misreads the statute, which, while saying that the subpoena "shall" issue, also says that it shall issue as sought or "as modified." The reviewing judge thus explicitly has authority to alter the scope and nature of the documents being sought—a power that cannot be exercised in the absence of substantive review of the subpoena request. Thus, the suggestion that the provisions of Section 215 preclude judicial review is simply mistaken. To the contrary, Section 215 authorizes judicial review and modification of the subpoena request which occurs before the subpoena is issued. This is a substantial improvement over the situation in traditional grand jury investigations where the subpoena is issued without judicial intervention and the review comes, at the end, only if the subpoena is challenged.

Nor is judicial oversight the only mechanism by which the use of Section 215 authority is monitored. The section expressly commands that the Attorney General "fully inform" Congress of how the section is being implemented. On October 17, 2002, the House Judiciary Committee, after reviewing the Attorney General's first report, indicated that it was satisfied with the Justice Department's use of Section 215: "The Committee's review of classified information related to FISA orders for tangible records, such as library records, has not given rise to any concern that the authority is being misused or abused."[40] If it were—if, for example, the Department were conducting investigations based upon the reading habits of suspects, in violation of the First Amendment—we can be sure that Congress would have said so. That it has not demonstrates that, once again, critics' fears far outpace reality.[41]

The second criticism—that Section 215 imposes an unwarranted gag rule—is equally unpersuasive. Sec-

38. A "United States person" is defined in Exec. Order 12333 part 3.4 as "a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States...."

39. For a similar point, *see* Daniel Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy," 75 S. Cal. L. Rev. 1083, 1124–28 (2002) (highlighting the significance of judicial oversight and warrant requirements in maintaining an "architecture of power" to protect privacy). Warrants raise the "standard of care of law enforcement officials by forcing them to document their requests for authorization" and the "requirement of prior approval prevents government officials from dreaming up post-hoc rationalizations." *Id.* at 1126–27. This provides an institutional/procedural check on abuse even if we assume that magistrates routinely defer to police and prosecutors.

40. *See* Statement of F. James Sensenbrenner, Jr. Chmn. House Jud. Comm (Oct. 17, 2002) (available at *http://www.house.gov/judiciary/news101702.htm*).

41. Indeed, they have ignored General George Patton's dictum: "Do not take counsel of your fears." *See* George S. Patton, Jr., *War as I Knew It* (Bantam 1989). Patton was repeating a sentiment originally attributed to General Stonewall Jackson.

tion 215 does prohibit recipients of subpoenas from disclosing that fact—a precaution that is necessary to avoid prematurely disclosing to the subjects of a terrorism investigation that they are subject to government scrutiny. That prohibition might be independently justified, given the grave nature of the potential threats being averted.

But it need not be—for, again, the secrecy provisions of Section 215 merely extend existing rules in traditional law enforcement grand juries to the more sensitive intelligence arena. In the grand jury context, it is common for custodians of third-party records to be prohibited from disclosing the existence of the document request. Banks, for example, may be obliged to conceal requests made to them.[42] And it is clear, beyond peradventure, that these grand jury secrecy obligations are constitutional. For example, when the nanny of JonBenet Ramsey was called to testify before a state grand jury, state law prohibited her from disclosing the substance of her testimony. When she challenged that law (on the ground that it infringed her freedom of speech), her challenge was rejected by the courts.[43]

The SAFE Act Would Hobble Section 215

The SAFE Act proposes to require a showing of "specific and articulable facts" before a Section 215 order may be issued. That showing would impose a greater obligation on law enforcement in an intelligence investigation than under the simple "relevance" standard that applies to federal grand juries investigating ordinary criminal offenses. The purpose of the non-intrusive records request is precisely to develop the specific and articulable facts that warrant a greater intrusion, for if specific and articulable facts to seek the records exist, police will have sufficient probable cause to execute a search warrant—and under warrant there is less possibility that the required records will be destroyed.

In other words, the balance between the standard and the degree of intrusion is a tradeoff: The lesser the standard law enforcement must meet, the lesser the intrusion permitted. By altering that balance, the SAFE Act will have the perverse effect of providing law enforcement with the incentive to prefer more intrusive means.

In short, critics of Section 215 make a very difficult and, in the end, unpersuasive argument. They offer the view, in effect, that traditional law enforcement powers that have been used in grand juries for years to investigate common law crimes and federal criminal offenses ought not to be used with equal authority to investigate potential terrorist threats. To many, that argument seems to precisely to reverse the evaluation—if anything, the powers used to investigate terrorism, espionage, and threats to national security ought to be greater than those used to investigate mere criminal behavior.[44]

This is not, of course, to denigrate the significance and seriousness of many federal and state crimes; but it is to recognize that, however grave those crimes are, they do not pose the same risk to the foundations of American society or to the security of large numbers of citizens as the risks posed by potential terrorist acts.

Consideration of Section 215 should be grounded in a solid understanding of what the section actually authorizes.[45] It should not be swayed by the public mythology that surrounds this provision. That myth has led to the rather absurd result that some librarians are destroying their borrowing records to prevent them from becoming available to the federal government.[46] In other words, those charged in our society with protecting and maintaining knowledge and information are destroying it. The interest in protecting civil liberties must be high—but not so high that we lapse into hysteria.[47]

Conclusion

The Patriot Act has become something of a political football in the past few months. One sees television commercials of anonymous hands ripping up

42. 12 U.S.C. §3604(c).

43. *Hoffmann-Pugh v. Keenan*, 338 F.3d 1136 10th Cir. 2003); *see also Hoffman-Pugh v. Ramsey*, 312 F.3d 1222 (11th Cir. 2002) (rejecting libel suit filed by nanny against the Ramsey family).

44. This view is not an idiosyncratic one. At the time the Patriot Act was passed, Senator Biden (D–DE) argued that "the FBI could get a wiretap to investigate the mafia, but they could not get one to investigate terrorists. To put it bluntly, that was crazy! What's good for the mob should be good for terrorists." Cong. Record at S11048 (Oct 25, 2001) (available at *http://www.lifeandliberty.gov/subs/support/senbiden102501_1.pdf*), *quoted in* Barbara Comstock, "Prez Calls Dems Patriot Games Bluff," Nat'l Review Online (Jan. 21, 2004) (available at *http://www.nationalreview.com/comment/comstock200401211300.asp*).

the Constitution, with a voice-over blaming Attorney General John Ashcroft. Print ads show an elderly gentleman leaving a bookstore with text decrying the use of government powers to get his book purchase list. But the hysteria is based on false premises.

We cannot decide policy based upon an overwrought sense of fear. Most of the steps proposed to combat terrorism were previously used to combat organized crime. And there is no evidence of any real abuse. No First Amendment liberties have been curtailed, no dissent or criticism suppressed.[48] While we must be cautious, John Locke, the 17th century philosopher who greatly influenced the Founding Fathers, was right when he wrote:

> In all states of created beings, capable of laws, where there is no law there is no freedom. For liberty is to be free from the restraint and violence from others; which cannot be where there is no law; and is not, as we are told, a liberty for every man to do what he lists.[49]

Thus, the obligation of the government is a dual one: to protect civil safety and security against violence *and* to preserve civil liberty.

In reviewing our policies and planning for the future, we must be guided by the realization that this is not a zero-sum game. We can achieve both goals—liberty and security—to an appreciable degree. The key is empowering government to do the right things while exercising oversight to prevent the abuse of authority. So long as we keep a vigilant eye on police authority, so long as the federal courts remain open, and so long as the debate about governmental conduct is a vibrant part of the American dialogue, the risk of excessive encroachment on our fundamental liberties can be avoided.

—Edwin Meese III is Ronald Reagan Distinguished Fellow in Public Policy and Chairman of the Center for Legal and Judicial Studies at The Heritage Foundation. Paul Rosenzweig is Senior Legal Research Fellow in the Center for Legal and Judicial Studies and Adjunct Professor of Law at George Mason University School of Law.

45. Critics of Section 215 do, however, have one strong argument against renewal of the Section 215 authority (which sunsets in December 2005)—that the authority granted may be unnecessary. Facing wide public criticism of the provisions of Section 215, the Attorney General has disclosed that, at least as of September 2003, the provision had not been used to secure any records. *See* Memorandum for Director Robert S. Muller (Sept. 18, 2003) (available at *http://www.cdt.org/security/usapatriot/030918doj.shtml*). But it is important to recognize that this is a question of *utility*, not a question of *abuse*. And we know that the September 11 terrorists did use Internet connections at libraries to communicate, well prior to the existence of any predication that they had committed a crime. *See, e.g.*, Farhad Manjoo, "Terrorists Leave Paperless Trail," Wired News (Sept. 20, 2001) (available at *http://www.wired.com/news/politics/0,1283,46991,00.html*). Thus, the potential utility of the section exists and the suggestion in the SAFE Act to unilaterally and prematurely exempt library Internet connections from surveillance is most unwise.

46. *See, e.g.*, Sen. Russ Feingold, Speech on the Libraries, Bookseller and Personal Records Privacy Act (Mar. 7, 2003) (available at *http://feingold.senate.gov/speeches/03/07/2003811915.html*) (reporting such events); "ACLU of Florida Urges Libraries to Warn Patrons of Government's New Domestic Spying Powers Under the USA Patriot Act" (July 30, 2003) (available at *http://www.aclufl.org/body_section215release.html*) (same).

47. As former Attorney General Meese has noted, the position adopted by librarians is particularly odd when contrasted with their long-standing opposition to federal provisions restricting children's on-line access to pornography. It is at least a little jarring that librarians see it as their duty to protect the access of minors to pornography while denying the government access to information of national security importance. *See* NBC News: Today (Sept. 30, 2003) (transcript available at 2003 WL 55607752). The American Library Association has also declined to condemn Fidel Castro's jailing of librarians. *See* Nat Hentoff, "Carrying Fidel's Water," Wa. Times at A19 (Jan. 26, 2004).

48. *See* Michael Chertoff, "Law, Loyalty, and Terror," The Weekly Standard 15, 16 (Dec. 1, 2003) (making this claim). Critics can point to little, if any, evidence rebutting this assertion.

49. John Locke, *Two Treatises of Government*, ed. Peter Laslett (Cambridge: Cambridge University Press, 1988), 305.

PREPARED STATEMENT OF ORIN S. KERR

Mr Chairman, Members of the Committee:

My name is Orin Kerr, and I am an Associate Professor at George Washington University Law School. It is my pleasure to submit this written testimony concerning the USA Patriot Act. My testimony will contain three parts: first, a brief explanation of my view that the public debate over the Patriot Act largely has misunderstood the Act; second, an overview of the legal issues raised by foreign intelligence surveillance; and third, an analysis of the constitutional issues raised by orders to compel information such as library records, bookstore records, and Internet communications.

I. THE DEBATE OVER THE USA PATRIOT ACT

The public debate over the USA Patriot Act has been based on a number of major misunderstandings about the scope and effect of the law. Millions of Americans believe that the Patriot Act profoundly reshaped the balance between privacy and security in a post-9/11 world. That is simply wrong. The truth is that the law is much more modest: Most of the Patriot Act consists of minor adjustments to a set of preexisting laws, such as the Foreign Intelligence Surveillance Act and the Electronic Communications Privacy Act. The Patriot Act left the basic framework of preexisting law intact, offering mostly minor changes to the set of statutory privacy laws Congress first enacted in the 1970's and 1980's. I explained this in greater depth in a law review article published in January 2003, and stand by that view today. *See* Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 Northwestern University Law Review 607 (2003), available at *http://papers.ssrn.com/sol3/papers.cfm?abstract—id=317501.*

Fortunately, the gap between the perception and the reality of the Patriot Act is beginning to narrow. In recent months, critics of the Patriot Act have come to acknowledge that most of the Act is consensus legislation that does not raise civil liberties concerns. For example, in an April 5, 2005 press release the American Civil Liberties Union acknowledged that:

> Most of the voluminous Patriot Act is actually unobjectionable from a civil liberties point of view and . . . the law makes important changes that give law enforcement agents the tools they need to protect against terrorist attacks. A few provisions . . . must be revised. . . .

See *Bipartisan Legislation Would Fix Worst Parts of Patriot Act While Maintaining Key Law Enforcement Powers,* available at *http://www.aclu.org/SafeandFree/SafeandFree.cfm? ID=17935&c=206.*

Although it is unfortunate that this acknowledgment appeared as late as it did, the ACLU's recognition that the Patriot Act debate is actually quite narrow is an important step to understanding Patriot Act reform. It reveals that the differences among pre-Patriot Act law, the law under the Patriot Act, and proposals to reform the Patriot Act tend to be relatively small. Of course, any legislative proposals that impact government power to conduct criminal or intelligence surveillance must be treated with the greatest consideration and care. Finding the right balance that both gives the government the power it needs to investigate terrorist threats and preserves our precious civil liberties is a very difficult task. At the same time, the effect of the Patriot Act and the scope of proposed amendments to it are much narrower than press accounts would lead one to believe.

II. OVERVIEW OF THE ISSUES RAISED BY THE USA PATRIOT ACT AND FOREIGN INTELLIGENCE SURVEILLANCE

I will now turn to an overview of the issues raised by the law of intelligence surveillance to help put the debate in better perspective. At the most basic level, any modern legal regime that allows the government to investigate crime or terrorism must address a number of basic methods for acquiring information. In particular, the law must cover three basic types of authorities:

(1) *Authority to conduct physical searches to retrieve physical evidence or collect information.*

(2) *Authority to compel third parties to produce physical evidence or disclose information.*

(3) *Authority to conduct real-time monitoring over communications networks.*

In the case of criminal investigations, the legal regime that covers these authorities is well- established. The first authority is governed by the traditional Fourth Amendment warrant requirement. The police must have a search warrant based on probable cause to enter a home or business unless a person with apparent or actual authority over the place consents, exigent circumstances exist, or another exception

to the warrant requirement applies. The second authority is governed by the Fourth Amendment rules governing subpoenas. Although many different types of subpoenas exist, and the rules can vary slightly depending on the type of subpoena, the general rule is that the police can compel third parties to disclose information in their possession using a subpoena. A subpoena can be issued under a wide range of circumstances: the information need only be relevant to the government's investigation, and compliance with the subpoena cannot be overly burdensome to the subpoena recipient. Finally, the third authority is regulated primarily by statutory law. Two different laws apply: the interception of contents such as phone calls and e-mails is regulated by the Wiretap Act, 18 U.S.C. §§ 2510–22, and the collection of non-content information such as phone numbers dialed and e-mail addresses is governed by the Pen Register statute, 18 U.S.C. §§ 3121–27. The former requires the law enforcement to obtain a "super warrant" based on probable cause unless an exception applies, while the latter permits law enforcement monitoring of non-content information under a relevance court order something like a subpoena.

The law governing monitoring for intelligence purposes is somewhat different than the law governing evidence collection for criminal cases. The Fourth Amendment's requirements are much less clear—and generally less strong—than in the routine criminal context. As a general matter, the few courts that have confronted how the Fourth Amendment applies to intelligence collection have held that the rules are somewhat similar to the rules for criminal investigations but also more flexible. When the Fourth Amendment applies, information and evidence collection must be reasonable in light of the countervailing demands and interest of intelligence collection. *See United States* v. *United States District Court*, 407 U.S. 297, 323–24 (1972); In re Sealed Case, 310 F.3d 717, 745–46 (Foreign Int. Surv. Ct. Rev. 2002). This legal framework appears to place Congress in the primary role of generating the law governing intelligence collection, with the Fourth Amendment serving as a backstop that reviews Congress's approach to ensure that it is constitutionally reasonable.

Congress has responded to the challenge by passing the Foreign Intelligence Surveillance Act, also known as "FISA." FISA attempts to create a statutory regime for intelligence monitoring that largely parallels analogous rules for gathering evidence in criminal cases. FISA covers the three basic authorities as follows: First, 18 U.S.C. §§ 1821–29 covers the authority to conduct physical searches, a parallel to the provision of the Federal Rules of Criminal Procedure that allows investigators to obtain a search warrant in criminal cases. Second, 18 U.S.C. §§ 1861–62 and 18 U.S.C. § 2709 covers authority to compel third-parties to disclose records and physical evidence, a parallel to the provision of the Federal Rules of Criminal Procedure that allows the issuance of subpoenas in criminal investigations. Third, 18 U.S.C. §§ 1801–22 and 18 U.S.C. §§ 1841–45 cover the authority to conduct real-time monitoring over communications networks. Specifically, §§ 1801–22 cover the authority to obtain the contents of communications, a parallel to the Wiretap Act used in criminal cases, and §§ 1841–45 cover the authority to obtain non-content information, a parallel to the Pen Register Statute used in crime investigations.

The debates over the FISA-related provisions of the Patriot Act focus primarily on the second type of authority: powers to compel third parties to produce physical evidence or disclose information. Specifically, critics object to the weak privacy regulations found in provisions such as Section 215 of the Patriot Act that address the government's power to compel third parties to produce physical evidence or disclose information in intelligence cases. For the most part, these weak privacy regulations match the standards applied in the analogous criminal context. For example, the Supreme Court has held that a grand jury subpoena can be issued if the order to compel seeks information that may be relevant to a criminal investigation. *See United States* v. *R. Enterprises, Inc.,* 498 U.S. 292 (1991). This authority "paints with a broad brush" by design, permitting subpoenas to be issued ordering third parties to disclose physical evidence and information "merely on suspicion that the law is being violated, or even just because . . . assurance [is sought] that it is not." *Id.* at 297 (quoting *United States* v. *Morton Salt Co.,* 338 U.S. 632, 642–643 (1950)). The Supreme Court has justified this low standard on the ground that orders to compel evidence from third parties are preliminary investigative tools designed to determine if more invasive forms of surveillance are necessary. "[T]he Government cannot be required to justify the issuance of a grand jury subpoena by presenting evidence sufficient to establish probable cause because the very purpose of requesting the information is to ascertain whether probable cause exists." *See R. Enterprises, Inc.,* 498 U.S. at 297.

The key question that the Committee must consider is whether a higher standard is appropriate for orders to compel in the context of intelligence investigations. The environment of intelligence investigations is somewhat different than the environ-

ment of criminal investigations. For example, subpoenas can be easily challenged and can be complied with under few time pressures, both of which are important explanations for the light legal regulations of subpoenas. *See United States* v. *Dionisio*, 410 U.S. 1, 10 (1973). At the same time, the harm that intelligence investigations seek to avoid is on average greater than the harm a typical criminal investigation seeks to deter. In addition, it is worth noting that Congress has opted to provide special privacy protections to protect some types of Internet communications and stored e-mails, raising the privacy protection beyond that provided by subpoenas. *See* 18 U.S.C. § 2703. Perhaps Congress should consider a similar approach in the intelligence context, permitting subpoena-equivalents to be used in some contexts but higher-threshold court orders to be used in other contexts that raise more substantial privacy concerns.

III. CONSTITUTIONALITY OF ORDERS TO COMPEL LIBRARY RECORDS AND INTERNET COMMUNICATIONS

The statutory regulation of orders to compel evidence from third parties is particularly important because the Fourth Amendment offers little in the way of regulation of such orders. In this final section, I wish to explain the constitutionality of orders to compel, specifically in the context of library records and Internet communications obtained from third party providers. My conclusion is that orders to compel the disclosure of evidence from third parties ordinarily do not require probable cause. Under current law, for example, probable cause is not required to compel libraries to compel library records.

The constitutionality of orders to compel evidence without probable cause can be justified on two alternative grounds. The first is that the disclosure of information to third parties has been held to eliminate Fourth Amendment protection in that information. As the Supreme Court stated in *United States* v. *Miller*, 425 U.S. 435, 443 (1976):

> This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

Under the disclosure rationale of *Miller*, third parties normally can be ordered to disclose records held by them without implicating the Fourth Amendment on the theory that the information was disclosed to them in the course of their coming into possession of the information.

Applying this rationale, courts have uniformly held that an individual does not retain Fourth Amendment rights in non-content records that reveal how that individual used an account or service provided by a third party. A person may reasonably believe that the third party will not disclose the information to the police, but this alone does not create a Fourth Amendment "legitimate" or "reasonable" expectation of privacy in the information. For example, a person does not retain a reasonable expectation of privacy in the information the telephone company retains about how a particular telephone account was used. *See United States* v. *Fregoso,* 60 F.3d 1314, 1321 (8th Cir. 1995). Similarly, a customer does not retain a reasonable expectation of privacy in the information that Western Union retains about how a particular Western Union account was used. *See* In re Grand Jury Proceedings, 827 F.2d 301, 302–03 (8th Cir. 1987).

The rationale also applies to library records. For example, in *Brown* v. *Johnston*, 328 N.W.2d 510 (Iowa 1983), a library challenged a subpoena obtained by a State investigator who wanted to gather library circulation records to see if anyone had checked out books relating to cattle mutilation. The Iowa Supreme Court rejected the argument that an ordinary subpoena could not be used to collect library records:

> It is true the State's investigation was only preliminary; and as Brown and the library board argue, no suspects were identified nor was the search for information limited to any named library patrons. This does not diminish the need for the information, however, as we assume the whole purpose in examining the record was to gain enough information so that the investigation could be narrowed.
>
> The State's interest in well-founded criminal charges and the fair administration of criminal justice must be held to override the claim of privilege here. Brown and the library board have cited no cases to us which have reached a contrary conclusion under similar facts, and we have found none. *Id.* at 513.

Although I have been unable to find any cases applying the Fourth Amendment to bookstore records, the same analysis would seem to apply to sales records kept

by bookstores. To be sure, some State courts have interpreted their own State constitutional provisions to create greater privacy protections to regulate State police officers in the context of bookstores. *See, e.g., Tattered Cover, Inc.* v. *City of Thornton*, 44 P.3d 1044 (Colo. 2002). But as far as I am aware, no court has held that a person retains a reasonable expectation of privacy in their bookstore customer records under the Fourth Amendment. As a general matter, the Fourth Amendment rules that apply to bookstores are the same as the Fourth Amendment rules that apply to other spaces. *See, e.g., Maryland* v. *Macon*, 472 U.S. 463 (1985).

Finally, the same rationale applies to non-content Internet account records. Non-content Internet account records are disclosed to the ISP, and are not protected under the Fourth Amendment. *See United States* v. *Hambrick*, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999), *aff'd*, 225 F.3d 656 (4th Cir. 2000) (unpublished opinion); *United States* v. *Kennedy*, 81 F. Supp. 2d 1103, 1110) (D. Kan. 2000) (same).

This does not mean an individual can never have a reasonable expectation of privacy in information held by third parties. Existing caselaw focuses on whether the information transferred to the third-party is disclosed to the third party or is sealed away from them. If a person gives third party a sealed container to hold on their behalf, then that person retains a reasonable expectation of privacy in the unexposed contents of that sealed container. *See, e.g., United States* v. *Most*, 876 F.2d 191, 197–98 (D.C. Cir. 1989); *United States* v. *Barry*, 853 F.2d 1479, 1481–83 (8th Cir. 1988). For that reason, a person retains a reasonable expectation of privacy in the contents of sealed postal letters or packages sent via UPS or FedEx until the point that the letters and packages arrive at their destination. *See* Ex Parte Jackson, 96 U.S. (6 Otto) 727, 733 (1877); *Walter* v. *United States*, 447 U.S. 649, 651 (1980).

It is unclear under current law how the sealed/unsealed distinction applies to disclosed information such as Internet communications, particularly in the context of the contents of Internet communications. Courts may conclude that by sending an e-mail, the user discloses that e-mail to an ISP under *Miller*. On the other hand, courts may conclude that the contents of e-mail can be analogized to the contents of a sealed letter, and thus retain Fourth Amendment protection. At the current time, all we know is that the Fourth Amendment does not protect non-content information held by ISPs, and may or may not protect content information held by ISPs. Notably, this uncertainty is part of what led Congress to impose greater statutory protections in the case of e-mail contents sought in criminal investigations under 18 U.S.C. § 2703(a).

Finally, existing cases suggest that a subpoena or equivalent order to compel without probable cause may be constitutionally sufficient even if a suspect retains a reasonable expectation of privacy in the information. The case here are sparse, as the courts have decided few cases in which the government ordered a third party to disclose sealed packages. But the few cases on this question suggest that the government can subpoena information even if that information is protected by a reasonable expectation of privacy; no probable cause warrant is required. *See United States* v. *Barr*, 605 F. Supp. 114, 119 (S.D.N.Y. 1985) (permitting subpoena served on third-party mail service for undelivered mail); *United States* v. *Schwimmer*, 232 F.2d 855, 861–63 (8th Cir. 1956) (permitting subpoena served on third-party storage facility for private papers in facility's possession); *Newfield* v. *Ryan*, 91 F.2d 700, 702–05 (5th Cir. 1937) (permitting subpoena served on telegraph company for copies of defendants' telegrams).

In light of these cases, current law points to the use of orders to compel evidence as being constitutional in the Fourth Amendment in most if not all cases without a requirement of probable case. The most difficult and least clear cases are orders to compel content records, such as the contents of e-mails and sealed letters. In most circumstances, however—and clearly in the case of non-content records such as library records—orders to compel evidence do not require probable cause under the Fourth Amendment.

PREPARED STATEMENT OF KATE MARTIN, DIRECTOR, CENTER FOR NATIONAL SECURITY STUDIES

While effective counterterrorism and counterintelligence require that agencies share relevant information, sections 203 and 905 of the USA Patriot Act fail to address the real difficulties in such sharing: How to determine what information is useful for counterterrorism and counterintelligence; how to determine what information would be useful if shared; how to identify whom it would be useful to share it with; and how to ensure that useful and relevant information is timely recognized and acted upon. To the contrary, the approach of the Patriot Act—which can fairly

be summarized as share everything with everyone—can be counted on to obscure and make more difficult the real challenge of information sharing.

Widespread and indiscriminate warehousing of information about individuals violates basic privacy principles. Amending the Patriot Act to require targeted rather than indiscriminate information sharing would restore at least minimal privacy protections and substantially increase the likelihood that the government could identify and obtain the specific information needed to prevent terrorist acts.

Section 203 of the USA Patriot Act allows unrestricted sharing of sensitive information gathered by law enforcement agencies with the CIA, the NSA, immigration authorities, the Secret Service, and White House officials. Such sharing is not limited to officials with responsibility for terrorism matters, nor are there any safeguards regarding the subsequent use or dissemination of such information by such officials (so long as the use is within the official duties of the recipient). Section 203 allows the sharing of all information that is in any way related to any American's contacts with or activities involving any foreign government, group, or individual. (Section 203 allows the sharing of "foreign intelligence information," "foreign intelligence" and "counterintelligence." The definition of "foreign intelligence information" included in section 203 is tied to threats and potential threats of terrorism, sabotage and clandestine intelligence-gathering, the national defense and foreign affairs, § 203(a)(1)(iv), 203(b)(2)(C), and 203(d)(2). However, the definitions of "foreign intelligence" and "counterintelligence" are not even that limited.) Section 203 applies to all intercepts of telephone conversations. It applies to all confidential information obtained by a grand jury, which has the power to subpoena virtually any records or testimony from any person merely at the request of a prosecutor.

Section 905 overlaps with section 203, but makes such sharing *mandatory*. It requires the Attorney General and the head of any other law enforcement agency to "expeditiously disclose" to the Director of Central Intelligence (and now the new Director of National Intelligence) all "foreign intelligence" acquired during a law enforcement investigation. The Attorney General may exempt only those classes of foreign intelligence whose disclosure "would jeopardize an ongoing law enforcement investigation or impair other significant law enforcement interests." Section 905 suffers from the same defects as section 203: it covers the most sensitive grand jury information and wiretap intercepts regardless of relevance, and contains no limits on the use or redisclosure of the information by intelligence agency staff. "Foreign intelligence" includes anything related to any American's contacts with a foreign government, group or person.

The Act sets no standards or safeguards for use of this information. While it requires the Attorney General to issue rules, those rules simply require that information concerning citizens and legal permanent residents be marked as such. Existing intelligence agency protocols are so broad as to allow intelligence agencies to keep all information obtained under section 203 or 905. *See* EO 12333 section 2.3.

Two and a half years after the passage of the Patriot Act, the 9/11 Commission staff confirmed that "there is no national strategy for sharing information to counter terrorism." The Department of Justice has yet to explain how these Patriot Act provisions will focus the bureaucracies on identifying what information is useful to locate actual terrorists, analyzing that information, and determining what actions to take based on the information. To the contrary, the provisions essentially direct agencies simply to dump massive volumes of unanalyzed information on other agencies. They facilitate the construction of a vast intelligence data base on Americans. And they effect an extraordinary change in the capability and authority of the foreign intelligence agencies, including the CIA, to keep information on Americans.

Congress should amend both sections 203 and 905 to provide some simple privacy safeguards, which will also ensure that information sharing is done in a more effective way.

Current law offers no protections against abuse. Too much information may be turned over to the CIA and others, including virtually all information about any American's contacts with any foreigner or foreign group, including humanitarian organizations, for example. Existing rules provide virtually no protection against authorized government compilation of dossiers on millions of Americans and use of those dossiers in intelligence operations.

Congress could provide some modest protections. The amendments proposed below—limiting shared information to information relating to terrorism or counterintelligence, limiting its dissemination to officials working on those matters, requiring judicial approval, and requiring marking to prevent redissemination—would not interfere with the needs of counterterrorism or counterintelligence.

While the Justice Department claims that any modifications to the information-sharing provisions would mean that agencies "would be required to identify proper legal authority prior to sharing or disseminating information outside of the col-

lecting agency or community," such objection misses the point. *See* Justice Department, USA Patriot Act: Sunsets Report, April 2005. The proposed amendments would not change the legal authorities for sharing information, they would simply help ensure that information is actually analyzed and determined to be useful to counterterrorism and counterintelligence. None of the uses of information outlined by the Justice Depaitinent in its Patriot Act report would be prohibited because all of them relate to terrorism.

But Congress should act to ensure that those agencies which first obtain information and are best positioned to understand its context do the work necessary to determine whether the information may be useful or relevant to other agencies. When in doubt, they should of course err on the side of transferring the information, but they should exercise some judgment in doing so. Ideally, they should describe the potential usefulness of the information when distributing it to other agencies. We note that intelligence officials are already reporting that under the current regime there is too much indiscriminate sharing of useless information.

Specifically Congress should consider the following modifications.

1. When information is gathered pursuant to judicial power, the court's approval should be required before transferring the information to intelligence agencies, White House personnel, or other law enforcement agencies in order to ensure that there is some real need for more widely distributing the information. Accordingly, court approval for sharing criminal wiretap intercepts of conversations and e-mail and secret grand jury information should be obtained, except when there is no time to obtain such approval in order to prevent an imminent terrorist act or the flight of a suspect.

2. The information that should be shared with the intelligence agencies, the White House, etc., should be limited to information relevant to terrorism or counterintelligence, rather than all information concerning any foreign contacts, the vast majority of which have nothing to do with terrorism. If the information transferred by law enforcement to the intelligence community were limited to "foreign intelligence information" as that term is defined in the Foreign Intelligence Surveillance Act, it would offer some protection against the CIA and others constructing a data base on the domestic activities of Americans. This safeguard was included in the Patriot Act, H.R. 2975 (107 Cong.), as approved by the House Committee on the Judiciary in October 2001.[1]

3. The information should be shared only with those officials who are directly involved in terrorism or counterintelligence.

4. There should be procedures for marking and safeguarding the shared information so these limits can be enforced and to protect against the redissemination of the information beyond these limits, much as classified information is marked and stored. Confidential grand jury information should be marked as such and intercepts of Americans' conversations and e-mails should be marked to prohibit indiscriminate circulation.

CONCLUSION

One of the most basic protections against government abuses has been the principle that a government agency should only collect information about individuals that it needs for a specific and articulated purpose, should use it only for the purposes for which it was collected, should not keep it any longer than necessary, and should not share it with other government agencies except for very good reasons. The Patriot Act violates that principle by adopting the approach that myriad government agencies should collect, share and maintain forever as much information on as many people as possible. Requiring the minimal protection that the government articulate why specific information could be useful for counterterrorism or counterintelligence before widely distributing it would help keep the government focused on the information needed to locate the next attackers, instead of warehousing personal information about millions of Americans.

Chairman ROBERTS. I now recognize the distinguished Vice Chairman.

Vice Chairman ROCKEFELLER. Thank you, Mr. Chairman. I will follow the same procedure you have. I think it's a wise one. I'm ready to hear the witnesses.

[The prepared statement of Vice Chairman Rockefeller follows:]

[1] See, H.R. REP. No. 236, 107th Cong., 1st Sess., pt. 1(2001), at 8, available at http://judiciary.house.gov/legacy/107–236p1.pdf.

PREPARED STATEMENT OF HON. JOHN D. ROCKEFELLER III, VICE CHAIRMAN

This week and next the Committee will hold two open hearings on the Patriot Act.

The Patriot Act, which was enacted soon after the attacks of September 11, 2001, contains 10 titles. Nine of those titles are permanent law.

One title of the Patriot Act—Title II on Enhanced Surveillance Procedures—has 16 provisions that will cease to have effect, or sunset, on December 31, 2005. In addition, the recently enacted Intelligence Reform Act authorizes the use of the Foreign Intelligence Surveillance Act in the case of so-called "lone wolf" terrorists. That new authority is also subject to sunset at the end of this year.

Congress should resolve two questions this year: first, on the basis of experience or further reflection since September 11, 2001, should any of the expiring authorities be amended; and second, as originally enacted or as amended, should they be made permanent?

The process of evaluation of the expiring provisions is under way. In response to a request from Senator Feinstein, the Department of Justice has submitted to Congress a lengthy "Sunsets Report" which sets forth a case for each of the 16 provisions of the Patriot Act that will sunset at the end of this year.

The Judiciary Committee has begun a series of Patriot Act hearings. It heard 2 weeks ago from the Attorney General and the FBI Director, something our Committee will do next week on April 27th. We have been informed that the Judiciary Committee plans to hold an additional hearing in May.

Members of the Senate have introduced bills that propose amendments to expiring Patriot Act provisions. There are also proposals to amend other provisions of the Act. On our Committee, Senator Corzine has joined a bipartisan group of 11 Members in cosponsoring S. 737, the "Security and Freedom Enhancement Act," a bill introduced by Senator Craig to amend several authorities in the Patriot Act. Senators Wyden and Corzine are cosponsors of S. 317, the "Library, Bookseller, and Personal Records Privacy Act."

In short, Congress has begun a serious effort to examine the expiring provisions of the Patriot Act. There were good reasons to act quickly after the September 11 attacks. Because of the need for speed then, it was wise to require, through a sunset provision, that there be a further evaluation of portions of the Act after several years of experience.

We now have an opportunity to assess carefully what surveillance and search powers are needed in gathering intelligence about terrorism and other threats. I look forward to hearing testimony and working with colleagues on our Committee and on the Judiciary Committee. Our goal, of course, should be to ensure that there is a sound, long-term basis for the effective gathering of intelligence in a manner consistent with our Constitution and values.

Our panel today will assist us in beginning that effort. The members of the panel—Jim Dempsey of the Center for Democracy and Technology, Heather Mac Donald of the Manhattan Institute for Policy Research, and Gregory Nojeim of the ACLU are all distinguished participants in the public debate about the Patriot Act. I look forward to their testimony today and to next week's testimony from the Administration.

In addition, the Committee has received four statements for the record: (1) from former Attorney General Edwin Meese and Paul Rosenzweig of the Heritage Foundation; (2) from former Congressman Bob Barr, chairman of a recently created coalition named Patriots to Restore Checks and Balances; (3) from Kate Martin, Director of the Center for National Security Studies; and (4) Orin Kerr, Associate Professor of Law at the George Washington University Law School.

I am pleased that the Chairman has asked for and obtained unanimous consent to place these additional statements on our record of this hearing. The statements will make an important contribution to the Committee's understanding of the issues before us. I thank the authors of each and the witnesses who are here today for their assistance to the Committee.

Chairman ROBERTS. We will go in the order of introduction. Mr. Nojeim, would you like to open up, please?

[The prepared statement of Mr. Nojeim follows:]

PREPARED STATEMENT OF GREGORY T. NOJEIM

Chairman Roberts, Vice Chairman Rockefeller and Members of the Committee:

I am pleased to appear before you today on behalf of the American Civil Liberties Union and its more than 400,000 members, dedicated to preserving the principles

of the Constitution and Bill of Rights at this rare, and crucial, public oversight hearing on USA PATRIOT Act of 2001.[1]

The Patriot Act was passed by Congress in 2001 just 6 weeks after the terrorist attacks of September 11. Although the act passed by wide margins, members on both sides of the aisle expressed reservations about its impact on fundamental freedoms and civil liberties. As a result, Congress included a "sunset clause" providing that over a dozen provisions will expire on December 31, 2005, if Congress does not act to renew them.

A number of the provisions that will expire are within the jurisdiction of this committee, including some of the most controversial provisions. This statement's main focus is on those Patriot Act intelligence provisions that pose the greatest risk for civil liberties.[2]

Congress should use the upcoming debate over the renewal of parts of the Patriot Act as an opportunity to reassert its rightful role in determining law enforcement and national security policy in the post-9/11 context, which has waned as the power of the executive branch has waxed. Before re-authorizing any intelligence power, this committee should require the executive branch to meet the standard articulated by the bipartisan 9-11 Commission.

• First, Congress should re-examine the specific provisions that sunset, taking care not to renew any provision unless the government can show "(a) that the power actually materially enhances security and (b) that there is adequate supervision of the executive's use of the powers to ensure protection of civil liberties."[3]

• Second, "[i]f the power is granted, there must be adequate guidelines and oversight to properly confine its use."[4]

• Third, because the issues of national security and civil liberties posed by anti-terrorism powers that are not part of the Patriot Act sunset are at least as serious as any posed by those provisions that do sunset, Congress should undertake a broader review of anti-terrorism powers, both within and outside of the Patriot Act, using the same standard of review.

• Finally, Congress should resist efforts by the executive branch to evade searching review of its existing powers, both under the Patriot Act and under other legal authorities, by shifting the debate to new anti-terrorism legislation, such as proposals for administrative subpoenas or new death penalties.

Congress may not be able to fully review or assess the effectiveness, and impact on civil liberties, of some anti-terrorism powers that the executive branch was granted in the Patriot Act. The lack of meaningful information about the use of many powers is sometimes a direct result of excessive secrecy in the executive branch, and sometimes the result of necessary secrecy. In any case where sufficient information is not available to undertake a thorough review, Congress should set a new sunset date and impose additional reporting requirements to facilitate a proper review, rather than cede those powers permanently to the executive branch.

Because many domestic intelligence authorities operate in complete secrecy, this committee plays a particularly critical role in determining whether specific intelligence powers "actually materially enhance security." Only an intensive and painstaking process of examining the facts regarding the use of these powers can answer that question.

This committee was created in large part to perform just that function. It should not be content with general statements of the Patriot Act's usefulness or selective accounts of how certain sections have been used. Rather, we hope it will aggressively and thoroughly examine whether administration claims that certain powers are vital to the prevention of terrorism are born out by specific facts.

Until now, the government has fallen short. Just last week, Judiciary Chairman Arlen Specter expressed frustration at the Justice Department's inability to provide such facts even in a classified setting. "This closed-door briefing was for specifics," Senator Specter explained. "They didn't have specifics."[5]

---

[1] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107–56, 115 Stat. 272.

[2] This statement is adapted from a longer memorandum that examines a number of other Patriot Act and related issues in greater depth, including immigration, material witness and "enemy combatant" detentions, criminal "sneak and peek" search warrants, the crime of material support of terrorism and the definition of domestic terrorism. *See* Memo to Interested Persons Outlining What Congress Should Do About the Patriot Act Sunsets, March 28, 2005, available at: *http://www.aclu.org/news/NewsPrint.cfm?ID=17846&c=206.*

[3] Final Report of the National Commission on Terrorist Attacks Upon the United States ("The 9/11 Commission Report") 294–95 (2004) (boldfaced recommendation)

[4] *Id.*

[5] Eric Lichtblau, *Specter Voices Frustration Over Briefing on Patriot Act*, N.Y. Times, Apr. 13, 2005.

CLEAR EVIDENCE OF PATRIOT ACT ABUSES, BUT EXTENT OF PROBLEM STILL SECRET

In its three and one-half years, the government has abused and misused the Patriot Act while seeking significant expansions of powers granted under the Patriot Act.

Secrecy permeates the Patriot Act, particularly in its expansions of intelligence authorities. Many powers are accompanied by statutory gag orders. Moreover, the administration has taken the posture that information that is embarrassing to it must be kept secret for reasons of national security. For these reasons, it has been extremely difficult to uncover information about how the Patriot Act has been used, and even information about whether particular sections have been used at all. The ACLU has repeatedly sought this information in letters, requests under the Freedom of Information Act (FOIA) and in FOIA litigation.

Despite the efforts of the executive branch to cover up information about how controversial provisions of the Patriot Act have been used, some information has become public. This information is disturbing in and of itself, and may be emblematic of other abuses that have not yet become public. Appended to this testimony are some examples of abuses of intelligence powers expanded under the Patriot Act, and of the chill on the exercise of First Amendment rights that such powers can create.

PATRIOT ACT INTELLIGENCE POWERS: GREATER SECRECY, LESS MEANINGFUL REVIEW

In the debate over the Patriot Act, we ask the committee to pay particular attention to the most intrusive expanded intelligence surveillance techniques.

Secret Records Searches Without Probable Cause or an Ability to Challenge: Library Records, Other "Tangible Things," and National Security Letters

Perhaps no sections of the Patriot Act have become more controversial than the sections allowing the government secretly to obtain confidential records in national security investigations—investigations "to protect against international terrorism or clandestine intelligence activities."

National security investigations are not limited to gathering information about criminal activity. Instead, they are intelligence investigations designed to collect infounation the government decides is needed to prevent—"to protect against"—the threat of terrorism or espionage. They pose greater risks for civil liberties because they potentially involve the secret gathering of information about lawful political or religious activities that Federal agents believe may be relevant to the actions of a foreign government or foreign political organization (including a terrorist group).

The traditional limit on national security investigations is the focus on investigating foreign powers or agents of foreign powers. Indeed, the "foreign power" standard is really the only meaningful substantive limit for non-criminal investigations given the astonishing breadth of information a government agent might decide is needed for intelligence reasons. The Patriot Act eliminated this basic limit for records searches, including the power under the Foreign Intelligence Surveillance Act (FISA) to obtain with a FISA court order any records or other "tangible things," and the FBI's power to obtain some records without any court review at all.

- Section 215 of the Patriot Act allows the government to obtain any records, e.g., library and bookseller records, medical records, genetic information, membership lists of organizations, and confidential records of refugee service organizations, as well as any other "tangible things" with an order from the FISC. The order is based merely on a certification by the government that the records are "sought for" a national security investigation and the judge is required to issue the order. The order contains an automatic and permanent gag order. Section 215 is subject to the sunset clause. Two weeks ago, the government acknowledged for the first time that Section 215 has been used, that it has been used 35 times, and that it was used to obtain credit, apartment, ISP and other records, but not library or medical records.
- Section 505 of the Patriot Act expanded the FBI's power to obtain some records in national security investigations without any court review at all. These "national security letters" can be used to obtain financial records, credit reports, and telephone, Internet and other communications billing or transactional records. The letters can be issued simply on the FBI's own assertion that they are needed for an investigation, and also contain an automatic and permanent nondisclosure requirement. Section 505 does not sunset.

Although such demands never required probable cause, they did require, prior to the Patriot Act, "specific and articulable facts giving reason to believe" the records pertain to an "agent of a foreign power." The Patriot Act removed that standard for issuing records demands in national security investigations.

As a result, a previously obscure and rarely used power can now be used far more widely to obtain many more records of American citizens and lawful residents. Be-

cause the requirement of individual suspicion has been repealed, records powers can now be used to obtain entire data bases of private information for "data mining" purposes—using computer software to tag law abiding Americans as terrorist suspects based on a computer algorithm.

These records search provisions are the subject of two court challenges by the ACLU. In *Muslim Community Association of Ann Arbor* v. *Ashcroft*, No. 03-72913 (E.D. Mich.), the ACLU has challenged section 215 of the Patriot Act First and Fourth Amendment grounds. As explained in the case example, the ACLU's challenge has uncovered serious and unconstitutional chilling effects of section 215 on the exercise of basic freedoms. The district court has not yet ruled in this case.

In *Doe* v. *Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004), a Federal district court struck down a "national security letter" records power expanded by the Patriot Act, agreeing with the ACLU that the failure to provide any explicit right for a recipient to challenge a national security letter search order violated the Fourth Amendment and that the automatic secrecy rule violated the First Amendment. The case is now on appeal before the United States Court of Appeals for the Second Circuit.

There has been some confusion about whether *Doe* v. *Ashcroft* struck down a provision of the Patriot Act. In fact, *Doe* v. *Ashcroft* struck down, in its entirety, 18 U.S.C. § 2709(b), the national security letter authority for customer records of communications service providers, as amended by section 505(a) of the Patriot Act. The court referred repeatedly to the Patriot Act in its opinion. To be clear, the court invalidated *all of section 505(a) of the Patriot Act*. It is simply inaccurate to imply that the court's decision was unrelated to the Patriot Act, or that it did not strike down a provision of the Patriot Act. If the court's decision is sustained on appeal, section 505(a) of the Patriot Act will no longer have any force or effect.[6]

Both FISA records demands and national security letters can be used to obtain sensitive records relating to the exercise of First Amendment rights. A FISA record demand could be used to obtain a list of the books or magazines someone purchases or borrows from the library. A FISA record demand could be used to obtain the membership list of a controversial political or religious organization. A national security letter could be used to monitor use of a computer at a library or Internet café under the government's theory that providing Internet access (even for free) makes an institution a "communications service provider" under the law.

While both national security letters and FISA records demands cannot be issued in an investigation of a United States citizen or lawful permanent resident if the investigation is based "solely" on First Amendment activities, this provides little protection. An investigation is rarely, if ever, based "solely" on any one factor; investigations based in large part, but not solely, on constitutionally protected speech or association are implicitly allowed. An investigation of a temporary resident can be based "solely" on First Amendment activities, and such an investigation of a foreign visitor may involve obtaining records pertaining to a United States citizen. For example, an investigation based solely on the First Amendment activities of an international student could involve a demand for the confidential records of a student political group that includes United States citizens or permanent residents.

The expanded scope and broader use of both FISA records demands and national security letters has exacerbated other constitutional problems with the statute under both the First Amendment and the Fourth Amendment. Unlike almost every other type of subpoena or records demand, neither statute contains any explicit right to file a motion to quash the demand before a court on the ground that the demand is unreasonable or seeks privileged information. Similarly, both types of records demands bar the recipient from disclosing that the demand has been issued. This permanent secrecy order is imposed automatically, in every case, without any review by a judge, without any right to challenge. The district court ruling in *Doe* v. *Ashcroft* makes clear these problems are severe enough to invalidate the entire national security letter statute—not just the portions amended by the Patriot Act.

A power to secretly obtain records of ordinary Americans—i.e., Americans who are not suspected of involvement with any foreign government or terrorist organization—outside of a criminal investigation is a vast power. The government bears the burden in showing such a power "actually materially enhances security." If the gov-

[6] While the use of national security letters are secret, the press has reported a dramatic increase in the number of letters issued, and in the scope of such requests. For example, over the 2003–04 holiday period, the FBI reportedly obtained the names of over 300,000 travelers to Las Vegas, despite casinos' deep reluctance to share such confidential customer information with the government. It is not clear whether the records were obtained in part with a national security letter, with the threat of such a letter, or whether the information was instead turned over voluntarily or to comply with a subpoena.

ernment sustains this burden, it is clear, as even Attorney General Gonzales has acknowledged, that additional safeguards must be added.

Recommendation: Congress should bring intelligence records powers (national security letters and FISA records search orders) back into line with basic constitutional freedoms. Congress should enact the SAFE Act, which restores the requirement of individual suspicion, provides a right to challenge records demands, limits the secrecy order and provides for a right to challenge the secrecy order.

The SAFE Act ("Security and Freedom Enhancement Act," S. 737) restores the requirement of "specific and articulable facts giving reason to believe" the records involve an "agent of a foreign power" for both FISA records demands and national security letters. In addition, the SAFE Act makes explicit the right to file a motion to quash the records demands because they are unreasonable, contrary to law, or seek privileged information. The SAFE Act also sets standards for a judicially imposed, temporary secrecy order that can be challenged by the recipient of a records demand. Finally, the SAFE Act provides a right to notice, and an opportunity to challenge, before information from a FISA records search or national security letter search can be used in a court proceeding.

As the Attorney General concedes is necessary, Congress should certainly make clear what the government has now conceded should be the law—that the secrecy order does not prevent recipients from discussing records demands internally or obtaining legal advice. Without public scrutiny, the potential for unreasonable "fishing expeditions" using a secret, unreviewable records power is simply too great.

Secret Searches and Surveillance of Homes and Offices

A government search or electronic surveillance of a home or office generally requires a warrant based on probable cause of crime under the Fourth Amendment. As a general rule, the owner of the home or office is entitled to notice of the search. Foreign intelligence searches have been an exception to this rule. They do not require criminal probable cause and forbid notice to the owner.

The special power to secretly search a home or office, without ever notifying the owner, is among the most intrusive domestic surveillance powers available to the Federal Government. Such "black bag jobs" were the hallmark of national security investigations run amok, including COINTELPRO and other investigations of civil rights activists, anti-war activists, and other Americans who in the end were guilty of nothing more than peacefully opposing government policies.

The inappropriate use of a secret search power, without court oversight, led directly to warrantless wiretaps of civil rights leaders and, eventually, an unauthorized "black bag job" at the Watergate, sending a shock wave through the Nation and prompting thorough and searching reviews of the intelligence community. These reviews led Congress to enact important reforms of intelligence powers, including the passage of the Foreign Intelligence Surveillance Act (FISA) and the creation of this committee.

While FISA secret searches and wiretaps pre-date the Patriot Act, two vital protections that cabined such searches until 2001 have been seriously eroded by amendments that are subject to the December 31, 2005 sunset. First, section 218 of the Patriot Act allowed the government to obtain a FISA secret search order even where the "primary purpose" of the search was not foreign intelligence. Second, for searches of so-called "lone wolf" terror suspects, section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004[7] eliminated, for the first time, the basic requirement applied by the Foreign Intelligence Surveillance Court for all FISA secret searches and surveillance: that probable causes exists that the target of the search is a foreign power or agent of foreign power.

Section 218 of the Patriot Act. This provision of the Patriot Act takes aim at a provision of FISA designed to ensure against the government using FISA improperly as an end-run around the Fourth Amendment for criminal suspects. Prior to the Patriot Act, government officials had to certify that the primary purpose of a secret FISA search was to obtain foreign intelligence.[8] Section 218 of the Patriot Act weakened this standard, allowing agents to obtain these warrants so long as they certify that "*a significant purpose*" of the search is foreign intelligence.

---

[7] Pub. L. No. 108–458, 118 Stat. 3638.

[8] The pre-Patriot Act statute required the government to certify that foreign intelligence was "the purpose" of the search. Where the government had both foreign intelligence and criminal investigation purposes, courts interpreted this language to mean that foreign intelligence purpose had to be the "primary purpose" of the search; otherwise, the government should use its criminal powers. *See In Re Sealed Case,* 310 F.3d 717, 726 (For. Intel. Surv. Ct. Rev. 2002) (collecting pre-Patriot Act cases).

The danger of section 218's lower standard is that the government will cut corners in criminal cases. Because foreign intelligence no longer must be the primary purpose of the search, the government can use FISA as a substitute for traditional criminal powers. As a result, now the government can—for what are primarily criminal searches—evade the Fourth Amendment's constraints of probable cause of crime and notice to the person whose property is being searched.

Brandon Mayfield is a case where such corners may have been cut. As described in more detail in the appendix, Mr. Mayfield is a Portland, Oregon resident who is a convert to Islam and a civil rights advocate. Mr. Mayfield was wrongly accused by the government of involvement in the Madrid bombing as a result of a evidence, including a mistaken fingerprint identification, that fell apart after the FBI re-examined its case following its arrest and detention of Mr. Mayfield on a material witness warrant.

As Attorney General Gonzales acknowledged at a hearing before the Senate Judiciary Committee, Section 218 of the Patriot Act was implicated in the secret search of Mr. Mayfield's home. The FBI secretly entered the home of an innocent man it wrongly suspected of a crime without a warrant based on criminal probable cause. It did so because the Patriot Act had made it easier to conduct such a search with a FISA search order. While there, agents took hundreds of photographs, copied four computer hard drives and seized 10 DNA samples. Prior to the Patriot Act, it is doubtful the search could have taken place under FISA, and instead would likely have been governed by normal search warrant procedures and the exacting standard of criminal probable cause.

Recommendation: Congress should permit limited access to FISA applications, consistent with national security, where FISA-gathered information is used in a criminal case. Congress can do so by enacting legislation applying CIPA to FISA surveillance. It should also ensure that prosecutors do not direct intelligence surveillance.

If the government is able to meet the burden of showing section 218 "actually materially enhances security," the Mayfield case and the danger of future abuses shows the need for additional safeguards. Without re-building the much-maligned "wall" between foreign intelligence and criminal investigations, Congress should follow the approach of the Foreign Intelligence Surveillance Court (FISC), restoring its power to serve its proper supervisory function to prevent the misuse of FISA. Congress should empower the court to make sure foreign intelligence investigations are not directed by Federal prosecutors, although prosecutors and criminal investigators should be allowed full briefings on such investigations.

In its first (and, so far, only) public opinion, the FISC, in an opinion by Judge Lamberth, expressed alarm at the fact that "criminal prosecutors will tell the FBI when to use FISA (perhaps when they lack probable cause)" of crime, and noting its highly intrusive aspects, including:

- a foreign intelligence standard instead of a criminal standard of probable cause;
- use of the most advanced and highly intrusive techniques for intelligence gathering; and
- surveillances and searches for extensive periods of time; based on a standard that the U.S. person is only using or about to use the places to be surveilled and searched, without any notice to the target unless arrested and prosecuted, and, if prosecuted, no adversarial discovery of the FISA applications and warrants."[9]

Judge Lamberth observed that the FISC's members had "specialized knowledge," had reviewed "several thousand FISA applications," and were "mindful of the FISA's pre-eminent role in preserving our national security, not only in the present national emergency, but for the long term as a constitutional democracy under the rule of law."[10] It reasoned that, as a result, it retained supervisory powers to protect against the misuse of FISA for criminal investigative purposes.

The Foreign Intelligence Surveillance Court of Review reversed this opinion, reasoning that section 218 of the Patriot Act had stripped the FISC of this role.[11] If Congress reauthorizes section 218, it should amend it to make clear that the provision does not prohibit the FISC from adopting guidelines to prevent the direction and control of foreign intelligence investigations by prosecutors for law enforcement ends.

Congress should also explore a remedy for one of the serious problems inherent in making FISA searches more available in what are primarily criminal investigations: the lack of "adversarial discovery for FISA applications and warrants." This

[9] *In re All Matters Submitted to the Foreign Intelligence Surveillance Court,* 218 F. Supp. 2d 611, 624 (For. Intel. Surv. Ct. 2002).

[10] *Id. at 615.*

[11] *See In re Sealed Case,* 310 F.3d 717 (For. Intel. Surv. Ct. Rev. 2002).

is in marked contrast to the extensive discovery available to criminal defendants, enabling the court to hold government officials accountable for unlawful searches and surveillance.

Congress should enact legislation making available to the defense such "adversarial discovery of FISA applications and warrants" using the carefully crafted Classified Information Procedures Act (CIPA). Last Congress, the ACLU strongly supported S. 1552, the Protecting the Rights of Individuals Act, sponsored by Senators Lisa Murkowsky (R-AK) and Ron Wyden (D-OR), which included this provision at section 9. An identical provision was also included as section 401 of S. 2528, the Civil Liberties Restoration Act, sponsored by Senators Kennedy (D-MA), Corzine (D-NJ) and Leahy (D-VT), among others.

Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004. Section 6001 further eroded the basic safeguards included in FISA by authorizing, for the first time, secret searches and surveillance of homes and businesses where there is neither criminal probable cause nor probable case that the person is acting on behalf of any foreign power.

FISA rests what would otherwise plainly be unconstitutional searches (because they are not based on probable cause of crime) on an alternate showing: probable cause that those individuals are acting on behalf of a foreign power. By eliminating this alternate showing for non-citizen visitors to the United States suspected of being "lone wolf" terrorists, we believe section 6001 violates the Fourth Amendment.

Moreover, section 6001 was not needed to address deficiencies in the use of FISA search powers uncovered after September 11, its original rationale. The National Commission on Terrorist Attacks Upon the United States ("9–11 Commission") uncovered a number of serious, structural breakdowns in the intelligence community prior to September 11. A lack of legal authority to collect intelligence information was not among its findings.

Section 6001 has erroneously been described as necessary to respond to the government's failure to seek a warrant to search the laptop computer of suspected terrorist Zacarias Moussaoui. The 9–11 Commission rejected that conclusion, finding that government agents "misunderstood and misapplied" guidelines regarding FISA search warrants, and that these mistakes contributed to their failure to seek either a criminal or FISA warrant in the Moussaoui case.[12] The 9-11 Commission did not recommend any change to existing legal authorities, including FISA.

In a February 2003 report on FISA oversight, Senators Leahy, Grassley and Specter noted, with respect to this proposed change, that the Department of Justice was unable to provide even a single case, even in a classified setting, that explained why what became section 6001 was needed. As the report states, "In short, DOJ sought more power but was either unwilling or unable to provide an example as to why."

Section 6001 could do serious harm to the government's anti-terrorism efforts if a court concludes that the surveillance it authorizes violates the Fourth Amendment, making the evidence obtained by such surveillance inadmissible. The "foreign power" standard—which section 6001 eliminates for non-citizens—is integral to the rationale given by the Foreign Intelligence Surveillance Court of Review in its opinion upholding FISA surveillance against a constitutional challenge.[13]

This committee should review carefully actual applications for secret searches or surveillances under the new power provided by section 6001 to determine whether such searches or surveillance could have been undertaken using traditional criminal powers, and whether section 6001 "actually materially enhances security." If the government satisfies this test and Congress decides to re-authorize section 6001, Congress should consider additional safeguards.

Recommendation: Congress should modify section 6001 to provide a presumption that an individual who is involved in international terrorism is acting for a foreign power. This compromise, offered by Senator Dianne Feinstein (D-CA) to legislation that became section 6001, would give the Foreign Intelligence Surveillance Court more discretion to ensure against misuse of FISA.

When S. 113, the legislation that became section 6001, was being debated in the Senate, Senator Dianne Feinstein offered a compromise that the ACLU supported. The Feinstein amendment would have formally preserved the FISA requirement that the FISA court determines that the target of a surveillance order is an agent of a foreign power before a surveillance order is authorized, but it allowed the court

---

[12] *Final Report of the National Commission on Terrorist Attacks Upon the United States* 79, 540 n.94 (2004).

[13] *See In re Sealed Case,* supra, at 738 (relying on "foreign power" probable cause to hold that FISA secret searches and surveillance satisfy Fourth Amendment standards of reasonableness).

to presume such agency based on conduct that does not necessarily show such agency. Because the amendment would preserve some discretion on the part of the FISA court to determine that an individual should not be subject to surveillance because they are not, in fact, an agent of a foreign power, the ACLU urges Congress to adopt the Feinstein amendment if it decides to reauthorize section 6001.

Wiretapping and Electronic Surveillance Without Judicial Safeguards Limiting Orders to the Targets of an Investigation

"General warrants"—blank warrants that do not describe what may be searched—were among those oppressive powers used by the British crown that led directly to the American Revolution. As a result, the framers required all warrants to "particularly describ[e] the place to be searched, and the persons or things to be seized."

The same "particularity" requirements apply to wiretap orders. In the landmark case *United States* v. *Donovan*, 429 U.S. 413 (1977), a majority upheld the Federal criminal wiretap law, noting that Congress had redrafted the law to include safeguards regarding, among other things, the need to identify targets of surveillance in response to the "constitutional command of particularization."[14]

Congress has also authorized Federal judges to issue electronic surveillance orders in foreign intelligence cases, including wiretaps of telephone conversations and intercepts of the content of other electronic communications (faxes, e-mail, etc.).

The Patriot Act erodes the basic constitutional rule of particularization:

• Section 206 creates "roving wiretaps" in foreign intelligence cases. As amended by later legislation, these wiretaps do more than allow the government to get a single order that follows the target of surveillance from telephone to telephone. The government can now issue "John Doe" roving wiretaps that fail to specify a target or a telephone, and can use wiretaps without checking that the conversations they are intercepting actually involve a target of the investigation. Section 206 is subject to the Patriot Act's sunset clause.

• Section 207 greatly increases the length of time that foreign intelligence wiretaps may be used without any judicial oversight—from 90 days to 6 months for the initial order, with renewals allowing surveillance to continue for a year before require judicial approval. Section 207 is subject to the Patriot Act's sunset clause.

Section 206 of the Patriot Act: Foreign intelligence "roving wiretaps." "Roving wiretaps" are a particularly potent form of electronic surveillance, allowing the government to obtain a single wiretap order that follows a target as the target uses different telephones or devices to communicate. Prior to the passage of the Patriot Act, roving wiretaps were available in criminal investigations (including criminal investigations of terrorists), but were not available in foreign intelligence investigations.

Because roving wiretaps contain more potential for abuse than traditional wiretaps, which apply to a single telephone or other device, when Congress enacted roving wiretaps for criminal investigations, it insisted on important privacy safeguards. First, a criminal wiretap must specify either the identity of the target or the communications device being used. In other words, a surveillance order may specify only the target, or only the phone, but it must specify one or the other. Second, a criminal wiretap that jumps from phone to phone or other device may not be used unless the government "ascertains" that the target identified by the order is actually using that device.

When Congress enacted the Patriot Act, it extended "roving wiretap" authority to FISA investigations, but did not include the common sense "ascertainment" safeguard. Shortly thereafter, the newly enacted roving wiretap authority was broadened by the Intelligence Act for fiscal year 2002, which authorized wiretaps where neither the target nor the device was specified. As a result, FISA now allows "John Doe" roving wiretaps—wiretaps that can follow an unknown suspect from telephone to telephone based only on a potentially vague physical description, opening the door to surveillance of anyone who fits that description, or anyone else who might be using that telephone.

Because of this danger, if Congress is satisfied the government has met its burden to show FISA roving surveillance authority "actually materially enhances security" and should be renewed, it should include additional privacy safeguards.

Recommendation: Congress should include an ascertainment requirement and should require electronic surveillance orders to specify either a target or a telephone or other device, by enacting the bipartisan SAFE Act of 2005.

Congress should tighten the FISA roving wiretap so that it has the same safeguards for privacy as criminal roving wiretaps. Supporters of the Patriot Act often

[14] *Id.* at 426–27 (quoting S. Rep. No. 1097, 90th Cong., 2nd Sess., at 66 (1968), *reprinted in* U.S. Code Cong. and Admin. News 1968, at 2190).

argue that changes to the law were needed to give the government the same powers in foreign intelligence investigations that it already had in criminal investigations. To the extent that is appropriate, it is fair to insist that the same safeguards apply as well.

Section 2 of S. 737, the SAFE Act, would provide just such safeguards. While it preserves FISA roving surveillance authority, it also makes sure that these privacy safeguards, which apply to criminal roving wiretaps, would also apply to FISA roving wiretaps.

Section 207 of the Patriot Act. The time periods for foreign intelligence surveillance orders were already much longer than for criminal surveillance orders even before the passage of the Patriot Act. Permitting surveillance to continue for a year with no judicial review opens the door for abuse. The Justice Department's main justification for allowing review to continue for such a long period has been the ability to conserve attorney time and other resources needed to process renewal applications.

If the administration can show the sharp increases in FISA secret searches and surveillance enabled by this and other provisions "actually materially enhances security," Congress should consider the cost in lost oversight of highly intrusive powers. It may be possible to get the benefits while preserving oversight.

Recommendation: Congress should extend the sunset provision on this section and conduct an investigation to determine whether it should shorten the periods for FISA surveillance, and it should consider providing additional resources to the Justice Department and the FISC.

Congress should consider whether it can shorten these periods by conducting a searching review of FISA surveillance conducted under the lengthened periods. Was it productive for the entire period it was authorized? If the problem is a lack of resources, the solution should not be to shortchange judicial oversight. Precisely because there is increased pressure to engage in surveillance early to prevent terrorism before it happens, there is an increased danger of abuse and an increased need for judicial oversight. Congress should provide sufficient funds both to the Department of Justice and to the Foreign Intelligence Surveillance Court to handle the important work of reviewing surveillance orders.

Internet Surveillance Without Probable Cause: Web Browsers, E-Mail, and "Pen/Trap" Devices

While the "probable cause" standard has long applied both to physical searches and electronic intercepts of the content of conversations, surveillance techniques that monitor only who is sending or receiving information (often called "routing information"), but do not intercept the content of communications, do not require probable cause.

For telephones, pen registers and "trap and trace" devices have long been available to track the telephone numbers dialed, and the telephone numbers of incoming calls. These numbers could then be cross-referenced, through a reverse telephone directory, to identify to whom a target of a pen/trap device is calling. A similar technique, "mail covers," is used to track the outside cover of an envelope sent through the mail. Neither technique requires probable cause, although a court order may be needed.

Prior to the passage of the Patriot Act, it was unclear how the law allowing pen/trap devices for telephone communications applied to communications over the Internet. Federal agents argued they should be allowed, without showing probable cause or obtaining a surveillance order, to monitor the "header" information of an e-mail and the URL of a web page.

Privacy advocates urged caution, noting that Internet communications operate very differently than traditional mail or telephone communications. For example, the "header" information of an e-mail contains a wealth of information, such as a subject line or an entire list of thousands or even hundreds of thousands of addressees. A monitoring order would allow the government to obtain, without probable cause, a political, charitable or religious organization's electronic mailing list. In short, e-mail headers provide far more content than is typical on the outside of an envelope.

Likewise, the "link" at the top of a web browser contains not only the website visited, but also the precise pages viewed, or the search terms or other information entered by the user on a web-based form. For example, in the popular search engine "google," a user looking for information about a drug such as "viagra" generates the web address *http://www.google.com/search?hl=en&lr=&q=viagra.*

Section 214 of the Patriot Act broadens the use of Internet surveillance, without probable cause, by extending the pen/trap surveillance technique from a relatively narrow arena of facilities used by agents of foreign powers or those involved in

international terrorism to include any facility. Pen/trap surveillance can now be used far more widely to monitor the Internet use of ordinary Americans.

Pen/trap for the Internet suffers from a basic flaw: in extending this intrusive surveillance authority to the Internet, Congress did not adequately take account the differences between the Internet and traditional communications that make intercept of Internet "routing information" far more intrusive as applied to Internet communications.

If the administration can show that section 214 of the Patriot Act "actually materially enhances security" and should be renewed, Congress should insist on additional protections to take into account the differences between Internet and traditional telecommunications.

Recommendation: Congress should insist on rules that clearly define content and prohibit the use of techniques that acquire content without a surveillance order based on probable cause. In addition, because obtaining "routing information" in the Internet world is even more intrusive than pen registers and trap and trace devices applied to traditional telecommunications. Congress should enact the SAFE Act, which provides that pen/trap orders require more specific justification.

Congress should insist on rules that:

• *Clearly define content for Internet communications.* Congress should be specific. For e-mails, at the very least, the subject line and any private (i.e., "bcc") list of addresses should be off limits without a surveillance order based on probable cause. For Internet browsing, obtaining any information behind the top level domain name should likewise be barred without probable cause. For example, an agent could obtain a list of websites visited (like *www.aclu.org*) but not of webpages visited (like *www.aclu.org/patriotact*) or search tetras entered (like *http://www.google.com/search?hl=en&q=aclu+craig+durbin+safe+act*).

• *Prevent techniques that acquire content from being used in the absence of an order based on probable cause.* The Internet does not work like traditional telephones or the mail. The constitutionally protected content of communications may be difficult, or even impossible, to separate from the "routing information." For example, e-mail may be sent through the Internet in discrete "packets," rather than as a single file, to permit the information to be sent along the most efficient route, then reassembled at the destination, using codes that are attached to the packets of information. The burden should be on the government to develop techniques that do not incidentally acquire content. In the absence of those techniques, a surveillance order based on probable cause should be required. Federal agents should not be put in the untenable position of incidentally gathering constitutionally protected content in the course of obtaining "routing information," and then being forced to delete or ignore the content information.

The debate over extending pen/trap authority, which is not based on probable cause, to Internet communications, is not about whether criminals or terrorists use the Internet. Of course they do. The question is how to ensure that Congress does not erode the privacy of everyone by authorizing surveillance techniques, not based on probable cause, that fail to account for the differences between traditional communications and Internet communications.

Because pen/trap authority as applied to the Internet is particularly intrusive, even with rules that define content more properly, Congress should insist that pen/trap orders require more specific justification. The ACLU urges adoption of the SAFE Act. Section 6(b) of the act would require, for FISA pen/trap authority, more than a simple certification that the information is relevant to a foreign intelligence investigation.

While the SAFE Act would not require probable cause for FISA pen/trap authority it adds teeth to the relevance test. The SAFE Act would require the government to provide a "statement by the applicant of specific and articulable facts showing there is reason to believe" the information obtained by the pen/trap device is relevant to the investigation.

CONCLUSION: RESTORING CHECKS AND BALANCES

The Patriot Act provisions that pose the greatest challenges share certain common themes. As a result of gag orders, or delayed notification, they permit surveillance with a far greater degree of secrecy than is common in most government investigations. They do not allow affected parties the opportunity to challenge government orders before a judge. Finally, because the substantive standards for some forms of surveillance have been modified, weakened, or even eliminated, the role of the Foreign Intelligence Surveillance Court in checking government abuse has been made less meaningful.

This committee's review of the Patriot Act and related legal measures in the ongoing effort to combat terrorism is needed to ensure continued public support for the government's efforts to safeguard national security. The controversy over the Patriot Act reflects the concerns of millions of Americans for preserving our fundamental freedoms while safeguarding national security. To date, resolutions in opposition to parts of the Patriot Act and other actions that infringe on fundamental rights have been passed in in 377 communities in 43 states including five state-wide resolutions.

Such widespread concern, across ideological lines, reflects the strong belief of Americans that security and liberty need not be competing values. Congress included a "sunset provision" precisely because of the dangers represented by passing such far-reaching changes in American law in the aftermath of the worst terrorist attack in American history. Now is the time for Congress to complete the work it began when it passed the Patriot Act, by bringing the Patriot Act back in line with the Constitution.

EXAMPLE OF PATRIOT ACT ABUSE—BRANDON MAYFIELD

On March 11, 2004 a bomb exploded in Madrid killing hundreds of people. The government obtained from Spanish authorities fingerprint images from a blue bag found at the scene containing seven detonators thought to be of the same type used in the bombing. The FBI concluded that the fingerprints matched those of a Portland attorney, Brandon Mayfield. He was arrested on May 6 on a material witness warrant.

Court documents show that Brandon Mayfield, a convert to Islam, was investigated at least in part because of his religion. For example, the material witness warrant alleged, among other things, that Mayfield, a Muslim, was seen driving from his home to the Bilal mosque, where he worshipped.

On March 24, 2005, the FBI admitted to Mayfield's attorney that his home had been secretly searched under the Foreign Intelligence Surveillance Act (FISA), which the Patriot Act amended. The FBI admitted that it copied four computer hard drives, digitally photographed several documents, seized 10 DNA samples and took approximately 335 digital photographs of the residence and Mr. Mayfield's property. At an April 5 hearing before the Senate Judiciary Committee, Attorney General Gonzales specified that Sections 207 and 218 of the Patriot Act had been used. Section 207 lengthened the allowable time allotted to the FBI to secretly search Mayfield's home. Section 218 makes it easier to use intelligence authorities in criminal cases.

The Patriot Act facilitated FISA search of Mayfield's home. Before the law's passage, the government could conduct a FISA search only if the "primary purpose" of the search was to gather foreign intelligence information. Under Section 218 of the Patriot Act, gathering such information need only be a "significant purpose" of a FISA search. The Mayfield search occurred directly after the Madrid bombing as part of the FBI's investigation. This suggests strongly that the "primary purpose" of the search was not to gather foreign intelligence information, but to uncover incriminating evidence.

Prior to the Patriot Act, authorities would not have been able to use FISA to conduct absolutely secret "black bag" intelligence searches where the primary purpose of the search was criminal investigation.

EXAMPLE OF PATRIOT ACT ABUSE—UNCONSTITUTIONAL NATIONAL SECURITY LETTERS

Section 505 of the Patriot Act expanded the government's authority to use National Security Letters (NSL's) to seize information from businesses and others, with no judicial approval. Prior to the Patriot Act, the government could use NSL's to obtain records about alleged terrorists or spies—people who were thought to be "foreign powers" or their agents. Financial, travel and certain Internet Service Provider (ISP) records are accessible under the NSL authority. Section 505 changed the law to allow the use of NSL's to obtain such records about anyone without the limitation that they be agents of foreign powers. In the Intelligence Authorization Act of 2004[15] Congress further expanded the NSL letter authority to permit seizure of casino and other records.

On a date that the government maintains must be kept secret for reasons of national security, the FBI served an NSL on an ISP the identity of which the government also claims must be kept secret for reasons of national security. Through its NSL authority at 18 U.S.C. Section 2709, the government can seek certain sensitive

[15] Pub. L. No. 108–177, Section 374 (Dec. 13, 2003).

customer records from ISPs—including information that may be protected by the First Amendment—but the ISP can never reveal that it has been served with an NSL, and nothing in the statute suggests that the NSL can be challenged in court. On behalf of the ISP and itself, the ACLU challenged the statute as amended by the Patriot Act, as a violation of the First and Fourth Amendments because it does not impose adequate safeguards on the FBI's authority to force disclosure of sensitive and constitutionally protected information and because its gag provision prohibits anyone who receives an NSL from disclosing in perpetuity and to any person even the mere fact that the FBI has sought information.

On September 28, 2004, Judge Victor Marrero of the Southern District of New York issued a landmark decision striking down as unconstitutional the NSL statute and its gag provision. The court struck down the entire statute as violative of Fourth and First Amendment rights, thus rendering any use of the statute an abuse of those rights. The court found that there have been hundreds of such uses.[16] It found that the statute was abusive in practice because it sanctioned NSL's that coerced immediate compliance without effective access to court review or an opportunity to consult with counsel:

> The form language of the NSL served upon [plaintiff ISP] Doe, preceded by an FBI phone call, directed him to *personally* provide the information to the FBI, prohibited him, his officers, agents and employees from disclosing the existence of the NSL to anyone, and made no mention of the availability of judicial review to quash or otherwise modify the NSL or the secrecy mandated by the letter. Nor did the FBI inform Doe personally that such judicial review of the issuance of the NSL or the secrecy attaching to it was available. The court concludes that, when combined, these provisions and practices essentially force the reasonable NSL recipient to immediately comply with the request.[17]

In finding the statute unconstitutional under the *Fourth* Amendment, Judge Marrero referred repeatedly to the amendments made by Section 505. He noted as an example of the kind of abuse now authorized by the statute that it could be used to issue a NSL to obtain the name of a person who has posted a blog critical of the government, or to obtain a list of the people who have e-mail accounts with a given political organization.[18] The government could not have obtained this information with an NSL prior to the Patriot Act amendment in Section 505, unless the blogger or the people with such accounts were thought to be foreign powers or agents of foreign powers. The court also cited Patriot Act Section 505 as a reason it struck down the statute on *First* Amendment grounds. The court determined that the tie to foreign powers—eliminated by Section 505—"limits the potential abuse" of the statute[19] and distinguishes it from other intelligence search provisions that retain the requirement of such a tie and include a statutory gag provision.

Because of the gag in 18 U.S.C. Section 2709(c), the government obtained a sealing order it has consistently used to suppress wholly innocuous information in the litigation. Until the court struck down the statute, the government prevented the ACLU from disclosing that it represented someone that had been served with an NSL, and from even acknowledging that the government had used a statutory power. The government has demanded that the ACLU redact a sentence that described its anonymous client's business as "*provid[ing] clients with the ability to access the Internet.*" Ironically, the government even insisted that the ACLU black out a *direct quote* from a Supreme Court case in an ACLU brief:

> "The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.' Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent."

The gag in Section 2709 would effectively prevent an ISP (or its lawyers) from disclosing other abuses of Section 2709. For example, if the government was targeting someone because of their First Amendment activity, or if the ISP was being

---

[16] *Doe* v. *Ashcroft*, (04 Civ. 2614, S.D.N.Y. Sept. 28, 2004), at 63–64. The court concluded that hundreds of NSL's had been requested by the FBI from October 2001 through January 2003, and hundreds must have been issued during the life of the statute. The government takes the position that even the number of NSL's it issues cannot be disclosed for reasons of national security, though it has disclosed publicly to Congress a number of such uses. *See, e.g.* "H.R. 3179, The "Anti-Terrorism Intelligence Tools Improvement Act of 2003," Hearings Before the Subcomm. on Crime, Terrorism, and Homeland Security of the House Comm. on the Judiciary, 108th Cong. (2004) (statement of Thomas J. Harrington, Deputy Assistant Director of the FBI Counterterrorism Division).

[17] *Id.* at pp. 44–45.

[18] *Id.* at p. 75.

[19] *Id.* at p. 93.

forced to turn over First Amendment protected information about associational activities, the gag would bar disclosure of this abuse.

EXAMPLES OF THE CHILLING EFFECTS OF PATRIOT ACT SECTION 215

In July 2003, the ACLU filed suit on behalf of six community and non-profit organizations because it had learned of a serious chilling effect that resulted from Section 215 of the Patriot Act.[20] Excerpts from some plaintiffs' declarations highlight how Section 215 chills political speech and hinder privacy rights:

The president of a community association: "The enactment of Section 215 has significantly changed the way members of [the Muslim Community Association of Ann Arbor, or MCA] participate in the organization. Many previously active members have become passive ones. Attendance at daily prayer services, educational forums, and social events has dropped. Some members have totally withdrawn their membership from MCA. Charitable donations to MCA have decreased."[21]

A prominent member of the association: "Although I had been very outspoken politically before passage of the Patriot Act, I became afraid after the Patriot Act was passed that if I continued to remain a vocal and visible Muslim, the government would target me for investigation and seek private records about me even though I had not done anything wrong.

"While I was upset by several policies of the U.S. and would have ordinarily taken a leadership role in protesting these policies, I decided to step out of the limelight to lessen the chances that the government would target me for an investigation under the Patriot Act."[22]

The administrator of a Christian refugee aid organization: "Section 215 has harmed our ability to serve our clients in a number of different ways.

"Section 215 has caused Bridge to redirect resources from client assistance. Resources that we otherwise would have used to help clients are instead being used to re-evaluate our recordkeeping and record retention policies.

"Because we would not have an opportunity to challenge a Section 215 order before complying with it, we have had no choice but to act now to ensure that our records do not contain personal or other sensitive information that we could be forced to disclose to the government. Accordingly, my staff and I have been deciding on a case-by-case basis to exclude some sensitive information from our files.

"While we believe that we have no practical choice but to adopt this policy, there is no question that the practice compromises the level of services we can provide to our clients."[23]

---

[20] *Muslim Community Association of Ann Arbor* v. *Ashcroft*, Civil Action No. 03–72913 (E.D. Mich., filed July 30, 2003).

[21] Nazih Hassan Decl. ¶ 22.

[22] John Doe (Member of MCA) Decl. ¶¶ 8–9.

[23] Mary Lieberman Decl. ¶¶ 23–27.

Patriot Act Intelligence Authorities: Recommended Safeguards

Intelligence Surveillance Power	Before 9/11	Now	Sunsets?	Recommended safeguard (if power is retained)
FISA records FISA search orders ..... ***Patriot Act § 215***	FISA search orders were available only for certain travel-related ''business'' records on basis of individualized suspicion connecting records to foreign agent..	Now these orders are available for any and all ''tangible things,'' including library records, medical records, and other highly personal records, without individual suspicion..	Yes	Congress should enact legislation limiting such orders to where the FBI has ''specific and articulable facts'' connecting records to foreign agent. In addition, Congress should provide a right to challenge the order, limits on the secrecy order and a right to challenge that order, and notice and an opportunity to challenge the use of such information in court. ***SAFE § 4 (S. 737, 109th Cong.)***
National security letters (no court order required) for financial records, telephone and ISP bills, consumer credit reports.. ***Patriot Act § 505*** ***Intelligence Act for FY 2004 § 334***	Were available only where FBI could show ''specific and articulable facts'' connecting records to foreign agent..	Now available without individual suspicion; definition of ''financial records'' greatly expanded..	No	Congress shouild enact legislation that restores the requirement of individual suspicion, provides a right to challenge records demands, limits the secrecy order and provides for a right to challenge the secrecy order, and providing notice to persons when the governmennt seeks to use information from such demands against them in court. ***SAFE § 5***
FISA secret searches and wiretaps in criinal investigations. ***Patriot Act § 218***	Available only if ''primary purpose'' is to obtain foreign intelligence.	Permitted when ''primary purpose'' is criminal investigation, as long as ''a significant purpose'' is foreign intelligence.	Yes	Congress should clarify that FISC retains supervisory power to ensure FISA searches are not directed or controlled by criminal prosecutors ***codify In re All Matters, 218 F. Supp. 2d 611 (FISC 2002)***
	.....	.....	.....	Congress should enact legislation to give the defense access to FISA applications and warrants, subject to the national security protections in the Classified Information Procedures Act ***S. 1552 § 9 (108th Cong.); § 2528 § 401 (108th Cong.)***

Extended duration of FISA secret searches and wiretaps. ***Patriot Act § 207***	Electronic surveillance orders for 90 days, renewal for 90 days; physical search orders last 45 days.	Initial electronic surveillance for 6 months, renewals for 1 year; physical search orders last 90 days for U.S. persons and 6 months for foreign visitors and temporary residents.	Yes	Congress should extend the sunset of this provision and investigate whether shorter time periods to ensure continued court oversight are appropriate, and should increase appropriations to Justice Department and FISC to provide sufficient resources to process applications.
FISA secret searches and wiretaps without connection to foreign power. ***Intelligence Reform Act of 2004 § 6001***	All secret search and surveillance orders required probable cause of connection to foreign power.	For non-U.S. persons, FISA secret search or surveillance allowed for persons ''involved in international terrorism'' or ''preparations therefore'' without any foreign power connection.	Yes	Congress should allow the FISC to presume that a non-U.S. person involved in international terrorism is acting for a foreign government or organization, but should not make such a presumption mandatory or eliminate altogether the ''foreign power'' requirement ***Feinstein Amdt. to S. 113 (108th Cong.)***
FISA roving wiretaps ..... ***Patriot Act § 206*** ***Intelligence Act for FY 2002 § 314***	No roving wiretaps under FISA, but were available for criminal investigations.	Now there are FISA roving wiretaps, but unlike criminal roving wiretaps, FISA roving wiretaps do not need to specify target and agents need not ascertain target is using that telephone.	Yes	Congress should enact legislation that would require FISA roving wiretaps to observe same requirements as criminal roving wiretaps, i.e., they must (1) specify a target, and (2) would have to ascertain target is using that facility. ***Safe Act § 2***
FISA surveillance of the Internet, other communications without probable cause with pen/trap authority. ***Patriot Act § 214***	Available only for facilities used by agents of foreign power or those involved in international terrorism activities.	Can be used for more broadly, including for U.S. persons, and regardless of what facility is being monitored.	Yes	Congress should require rules that define content for the Internet more clearly and prohibit techniques that acquire content without probable cause. (no legislatove language)
	.....	.....	.....	Congress should require determination of relevance to be based on a statement of ''specific and articulable facts,'' not on mere certification ***SAFE Act § 6***

STATEMENT OF GREGORY T. NOJEIM, ASSOCIATE DIRECTOR AND CHIEF LEGISLATIVE COUNSEL, WASHINGTON LEGISLATIVE OFFICE, AMERICAN CIVIL LIBERTIES UNION

Mr. NOJEIM. Thank you, Chairman Roberts.

Chairman ROBERTS. Please understand that virtually every word of your very valuable testimony will be in the record and feel free to summarize and/or do what you deem appropriate under the circumstances.

Mr. NOJEIM. Thank you very much.

It's a pleasure to testify before you today on behalf of the ACLU about the intelligence-related provisions of the USA PATRIOT Act. I come before you mindful that today marks the 10-year anniversary of the Murrah Building in Oklahoma City. That crime and the attacks of September 11, 2001, underscore a sobering truth—terrorism has been with us for a long time; it will likely be with us for generations to come. The decisions that you make in the coming months about the PATRIOT Act will be taken with an eye toward that reality.

The PATRIOT Act became law only 45 days after the September 11 attacks. Though it acted swiftly, Congress in its wisdom included approximately 12 provisions of the Act that sunset on December 31, 2005. I would focus your attention on just three PATRIOT Act provisions. Two of them deal with records requests under FISA and the other with roving wiretaps.

The PATRIOT Act expanded two existing sections of law that allow the FBI to compel people in businesses to produce documents. Section 505 of the PATRIOT Act expanded the National Security Letter authority to allow the FBI to issue a letter compelling Internet service providers, financial institutions and consumer credit reporting agencies to produce records about people who use or benefit from their services. This power was later expanded to include records of car dealers, boat dealers, jewelers, real estate professionals, pawn brokers, and others.

Section 215 of the PATRIOT Act expanded a different provision of law to authorize the FBI to more easily obtain a court order requiring a person or business to turn over documents or things "sought for" an investigation to protect against international terrorism or clandestine intelligence activities.

In both cases, the PATRIOT Act removed from the law the requirement that the records produced pertain to an agent of a foreign power—that is, foreign countries, businesses, and terrorist organizations. This significantly expanded law enforcement access to records pertaining to Americans. In these days of data mining, one cannot ignore this stark fact: under these provisions the government can easily obtain records pertaining to thousands of Americans who have nothing to do with terrorism, so long as the records are sought for or are allegedly relevant to one of these investigations.

Neither of these statutes signals the recipient of a letter or order that the recipient can challenge in court. Both statutes indicate that the recipient can tell no one that the recipient has received the order or letter, and that includes any attorney with whom they might want to consult. In common parlance, the recipient is

gagged, and under the statutory language the gag stays in place forever.

We do not ask that you repeal either of these sections of the law. Rather, we ask that you restore the agent of a foreign power requirement and that you amend the statute to time-limit the gag, exempt attorney-client communications from it, and allow for court challenges. If these changes are made to the NSL statute, they would satisfy the court that struck down that statute as a violation of the First and the Fourth Amendment.

In addition, we ask that you conform the multi-point or roving wiretap authority that was created in the PATRIOT Act for intelligence wiretaps to the corresponding authority for roving wiretaps that appears in the criminal code. Doing this would entail borrowing from the criminal code the ascertainment requirement that ensures that law enforcement agents listen in only on the conversations to which the target is a party. It also entails requiring the government to specify in its application for a wiretap either identity of the person whose phone or computer would be tapped or to specify the facility that would be tapped.

In short, we're not asking that law enforcement tools be taken away, rather that they be made subject to reasonable checks and balances, such as meaningful judicial oversight and appropriate disclosure to the public of the use of the power.

Congress could easily adopt all of the reforms that I have mentioned and most of the reforms that I have mentioned in my written testimony by enacting the Security and Freedom Enhancement Act or SAFE Act, S. 737. This bipartisan legislation, co-sponsored by Senators Craig and Durbin, contains a series of carefully calibrated adjustments to the PATRIOT Act that would go a long way toward bringing it more into line with the Constitution and advancing the goal of keeping America both safe and free.

Thank you.

Chairman ROBERTS. We thank you. Mr. Dempsey, please.

[The prepared statement of Mr. Dempsey follows:]

PREPARED STATEMENT OF JAMES X. DEMPSEY, EXECUTIVE DIRECTOR, CENTER FOR DEMOCRACY & TECHNOLOGY[1]

Mr. Chairman, Sen. Rockefeller, Members of the Committee, thank you for the opportunity to testify at this important hearing. In CDT's view, there are few if any provisions in the PATRIOT Act that are per se unreasonable. We see not a single power in the Act that should sunset. The question before us—and it is one of the most important questions in a democratic society—is what checks and balances should apply to those powers. In our view, the investigative powers of the PATRIOT Act would be just as effective, maybe even more so, if subject to some basic checks and balances—

- particularized suspicion,
- a minimal factual showing,
- judicial approval,
- eventual notice to targets in a wider range of circumstances, and
- more detailed unclassified reporting to Congress.

In particular, we urge the Committee to enhance the role of the judiciary. We fully recognize that intelligence investigations must sometimes proceed with speed

[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 information privacy and security issues.

and that they often require secrecy. But in this age of cell phones, ubiquitous Internet access, encryption, BlackBerries and other communications technologies, it seems unnecessary to vest domestic intelligence agencies with extra-judicial powers. FBI agents and others operating domestically in intelligence matters—who have to seek supervisory approval for exercise of PATRIOT Act powers in almost all cases anyhow—could electronically prepare minimal fact-based applications for access to information, submit them to judges electronically, and receive approval electronically, promptly, efficiently, but with the crucial check provided by a neutral and detached magistrate.

CDT supports the Security and Freedom Enhancement (SAFE) Act, a narrowly tailored bipartisan bill that would revise several provisions of the PATRIOT Act. It would retain all of the expanded authorities created by the Act but place important limits on them. It would protect the constitutional rights of American citizens while preserving the powers law enforcement needs to fight terrorism.

PREVENTION OF TERRORISM DOES NOT REQUIRE SUSPENSION OF STANDARDS AND OVERSIGHT

At the outset, let me stress some basic points on which I hope there is widespread agreement:

• Terrorism poses a grave and imminent threat to our nation. There are people—almost certainly some in the United States—today planning additional terrorist attacks, perhaps involving biological, chemical or nuclear materials.

• The government must have strong investigative authorities to collect information to prevent terrorism. These authorities must include the ability to conduct electronic surveillance, carry out physical searches effectively, and obtain transactional records or business records pertaining to suspected terrorists.

• These authorities, however, must be guided by the Fourth Amendment, and subject to Executive and judicial controls as well as legislative oversight and a measure of public transparency.

SINCE 9/11, THERE HAVE BEEN EGREGIOUS AND COUNTERPRODUCTIVE ABUSES OF CIVIL LIBERTIES AND HUMAN RIGHTS OUTSIDE THE PATRIOT ACT

Since 9/11, the Federal Government has engaged in serious abuses of constitutional and human rights, some now documented in official reports. The most egregious of these abuses have taken place outside of the PATRIOT Act or any other Congressional authorization. These include:

• The torture at Abu Ghraib and other locations.

• The detention of US citizens in military jails without criminal charges.

• The detention of foreign nationals in Guantanamo and other locations, under what the executive branch claimed was unreviewable authority, and the continuing detention of those individuals after the Supreme Court rejected the Administration's claims.

• The rendition of detainees to other governments known to engage in torture.

• Haphazard and prolonged post 9/11 detentions of foreign nationals in the U.S., the physical abuse of some and the blanket closing of deportation hearings.

• Abuse of the material witness law to hold individuals in jail without charges.

CONCERNS WITH THE PATRIOT ACT: INTELLIGENCE SEARCHES—BROADER SCOPE AND GREATER SECRECY CALL FOR COMPENSATING CONTROLS

In the PATRIOT Act, not surprisingly given the pressures under which that law was enacted and the lack of considered deliberation, the pendulum swung too far, and Congress eliminated important checks and balances that should now be restored in the interest of both freedom and security. One of the most fundamental themes of the PATRIOT Act was the elimination of checks and balances on intelligence access to financial, communications and other records.

As this Committee well knows, the FBI operates under two sets of authorities when investigating international terrorism: criminal and foreign intelligence/counterintelligence. Over the past 25 years, a series of intelligence authorities have grown up giving investigators the ability to conduct electronic surveillance and obtain access to stored records.

Constitutionally speaking, there are two concerns with national security authorities:

• The scope of intelligence investigations is broader than criminal investigations. Intelligence investigations cover both legal and illegal activities. In criminal investigations, the criminal code provides an outer boundary, and a prosecutor is often involved to guide and control the investigation. An intelligence investigation is driven not by a desire to arrest and convict, but by a range of foreign policy interests.

The breadth of disclosure of information is greater, including intelligence, military, diplomacy, policy development, protective, immigration, and law enforcement.

• Intelligence investigations require a greater degree of secrecy than criminal investigations. In criminal cases, an important protection is afforded by notice to the target and other affected parties as the government collects information and the notice and right to confront when a matter reaches trial. Under the intelligence rules, persons whose records are accessed by the government are never provided notice unless the evidence is introduced against them in court. While recipients of grand jury subpoenas can publicly complain about overbreadth and often can even notify the target, recipients of intelligence disclosure orders are barred from disclosing their existence.

The PATRIOT Act failed to include protections that can respond to these difference and provide appropriate protection of Fourth Amendment principles.

Particularized Suspicion and a Factual Basis for Disclosure Demands

In the PATRIOT Act, Sections 214 (relating to pen registers under FISA), 215 (relating to travel records and other business records) and 505 (relating to National Security Letters for credit reports, financial records and communications transactional data) all pose the same set of issues. Prior to the PATRIOT Act, the FBI was able to obtain access to certain key categories of information upon a showing that the information pertained to a foreign power or an agent of a foreign power:

• Real time interception of transactional data concerning electronic communications was available with a pen register or trap and trace order issued by the FISA court.

• Records regarding airline travel, vehicle rental, hotels and motels and storage facilities were available with a court order issued by the FISA court.

• Financial records, credit reports, and stored transactional records regarding telephone or Internet communications were available with a National Security Letter issued by a senior FBI official.

In all cases, prior to PATRIOT, these records were available upon a certification or showing that there were "specific and articulable facts" giving reason to believe that the person whose records were being sought was a foreign power or an agent of a foreign power, or had been in contact with a foreign power or its agent. The FBI complained that this standard was too narrow. Rather than come up with a focused standard, the PATRIOT Act eliminated both prongs of this standard: It eliminated the particularity requirement; and it eliminated the requirement that the FBI have any factual basis for its interest in certain records.

FBI and DOJ descriptions of these changes in guidance to the field and in statements to Congress suggest that the government does not interpret them as going as far as they seem to on their face. The FBI indicates that it still names particular subjects in its applications, and both DOJ and FBI indicate that there is some factual basis for every request.

The fact that records must be relevant to an open investigation is not any real protection at all. Consider the following: there is undoubtedly a properly authorized FCI investigation of al Qaeda (or UBL). Under sections 214, 215 and 505, the FBI could get any records from any entity by claiming that they were relevant to that investigation. Even though 215 requires a court order, the statute requires the judge to grant the governments request in whole or part so long as the government makes the proper assertion—that the records are sought for an existing investigation, however broad that investigation. There is no requirement that the application or the court order or NSL name the person or account for which information is sought.

Both the particularity requirement and the factual showing requirement should be made explicit in statute, in order to prevent overbroad or ill-focused searches and to provide clear guidance to the field and the FISA court.

At the same time, the concept of a National Security Letter should be revisited. in this age of cell phones, ubiquitous Internet access, encryption, BlackBerries and other communications technologies, it seems unnecessary to vest domestic intelligence agencies with extra-judicial powers. FBI agents and others operating domestically in intelligence matters—who have to seek supervisory approval for exercise of PATRIOT Act powers in almost all cases anyhow—could electronically prepare minimal fact-based applications for access to information, submit them to judges electronically, and receive approval electronically, promptly, efficiently, but with the crucial check provided by a neutral and detached magistrate.

Notice

A second area in which the PATRIOT Act lacks adequate protections is in the area of notice. Under the PATRIOT Act, as in the past, intelligence authorities are exercised under a cloak of perpetual secrecy. In the world of spy versus spy, surveil-

lances could go on for many years, the same techniques could be used in the same context for decades, and known spies would be allowed to operate with no overt action ever taken against them. To a certain extent, these secrecy interests remain paramount in counter-terrorism investigations. But the wall between intelligence and criminal has now been brought down, and information collected in intelligence investigations is now being ever more widely shared and used. The question of when and how individuals are provided notice needs to be reexamined. Especially individuals whose records were obtained by the government but who were later determined not to be of any interest to the government should be told of what happened to them.

In ordinary criminal investigations, the PATRIOT Act created what might be called "off the books surveillance." Section 212 authorizes an ISP to disclose e-mail, stored voicemail, draft documents and other stored information to law enforcement when government states that there is an emergency involving a threat to life. Section 217 authorizes the government to carry out real-time surveillance when an ISP, a university, or another system operator authorizes the surveillance on the grounds that there is a "trespasser" within the operator's computer network. Under both sections 212 and 217:

- There is never a report to a judge. (In contrast, under both Title III and FISA, when electronic surveillance is carried out on an emergency basis, an application must be filed after the fact.)
- There is no time limit placed on the disclosures or interceptions. (A Title III wiretap cannot continue for more than 30 days without new approval.)
- There is never notice to the person whose communications are intercepted or disclosed.
- The interceptions and disclosures are not reported to Congress.

DOJ, in its defense of Section 217 claims that the privacy of law-abiding computer users is protected because only the communications of the computer trespasser can be intercepted. But what if the system operator is wrong? What if there is a legitimate emergency, but law enforcement targets the wrong person. Under Sections 212 and 217, a guilty person gets more notice than an innocent person—the guilty person is told of the surveillance or disclosure but the innocent person need never be notified. That should be rectified.

Congressional Oversight and Public Reporting

Currently, the Justice Department is required to report to Congress on its use of some sections of the PATRIOT Act, such as its use of Section 215, but it is not required statutorily to report on its use of other sections. Although the Justice Department, under the pressure of the sunsets and with considerable prodding from Congress, has voluntarily reported some information on its use of other PATRIOT Act powers, like delayed notice warrants under Section 213, routine and more detailed reporting would increase both Congressional oversight and public transparency. Congress should codify reporting requirements, enabling Congress and the public to assess the efficacy of these provisions and to gauge the likelihood of their misuse.

SPECIFIC PROVISIONS OF THE PATRIOT ACT

In this section, we will comment on specific provisions of the PATRIOT Act.

Sneak and Peek Searches

Section 213, which does not sunset but nevertheless should be re-examined, is a good idea gone too far. It is also a perfect example of how the PATRIOT Act was used to expand government powers, without suitable checks and balances, in areas having nothing to do with terrorism. Finally, it illustrates how, when rhetoric is left behind, it is possible to frame appropriate checks and balances for what, by any definition, are some especially intrusive powers.

As a starting point, of course, in serious investigations of international terrorists, the government should be able to act with secrecy. But guess what proponents of Section 213 never mention? In international terrorism investigations, even before the PATRIOT Act, the government already had the authority to carry out secret searches. The Foreign Intelligence Surveillance Act was amended in 1994 to allow secret searches in intelligence investigations, including international terrorism cases; before 1994, the Attorney General authorized secret searches in intelligence investigations of terrorist groups without any judicial scrutiny. And during the limited debate over the PATRIOT Act, reasonable voices proposed that secret searches be statutorily authorized in criminal investigations of terrorism.

As enacted, however, Section 213 was not limited to terrorism cases. It would astound most Americans that government agents could enter their homes while they are asleep or their places of business while they are away and carry out a secret

search or seizure and not tell them until weeks or months later. It would especially astound them that this authority is available for all Federal offenses, ranging from weapons of mass destruction investigations to student loan cases. That is what Section 213 of the PATRIOT Act authorizes. Indeed, the Justice Department has admitted that it has used Section 213 sneak and peek authority in nonviolent cases having nothing to do with terrorism. These include, according to the Justice Department's October 24, 2003 letter to Senator Stevens, an investigation of judicial corruption, where agents carried out a sneak and peek search of a judge's chambers, a fraudulent checks case, and a health care fraud investigation, which involved a sneak and peek of a home nursing care business.

Section 213 fails in its stated purpose of establishing a uniform statutory standard applicable to sneak and peek searches throughout the United States. For a number of years, under various standards, courts had allowed delayed notice of sneak and peek searches. The term "sneak and peek," by the way, was not contrived by opponents of the PATRIOT Act—before the PATRIOT Act, it was used by FBI agents, DOJ officials, and judicial opinions. Rather than "codifying existing case law under a single national standard to streamline detective work," Section 213 confuses the law. Rather than trying to devise a standard suitable to breaking and entering into homes and offices for delayed notice searches, Congress, in the haste of the PATRIOT Act, merely incorporated by reference a definition of "adverse result" adopted in 1986 for completely unrelated purposes, concerning access to e-mail stored on the computer of an ISP. Under that standard, not only can secret searches of homes and offices be allowed in cases that could result in endangering the life of a person or destruction of evidence, but also in any case that might involve "intimidation of potential witnesses" or "seriously jeopardizing an investigation" or "unduly delaying a trial." These broad concepts offer little guidance to judges and will bring about no national uniformity in sneak and peek cases.

Section 213 also leaves judges guessing as to how long notice may be delayed. The Second and Ninth Circuits had adopted, as a basic presumption, a 7-day rule for the initial delay. Section 213 says that notice may be delayed for "a reasonable period." Does this mean that lower courts in the Ninth Circuit and the Second Circuit no longer have to adhere to the 7-day rule? At the least, it suggests that courts outside those Circuits could make up their own rules. "Reasonable period" affords judges considering sneak and peek sneak and peek searches no uniform standard.

If, as Section 213 supporters claim, sneak and peek searches are a "time-honored tool," and if courts "around the country have been issuing them for decades," as DOJ claims, why did the Justice Department push so hard in the PATRIOT Act for a Section 213 applicable to all cases? The answer, I believe, is that the sneak and peek concept stands on shaky constitutional ground, and the Justice Department was trying to bolster it with Congressional action—even action by a Congress that thought it was voting on an antiterrorism bill, not a general crimes bill.

The fact is, there is a constitutional problem with Section 213: The sneak and peek cases rest on an interpretation of the Fourth Amendment that is no longer valid. The major Circuit Court opinions allowing sneak and peek searches date from the 1986, *United States* v. *Freitas,* 800 F.2d 1451 (9th Cir.), and 1990, *United States* v. *Villegas,* 899 F.2d 1324 (2d Cir.). These cases were premised on the assumption that notice was not an element of the Fourth Amendment. *United States* v. *Pangburn,* 983 F.2d 449, 453 (2d Cir. 1993) starts its discussion of sneak and peek searches stating: "No provision specifically requiring notice of the execution of a search warrant is included in the Fourth Amendment." *Pangburn* goes on to state "The Fourth Amendment does not deal with notice of any kind. . . ."

Yet in *Wilson* v. *Arkansas,* 514 U.S. 927 (1995), in a unanimous opinion by Justice Thomas, the Supreme Court held that the knock and notice requirement of common law was incorporated in the Fourth Amendment as part of the constitutional inquiry into reasonableness. Notice is part of the Fourth Amendment, the court held, directly repudiating the premise of the sneak and peek cases. *Wilson* v. *Arkansas* makes it clear that a search without notice is not always unreasonable, but surely the case requires a different analysis of the issue than was given it by those courts that assumed that notice was not a part of the constitutional framework for searches at all. A much more carefully crafted set of standards for sneak and peek searches, including both stricter limits of the circumstances under which they can be approved and a 7-day time limit, is called for.

Section 213's attempted codification of the sneak and peek authority went too far. To fix it, Congress should leave the statutory authority in place but add several limitations:

• Congress should narrow the circumstances in which notification may be delayed so that Section 213 does not apply to virtually every search. Under Section 213, the government need only show that providing notice would seriously jeopardize an in-

vestigation or unduly delay a trial. This "catch-all" standard could apply in almost every case and therefore is simply too broad for this uniquely intrusive type of search. Congress should allow sneak and peek searches only if giving notice would likely result in: danger to the life or physical safety of an individual; flight from prosecution; destruction of or tampering with evidence; or intimidation of potential witnesses.

• Congress should require that any delay in notification not extend for more than 7 days without additional judicial authorization. Section 213 permits delay for a "reasonable time" period, which is undefined in the statute. Pre-PATRIOT Act case law in the Ninth and Second Circuits stated that 7 days was an appropriate time period. Indeed, DOJ' s internal guidance recognizes that 7 days is the most common period, but also suggests that it may seek much longer delays. Congress should set a basic 7 day rule, while permitting the Justice Department to obtain additional 7-day extensions of the delay if it can continue to meet one of the requirements for authorizing delay in the first instance.

• Section 213 only requires a judge to find "reasonable cause" to believe that an adverse result will happen if notice is not delayed. The Supreme Court has allowed a limited exception to the notice rule upon "reasonable suspicion," by allowing police to enter and provide notice as they were entering when they faced a life-threatening situation in executing a warrant. *Richards* v. *Wisconsin,* 520 U.S. 385 (1997). If "reasonable suspicion" is the standard for delaying notice by minutes, probable cause would be a more appropriate standard when notice is delayed for days or weeks.

• Finally, Congress should require the Justice Department to continue to report on its use of the "sneak and peek" power. Congress should codify a requirement that the Attorney General report the number of requests for delayed notification, the number of those requests granted or denied, the number of extensions requested, granted and denied, and the prong of the statutory test used for each case, so that Congress and the public can determine if this technique is being narrowly applied.

Even with these changes, sneak and peek searches, especially of homes, stand on shaky constitutional ground except in investigations of the most serious crimes. Judicial caution is necessary. The reasonable changes outlined above would leave the statutory authority in place but bring it under more appropriate limitations and oversight.

Section 215—Business Records

As noted above, Section 215 amended the Foreign Intelligence Surveillance Act to authorize the government to obtain a court order from the FISA court or designated magistrates to seize "any tangible things (including books, records, papers, documents, and other items)" that an FBI agent claims are "sought for" an authorized investigation "to protect against international terrorism or clandestine intelligence activities." The subject of the order need not be suspected of any involvement in terrorism whatsoever; indeed, if the statute is read literally, the order need not name any particular person but may encompass entire collections of data related to many individuals. The Justice Department often says that the order can be issued only after a court determines that the records being sought are "relevant" to a terrorism investigation, but the PATRIOT Act provision says only that the application must specify that the records concerned are "sought for" an authorized investigation. And the judge does not determine that the records are in fact "sought for" the investigation—the judge only can determine whether the FBI agent has said that they are sought for an investigation. The PATRIOT Act does not require that applications must be under oath. It doesn't even require that the application must be in writing. It doesn't require, as for example the pen register law does, that the application must indicate what agency is conducting the investigation. Section 505 of the PATRIOT Act similarly expanded the government's power to obtain telephone and e-mail transactional records, credit reports and financial data with the use of a document called the National Security Letter (NSL), which is issued by FBI officials without judicial approval.

The Justice Department argues that Section 215 merely gives to intelligence agents the same powers available in criminal cases, since investigators in criminal cases can obtain anything with a subpoena issued on a relevance standard. First of all, as noted, a criminal case is at least cabined by the criminal code—something is relevant only if it relates to the commission of a crime. But on the intelligence side, the government need not be investigating crimes—at least for non-U.S. persons, it can investigate purely legal activities by those suspected of being agents of foreign powers.

There are other protections applicable to criminal subpoenas that are not available under Section 215 and the NSLs. For one, third party recipients of criminal

subpoenas can notify the record subject, either immediately or after a required delay. Section 215 and the NSLs prohibit the recipient of a disclosure order from ever telling the record subject, which means that the person whose privacy has been invaded never has a chance to rectify any mistake or seek redress for any abuse. Second, the protections of the criminal justice system provide an opportunity for persons to assert their rights and protect their privacy, but those adversarial processes are not available in intelligence investigations that do not end up in criminal charges.

Use of FISA evidence in criminal cases without full due process

Before the PATRIOT Act, there was no legal barrier to using FISA information in criminal cases. The wall between prosecutors and intelligence officers, as it evolved over the years, was a secret invention of the FISA court, the Department's Office of Intelligence Policy and Review, and the FBI, with little basis in FISA itself. It did not serve either civil liberties or national security interests. The primary purpose standard did not have to be changed to promote coordination and information sharing.

As a result of the PATRIOT Act and the decision of the FISA Review Court, criminal investigators are now able to initiate and control FISA surveillances. The number of FISA has gone up dramatically. The FISA court now issues more surveillance orders in national security cases than all the other Federal judges issue in all other criminal cases. In the past, when FISA evidence has been introduced in criminal cases, it has not been subject to the normal adversarial process. Unlike ordinary criminal defendants in Title III cases, criminal defendants in FISA cases have not gotten access to the affidavit serving as the basis for the interception order. They have therefore been unable to meaningfully challenge the basis for the search. Defendants have also been constrained in getting access to any portions of the tapes other than those introduced against them or meeting the government's strict interpretation of what is exculpatory. If FISA evidence is to be used more widely in criminal cases, and if criminal prosecutors are able to initiate and control surveillances using the FISA standard, then those surveillances should be subject to the normal criminal adversarial process. Congress should make the use of FISA evidence in criminal cases subject to the Classified Information Procedures Act. Congress should also require more extensive public reporting on the use of FISA, to allow better public oversight, more like the useful reports issued for other criminal wiretap orders.

Definition of "domestic terrorism"

The PATRIOT Act's definition of domestic terrorism is a looming problem. Section 802 of the Act defines domestic terrorism as acts dangerous to human life that violate any State or Federal criminal law and appear to be intended to intimidate civilians or influence government policy. 18 USC 2331(5). Under the PATRIOT Act, this definition has three consequences—the definition is used as the basis for:

- Seizure of assets (Sec. 806)
- Disclosure of educational records (Secs. 507 and 508)
- Nationwide search warrants (Sec. 219)

The definition appears many more times in Patriot II, where it essentially becomes an excuse for analysis and consideration. Congress should either amend the definition or refrain from using it. It essentially amounts as a transfer of discretion to the executive branch, which can pick and choose what it will treat as terrorism, not only in charging decisions but also in the selection of investigative techniques and in the questioning of individuals.

SAFE ACT

CDT strongly supports that the Security and Freedom Enhancement (SAFE) Act is a narrowly tailored bipartisan bill that would revise several provisions of the USA PATRIOT Act. It would retain all of the expanded authorities created by the PATRIOT Act but place important limits on these authorities. It would protect the constitutional rights of American citizens while preserving the powers law enforcement needs to fight terrorism.

Section 2—FISA Roving Wiretaps (Section 206 of the PATRIOT Act)

The SAFE Act would retain the PATRIOT Act's authorization of roving wiretaps and "John Doe" wiretaps under the Foreign Intelligence Surveillance Act (FISA), but would eliminate "John Doe" roving wiretaps, a sweeping power never before authorized by Congress. A "John Doe" roving wiretap does not identify the person or the phone to be wiretapped. The SAFE Act would also require law enforcement to

ascertain the presence of the target of the wiretap before beginning surveillance. This would protect innocent Americans from unnecessary surveillance.

Section 3—"Sneak & Peek" Searches (Section 213)

The SAFE Act would retain the PATRIOT Act's authorization of delayed notification or "sneak and peek" searches when one of an enumerated list of specific, compelling reasons to delay notice is satisfied. However, it would eliminate the catch-all provision that allows sneak and peek searches in any circumstances seriously jeopardizing an investigation or unduly delaying a trial. The SAFE Act would require notification of a covert search within 7 days, instead of the undefined delay that is currently permitted by the PATRIOT Act. A court could allow unlimited additional 21-day delays of notice in specific, compelling circumstances.

Section 4—FISA Orders for Library and Other Personal Records (Section 215)

The SAFE Act would retain the PATRIOT Act's expansion of the FISA records provision, which allowed the FBI to obtain "any tangible things" from any entity. However, it would restore a standard of individualized suspicion for obtaining a FISA order and create procedural protections to prevent abuses. The government would be able to obtain an order if they could show facts indicating a reason to believe the tangible things sought relate to a suspected terrorist or spy. As is required for grand jury subpoenas, the SAFE Act would give the recipient of a FISA order the right to challenge the order, require a showing by the government that a gag order is necessary, place a time limit on the gag order (which could be extended by the court), and give a recipient the right to challenge the gag order. The SAFE Act would require notice to the target of a FISA order if the government seeks to use the things obtained from the order in a subsequent proceeding, and give the target an opportunity to challenge the use of those things. Such notice and challenge provisions are required for other FISA authorities (wiretaps, physical searches, pen registers, and trap and trace devices).

Section 5—National Security Letters (Section 505)

The SAFE Act would restore a standard of individualized suspicion for using an NSL, requiring that the government have reason to believe the records sought relate to a suspected terrorist or spy: As is the case for grand jury subpoenas, the SAFE Act would give the recipient of an NSL the right to challenge the letter and the nondisclosure requirement, and place a time limit on the nondisclosure requirement (which could be extended by the court). As is the case for FISA authorities, the SAFE Act would give notice to the target of an NSL if the government seeks to use the records obtained from the NSL in a subsequent proceeding, and give the target an opportunity to challenge the use of those records.

Section 6—Pen Registers and Trap and Trace Devices (Section 216)

The SAFE Act would retain the PATRIOT Act's expansion of the pen/trap authority to electronic communications. In recognition of the vast amount of sensitive information that law enforcement can now access, the SAFE Act would create modest safeguards allowing increased Congressional, public, and judicial oversight of pen/trap usage. The SAFE Act would require additional Congressional reporting, require delayed notice to individuals who are targets of pen/traps (pen/trap targets currently receive no notice, unlike the targets of wiretaps), and slightly raise the burden of proof for obtaining pen/trap orders. Under the current standard, the government need only to certify that the information sought is relevant, a certification that a judge has no power to question. Under the revised standard, the government would have to show facts indicating a reason to believe that the information sought is relevant.

Section 7—Domestic Terrorism Definition (Section 802)

The PATRIOT Act's overbroad definition of domestic terrorism could include acts of civil disobedience by political organizations. While civil disobedience is and should be illegal, it is not necessarily terrorism. The SAFE Act would limit the qualifying offenses for domestic terrorism to those that constitute a Federal crime of terrorism, instead of any Federal or State crime, as is currently the case.

Section 8—FISA Public Reporting

The PATRIOT Act made it much easier for law enforcement to use FISA to conduct secret surveillance on American citizens regardless of whether they are suspected of involvement in terrorism or espionage and whether the primary purpose of the underlying investigation is intelligence gathering. In 2003, the most recent year for which statistics are available, the number of FISA wiretaps exceeded the number of criminal wiretaps for the first time since FISA became law. It is impor-

tant for Congress and the American people to learn more about how the FBI is using FISA since the passage of the PATRIOT Act. Therefore, the SAFE Act would require increased public reporting on the use of FISA.

CONCLUSION

In the debate over the PATRIOT Act, civil libertarians did not argue that the government should be denied the tools it needs to monitor terrorists' communications or otherwise carry out effective investigations. Instead, privacy advocates urged that those powers be focused and subject to clear standards and judicial review. The tragedy of the response to September 11 is not that the government has been given new powers—it is that those new powers have been granted without standards or checks and balances.

• Of course, the FBI should be able to carry out roving taps during intelligence investigations of terrorism, just as it has long been able to do in criminal investigations of terrorism. But the PATRIOT Act standard for roving taps in intelligence cases lacks important procedural protections applicable in criminal cases.

• Of course, the law should clearly allow the government to intercept transactional data about Internet communications (something the government was doing before the PATRIOT Act anyhow). But the pen register/trap and trace standard for both Internet communications and telephones, under both the criminal wiretap law and under FISA, is so low that judges are reduced to mere rubber stamps, with no authority to even consider the factual basis for a surveillance application.

• Of course, prosecutors should be allowed to use FISA evidence in criminal cases (they did so on many occasions before the PATRIOT Act) and to coordinate intelligence and criminal investigations (there was no legal bar to doing so before the PATRIOT Act). But FISA evidence in criminal cases should not be shielded from the adversarial process (as it has been in every case to date).

We need limits on government surveillance and guidelines for the use of information not merely to protect individual rights but to focus government activity on those planning violence. The criminal standard and the principle of particularized suspicion keep the government from being diverted into investigations guided by politics, religion or ethnicity. Meaningful judicial controls do not tie the government's hands—they ensure that the guilty are identified and that the innocent are promptly exonerated.

APPENDIX—OVERVIEW OF PATRIOT SUNSETS

Of over 150 provisions in the PATRIOT Act, only 16 provisions are covered by the sunset. Some of those covered are uncontroversial, while some of the most controversial provisions in the Act are not slated to sunset. The sunset does not apply to pending investigations.

Here's what the sunset covers—**bold** indicates those that are controversial in CDT's view—we have no objections to the others:

Sec. 201—certain terrorism crimes as wiretap predicates
Sec. 202—computer fraud as wiretap predicate
Sec. 203(b)—sharing criminal wiretap information w/intelligence agencies
Sec. 204—technical clarification of no conflict between Title III and FISA
Sec. 206—roving taps under FISA
Sec. 207—extending duration of FISA taps of non-us persons
Sec. 209—seizure of voice mail pursuant to warrant
Sec. 212—emergency disclosures of e-mail w/o a court order
Sec. 214—lowering standard for pen registers and trap and trace devices under FISA
Sec. 215—access to business records under FISA (the "library records" provision)
Sec. 217—interception of computer trespasser communications w/o a court order
Sec. 218—the "significant purpose" provision
Sec. 220—nationwide service of search warrant for electronic evidence
Sec. 223—civil liability for unauthorized disclosures of wiretap info
Sec. 224—the sunset provision itself
Sec. 225—immunity for compliance with FISA wiretap

A number of highly controversial PATRIOT provisions are not covered by the sunset, and deserve to be reconsidered by Congress, including:

Sec 203(a)—sharing grand jury information
Sec. 213—sneak and peek searches

Sec. 216—pen registers for the Internet
Sec. 358—exceptions to the financial privacy laws
Sec. 505—"National Security Letter" exceptions to privacy laws
Sec. 802—definition of domestic terrorism

STATEMENT OF JAMES X. DEMPSEY, EXECUTIVE DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. DEMPSEY. Mr. Chairman, Vice Chairman Rockefeller, Senators, good afternoon. Thank you for the opportunity to testify at this important hearing.

Let me start out by stressing that, in the view of the Center for Democracy and Technology, as a civil liberties advocacy organization, we see few, if any, provisions in the PATRIOT Act that are per se unjustified. We see not a single power in the Act that needs to sunset or go away entirely. However, there are serious and legitimate concerns with some of the provisions. That is understandable, given the haste with which the law was enacted.

In 2001, in response to some legitimate complaints of the Administration that the prior rules for counterterrorism investigations were unreasonable or were out of date or ill-suited to the threat of terrorism, Congress adopted the PATRIOT Act, but it really didn't come up with better rules. In the anxiety of those weeks after 9/11, Congress eliminated the old rules but didn't replace them with any new ones, giving the Executive branch too much latitude, in some cases almost carte blanche.

The question before this Committee and before the Congress between now and December is what checks and balances should apply to these powers. As I will explain later, the bipartisan SAFE Act introduced in the Senate offers a set of modest but significant reforms that will leave all the PATRIOT Act powers in place but add the checks and balances that were left behind in October 2001.

Unless reasonable checks and balances are added, I think there are some provisions of the PATRIOT Act that should continue to be subject to a sunset, perhaps another 5 years, until we can get those rules right. I think we have in front of us an opportunity to adopt those checks and balances.

Now, what do I mean by "checks and balances?" Experience shows that in both criminal and intelligence investigations governmental powers are most effectively exercised and civil liberties are best protected if the intrusive data-gathering powers of the government are subject to certain principles. First among these is particularized suspicion, by which I mean that the government should focus its effort on individuals that it has some reason to believe are involved in planning terrorist activities or are members of a terrorist group or have some connection with a terrorist group or have some information that might lead to a terrorist group. This isn't about the government waiting for the crime to occur. This is in the context of preventive action, but to have some particularized focus, some particularized suspicion.

Secondly, the factual basis that the government has to have to collect information doesn't have to be very detailed. We're not talking about anything close to probable cause. It can be as little as a shared address or the fact that someone received a phone call from or made a phone call to a suspected terrorist. There has to

be some minimum specificity based on some documentable fact. This is what the FBI sometimes refers to as the predicate.

Third, whenever feasible, intrusive data gathering or surveillance should have the prior approval of a judicial officer. I'll expand upon this a little bit more in a second. There may be emergency exceptions. Under the wiretap law, under FISA, there are emergency exceptions. By and large, the rule for access to both stored records and real-time communications should involve judicial approval.

Fourth, while secrecy is important and especially important in intelligence investigations, as a general rule individuals should eventually receive notice of what has happened to them, when information has been collected about them, at least when the information is used to make decisions about them, not in the intelligence context but in the criminal justice context, in the immigration context. This is the concept of notice.

Finally, of course, there needs to be congressional oversight, which I know this Committee takes very, very seriously, and the process that you are in the midst of now is certainly part of that, and you are to be congratulated on taking the care with looking at these laws. I also think there could be and needs to be some greater public oversight and accountability. I think it might actually to some extent increase trust in what the government is doing to actually have some more information about at least how often and to what extent these authorities are being used.

We have the broader scope of intelligence investigations that are not only focused on criminal activity, are not cabined-in by the definitions of the criminal law, can clearly be used to collect information about legal activities. They don't lead up to that crucible of the trial, with the checks and balances and the adversarial process that that affords. We have the greater degree of secrecy and necessity. The question is, what compensating controls can be adopted?

In considering specifically some of the investigative techniques of the PATRIOT Act, I think that there are five questions that you should ask. First of all, should the government have access to the information at issue? In almost every case, indeed I would say in every case covered by the PATRIOT Act, I don't question that the government should have the right to the information under certain circumstances.

Secondly, does the investigation require speed? Obviously, yes, sometimes it does. Does it require secrecy? Usually, but maybe not forever, but certainly secrecy. Saying that the government needs the information, and it needs it quickly sometimes and it has to operate within secrecy, doesn't answer the final two questions.

Who should be the approving officer for the technique, and what should be the standard of proof or the standard of justification for access to certain information?

As I said, in our view, the judicial officer is very important. In this age of cell phones and Blackberries and encryption and almost ubiquitous Internet access, it seems unnecessary to vest domestic intelligence agencies with extrajudicial powers. FBI agents and others operating domestically in intelligence matters, who have to seek supervisory approval for exercise of PATRIOT Act authorities anyhow, could electronically prepare a minimal fact-based applica-

tion, submit it electronically to judges, get the approval electronically.

We allow search warrants to be obtained by telephone, orally, the FBI agent on one end—in criminal cases—the judge on the other end. The FBI agent can write it down by hand on his end and just signify the judge's approval. That's considered to be a sufficient warrant under the Fourth Amendment. We can have the speed, with that neutral magistrate in there asking, "What is the factual basis for this? Explain to me a little bit why you think this particular information is relevant or necessary to an intelligence investigation."

The mere fact that there is an investigation is not sufficient, obviously, because we have some very broad investigations. There's clearly an ongoing investigation of Usama bin Ladin or UBL that's clearly a properly justified investigation. The mere fact of the investigation is not enough. Yet the PATRIOT Act says that the government can obtain pen registers, business records, and the transactional data available under National Security Letters just by saying, either to a judge or to itself, "We have an investigation and the information is sought for that investigation."

That really does not give the kind of focus and the kind of minimal check and balance that is appropriate for intruding upon privacy by conducting a pen register, accessing business records, et cetera.

We have concerns under the legislation as well with the roving tap authority. Clearly, there should be roving tap authority in intelligence cases of terrorist groups, just as there are criminal investigations of terrorist groups. As Mr. Nojeim pointed out, in trying to carry over the criminal concept of roving surveillance into the FISA—and they are somewhat different statutes, of course, that use different terminology—the roving tap concept was sort of pasted in, almost sort of shoe-horned into FISA, and I think a mistake was made in that process and some of the checks and balances were left out, and some of that may have been unintentional but certainly now is the time to go back and correct that. I would be happy to discuss in more length what I have in mind there.

Sneak and peek searches has been another controversial provision. This one is unrelated to intelligence investigations. The sneak and peek authority has existed for a number of years under FISA, so intelligence investigations have always had the sneak and peek authority. We're talking here about criminal investigations. The sneak and peek authority in the PATRIOT Act is not limited to terrorism investigations. It applies to all Federal criminal investigations.

The FBI used that to break into a judge's chambers about a year ago, using the PATRIOT Act to break into a judge's chambers and do a sneak and peek search. They went into an office of a health care provider in a Medicare investigation, sneak and peek. These are nonviolent crimes, and yet they were using PATRIOT Act authority, again without, in our view, adequate checks and balances.

Mr. Chairman, with that I will conclude. I'm happy to go into greater depth on some of the individual provisions—the use of FISA in criminal proceedings, et cetera. Thank you, Mr. Chairman.

Chairman ROBERTS. Mr. Dempsey, we thank you for your comprehensive statement. I am sure that some of those matters will be taken up by the questions. Let me just say that this open hearing is the first in a series of three that are designed to educate Members as the Senate considers the repeal of the sunset provisions and modifications to other intelligence authorities.

On Thursday, the Committee will hold a closed hearing on operational matters relating to the Act. Next Wednesday, we will hear from the Attorney General and the Director of the FBI and the Director of Central Intelligence.

Ms. MacDonald.

[The prepared statement of Ms. MacDonald follows:]

PREPARED STATEMENT OF HEATHER MACDONALD, SENIOR FELLOW, MANHATTAN INSTITUTE FOR POLICY RESEARCH, NEW YORK, NY

Thank you, Mr. Chairman and members of the Committee. My name is Heather Mac Donald. I am a senior fellow at the Manhattan Institute for Policy Research, a think tank in New York City. I have written extensively on homeland security for the *Washington Post*, the *Wall Street Journal*, the *Los Angeles Times*, and *City Journal*, among other publications. I appreciate the opportunity to testify today on this important topic.

The most powerful weapon against terrorism is intelligence. The United States is too big a country to rely on physical barriers against attack; the most certain defense is advanced knowledge of terrorist plans.

In recognition of this fact, Congress amended existing surveillance powers after 9/11 to ready them for the terrorist challenge. The signal achievement of these amendments, known as the Patriot Act, was to tear down the regulatory "wall" that had prevented anti-terrorism intelligence agents and anti-terrorism criminal agents from sharing information. That wall was neither constitutionally nor statutorily mandated, but its effect was dire: it torpedoed what was probably the last chance to foil the 9/11 plot in August 2001. Thanks to the Patriot Act, all members of the anti-terrorism community can now collaborate to prevent the next tertoristrike before it happens.

Besides dismantling the wall, the Patriot Act made other necessary changes to surveillance law: it extended to terrorism investigators powers long enjoyed by criminal investigators, and it brought surveillance law into the 21st century of cell phones and e-mail. Where the act modestly expands the government's authority, it does so for one reason only: to make sure that the government can gather enough information to prevent terrorism, not just prosecute it after the fact.

Each modest expansion of government power in the Patriot Act is accompanied by the most effective restraint in our constitutional system: judicial review. The act carefully preserves the traditional checks and balances that safeguard civil liberties; 4 years after its enactment, after constant monitoring by the Justice Department's Inspector General and a host of hostile advocacy groups, not a single abuse of government power has been found or even alleged.

This record of restraint is not the picture of the act most often presented in the media or by government critics, however. The Patriot Act has been the target of the most successful disinformation campaign in recent memory. From the day of its passage, law enforcement critics have portrayed it as an unprecedented power grab by an administration intent on trampling civil rights.

As lie after lie accumulated, the administration failed utterly to respond. As a result, the public is wholly ignorant about what the law actually does. Hundreds of city councils have passed resolutions against the act; it is a safe bet that none of them know what is in it. The Committee is to be congratulated for taking the time to get the truth out.

Though the charges against the Patriot Act have been dazzling in their number, they boil down to four main strategies. This afternoon I would like to dissect those strategies, with particular reference to the most controversial sections of the act: sections 215 and 213. Discredit the anti-Patriot Act strategies in those contexts, and you have the key for discrediting them in every other context.

STRATEGY #1: HIDE THE JUDGE

The most pervasive tactic used against the Patriot Act is to conceal its judicial review provisions, as witnessed in the campaign against section 215. Section 215 al-

lows anti-terror investigators access to business records in third party hands. The section may also be called the librarian's hysteria provision. The American Library Association has declared section 215 a "present danger to the constitutional rights and privacy of library users," though the section says not a word about libraries. Such hyperbole is standard, and completely unwarranted.

The section works as follows: Under Section 215, the FBI may ask the Foreign Intelligence Surveillance Court for permission to seek business records—the enrollment application of a Saudi national in an American flight school, say—while investigating terrorism. The section broadens the categories of institutions whose records the government may seek, on the post-9/11 recognition that lawmakers cannot anticipate what sorts of organizations terrorists may exploit. In the past, to trace the steps of a Soviet spy, it may have been enough to get hotel bills or storage-locker contracts (two of the four categories of records covered in the previous section of the Foreign Intelligence Surveillance Act that Section 215 amended); today, however, gumshoes may find they need receipts from scuba-diving schools or farm-supply stores to piece together a plot to blow up the Golden Gate Bridge.

Section 215 removed the previous requirement in FISA that the records concern an "agent of a foreign power," since the scope of an anti-terror investigation is hard to predict in advance. An unwitting bystander may have purchased fertilizer for a terrorist posing as an aspiring farmer; finding out whether and how much fertilizer was purchased may be an essential link in the investigative chain.

These commonsensical reforms of existing investigative power have called forth a crescendo of hysteria. The ACLU warns that with section 215, "the FBI could spy on a person because they don't like the books she reads, or because they don't like the websites she visits. They could spy on her because she wrote a letter to the editor that criticized government policy." Librarians, certain that the section is all about them, are scaring library users with signs warning that the government may spy on their reading habits.

The force of these charges rests on the strategy of hiding the judge. Critics of section 215 conceal the fact that any request for items under the section requires judicial approval. An FBI agent cannot simply walk into a flight school or a library and demand records. The bureau must first convince the Foreign Intelligence Surveillance Court that the documents are relevant to protecting against international terrorism. The chance that the FISA court will approve a 215 order because the FBI "doesn't like the books [a person] reads . . . or because she wrote a letter to the editor that criticized government policy" is zero. If the bureau can show, on the other hand, that someone using a library's computers was seen with other terror suspects in Lahore, Pakistan, and has traveled regularly to Afghanistan under a false passport, then the court may well grant an order to get the library's Internet logs. As Andrew McCarthy has pointed out, literature evidence was a staple of terrorism prosecutions throughout the 1990's. Terrorists read bomb manuals, and often leave fingerprints on pages spelling out explosive recipes that match the forensics of particular bombings (like the 1993 attack on the World Trade Center).

Before the FBI can even approach the FISA court, agents must have gone through multiple levels of bureaucratic review just to open an anti-terror investigation. And to get to the court itself, intelligence agents must first persuade the Justice Department's Office of Intelligence and Policy Review that a section 215 order is warranted, a process of persuasion that traditionally has taken months of vetting and voluminous documentation.

STRATEGY #2: INVENT NEW RIGHTS

Besides concealing judicial review requirements, anti-Patriot Act demagogues also invent new rights. A running theme of the campaign against section 215 is that it violates the Fourth Amendment right to privacy. But there is no Fourth Amendment privacy right in records or other items disclosed to third parties. A credit-card user, for example, reveals his purchases to the seller and to the credit-card company. He therefore has no privacy expectations in the record of those purchases that the Fourth Amendment would protect. As a result, the government, whether in a criminal case or a terror investigation, may seek his credit-card receipts without a warrant or "probable cause" to believe that a crime has been or is about to be committed.

Despite librarians' fervent belief to the contrary, this analysis applies equally to library patrons' book borrowing or Internet use. The government may obtain those records without violating anyone's Fourth Amendment rights, because the patron has already revealed his borrowing and web browsing to library staff, other readers (in the days of handwritten book checkout cards), and Internet service providers. It

is worth noting, however, that after all the furor raised about library users' privacy rights, section 215 has not once been used to obtain library or book store records.

It is the lack of a Fourth Amendment privacy interest in third party records that has allowed prosecutors for decades to seek business and library records without any judicial review whatsoever. Section 215, by requiring judicial review, is far more protective of privacy than longstanding subpoena power in ordinary criminal investigations. Patriot critics have provided no evidence that the subpoena power has been abused to spy on Americans' reading habits; there is no reason to believe that section 215 will be any more susceptible to abuse.

Recipients of a section 215 production order may challenge the order in court, as Attorney General Alberto Gonzales recently testified, but they may not disclose the order in public. This is perfectly appropriate. Pre-emptive terror investigations cannot be conducted in the news media. The government would seek a terror suspect's airplane itineraries, for example, not in order to prosecute a hijacking after it happens, but to pre-empt a hijacking before the fact. The battleground is not the courtroom but the world beyond, where speed and secrecy can mean life or death.

STRATEGY #3: CONCEAL LEGAL PRECEDENT

Attacks on the other most controversial section of the Patriot Act, section 213, illustrate the key ruse of concealing the act's legal precedents. Section 213 allows the government to delay notice of a search, something criminal investigators have been allowed to do for decades.

Say the FBI wants to plumb Mohammad Atta's hard drive for evidence of a nascent terror attack. If a Federal agent shows up at his door and says: "Mr. Atta, we have a search warrant for your hard drive, which we suspect contains information about the structure and purpose of your cell," Atta will tell his cronies back in Hamburg and Afghanistan: "They're on to us; destroy your files—and the infidel who sold us out." The government's ability to plot out that branch of Al Qaeda is finished.

To avoid torpedoing pre-emptive investigations, Section 213 lets the government ask a judge for permission to delay notice of a search. The judge can grant the request only if he finds "reasonable cause" to believe that notice would result in death or physical harm to an individual, flight from prosecution, evidence tampering, witness intimidation, or other serious jeopardy to an investigation. In the case of Mohammad Atta's hard drive, the judge will likely allow a delay, since notice could seriously jeopardize the investigation, and would likely result in evidence tampering or witness intimidation.

The government can delay notifying the subject only for a "reasonable" period of time; eventually officials must tell Atta that they inspected his hard drive.

Section 213 carefully balances traditional expectations of notice and the imperatives of pre-emptive terror and crime investigations. That's not how left- and right-wing libertarians have portrayed it, however. They present Section 213, which they have dubbed "sneak-and-peek," as one of the most outrageous new powers seized by former Attorney General John Ashcroft. The ACLU's fund-raising pitches warn:

> "Now, the government can secretly enter your home while you're away . . . rifle through your personal belongings . . . download your computer files . . . and seize any items at will. . . . And, because of the Patriot Act, you may never know what the government has done."

Notice the ACLU's "Now." Like every anti-213 crusader, the ACLU implies that section 213 is a radical new power. This charge is a rank fabrication. For decades, Federal courts have allowed investigators to delay notice of a search in drug cases, organized crime, and child pornography, for the same reasons as in section 213. Indeed, the ability to delay notice of a search is an almost inevitable concomitant of investigations that seek to stop a crime before it happens. But the lack of precise uniformity in the court rulings on delayed notice slowed down complex national terror cases. Section 213 codified existing case law under a single national standard to streamline detective work; it did not create new authority regarding searches. Those critics who believe that the target of a search should always be notified prior to the search, regardless of the risks, should have raised their complaints decades ago—to the Supreme Court and the many other courts who have recognized the necessity of a delay option.

Critics of Section 213 raise the spectre of widespread surveillance abuse should the government be allowed to delay notice. FBI agents will be rummaging around the effects of law-abiding citizens on mere whim, even stealing from them, allege the anti-Patriot propagandists. But the government has had the delayed notice power for decades, and the anti-Patriot demagogues have not brought forward a single case of abuse under delayed notice case law. Their argument against Section 213

remains purely speculative: It *could* be abused. But there's no need to speculate; the historical record refutes the claim.

Moreover, such wild charges against Section 213 "hide the judge." It is a Federal judge who decides whether a delay is reasonable, not law enforcement officials. And before a government agent can even seek to delay notice of a search, he must already have proven to a judge that he has probable cause to conduct the search in the first place. This is hardly a recipe for lawless executive behavior—unless the anti-Patriot forces are also alleging that the Federal judiciary is determined to violate citizens rights. If that's what they mean, they should come out and say it.

In fact, the recent history of government intelligence-gathering belies the notion that any government surveillance power sets us on a slippery slope to tyranny. There *is* a slippery-slope problem in terror investigations—but it runs the other way. Since the 1970's, libertarians of all political stripes have piled restriction after restriction on intelligence-gathering, even preventing two anti-terror FBI agents in the same office from collaborating on a case if one was an "intelligence" investigator and the other a "criminal" investigator. By the late 1990's, the bureau worried more about avoiding a pseudo-civil liberties scandal than about preventing a terror attack. No one demanding the ever-more Byzantine protections against hypothetical abuse asked whether they were exacting a cost in public safety. We know now that they were.

The libertarian certainty about looming government abuse is a healthy instinct; it animates the Constitution. But critics of the Patriot Act and other anti-terror authorities ignore the sea change in law enforcement culture over the last several decades. For privacy fanatics, it's always 1968, when J. Edgar Hoover's FBI was voraciously surveilling political activists with no check on its power. That FBI is dead and gone. In its place arose a risk-averse and overwhelmingly law-abiding Bureau, that has internalized the norms of restraint and respect for privacy.

This respect for the law now characterizes intelligence agencies across the board. Lieutenant General Michael V. Hayden, the nominee for Principal Deputy Director of National Intelligence, told this committee last week that the challenge for supervisors in the National Security Agency was persuading analysts to use all of their legal powers, not to pull analysts back from an abuse of those powers.

It is because of this sea-change in law enforcement culture that Patriot Act critics cannot point to a single abuse of the act over the last 4 years, and why they are always left to argue in the hypothetical.

STRATEGY #4: REJECT SECRECY

A subtext of many Patriot Act critiques is a refusal to grant any legitimacy to government secrecy. Recipients of document production orders in terror investigations—whether Section 215 orders or national security letters under the 1986 Electronic Communications Privacy Act—should be able to publicize the government's request, say the critics; targets of searches should be notified at the time of the search. Time and again, law enforcement critics disparage the Foreign Intelligence Surveillance Court, because its proceedings are closed to the public. The ACLU, for example, opposes the roving wiretap authority for terrorism investigations in the Patriot Act (Section 206), even though criminal investigators have long had the roving wiretap option, because Section 206 wiretaps "are authorized secretly without a showing of probable cause of crime." (Section 206 requests must demonstrate probable cause that the wiretap target is an agent of a foreign power and that he will be using the tapped communications devices.)

This transparent approach may satisfy those on the left and right who believe that the American people have no greater enemy than their own government, but it fails to answer the major question: how would it possibly be effective in protecting the country? The Patriot Act critics fail to grasp the distinction between the prosecution of an already committed crime, for which probable cause and publicity requirements were crafted, and the effort to pre-empt a catastrophic attack on American soil before it happens. For pre-emptive investigations, secrecy is of the essence. Opponents of the Patriot Act have never explained how they think the government can track down the web of Islamist activity in public.

These four strategies, in various combinations—hide the judge, invent new rights, conceal legal precedent, and reject secrecy—lie behind nearly all of the Patriot Act attacks. The crusade against Section 214, for example, which allows the government to record the numbers dialed from a phone if relevant to a terrorism investigation (the so-called pen register power), uses all four strategies. (A related section, Section 216, extends the longstanding rules on pen registers, to the 21st century technologies of e-mail. Section 216 allows the government to capture only an e-mail's routing and addressing information, not its content.)

Section 214 merely allows the agents investigating a terrorism case the same power that criminal investigators have. But the Electronic Frontier Foundation calls the section "a serious threat to privacy." This charge rests on inventing new rights. In fact, pen registers threaten no privacy rigths, as the Supreme Court has held, because there is no legitimate expectation of privacy in the numbers dialed from a phone, which are recorded already by telephone companies. Even though judicial authorization for a pen register is not constitutionally required, section 214 nevertheless mandates that the government obtain an order from the FISA court for their use. EFF dismisses the value of the court, however, because it "operates in total secrecy."

In conclusion, the Patriot Act is a balanced updating of surveillance authority in light of the new reality of catastrophic terrorism. It corrects anachronisms in law enforcement powers, whereby health care fraud investigators, for example, enjoyed greater ability to gather evidence than Al Qaeda intelligence squads. It created no novel powers, but built on existing authorities within the context of constitutional checks and balances. It protects civil liberties while making sure that intelligence analysts can get the information they need to protect the country. The law should be re-enacted.

STATEMENT OF HEATHER MACDONALD, SENIOR FELLOW, MANHATTAN INSTITUTE FOR POLICY RESEARCH

Ms. MACDONALD. Mr. Chairman, thank you very much. I'm honored to be here today and I hope both you and the Vice Chairman will eventually share your wonderful opening statements with us. I would look forward to reading them.

The PATRIOT Act has been subject to the most successful misinformation campaign in recent memory. From the day of its passage it was portrayed as an unprincipled power grab by an administration intent on trampling civil rights. As I've debated the Act across the country, I've been amazed by the universal ignorance about what the Act actually contains. I applaud the Committee for taking the time to finally get the facts out.

The PATRIOT Act recognizes the fundamental truth about terrorism. Our only weapon against it is intelligence. Accordingly, Congress, in passing the Act, amended existing surveillance powers to ready them for the terrorist challenge. Its most important contribution was tearing down the wall that prevented information-sharing among all terror investigators. Today, thanks to Congress, all members of the anti-terror community can collaborate to try to prevent the next strike before it happens.

The PATRIOT Act made other necessary changes to surveillance law as well. It extended to terrorism investigators powers long enjoyed by criminal investigators, and it brought our laws into the 21st century of cell phones and e-mail. Each of those changes was accompanied by the most powerful restraint we have in our Constitution, judicial review. The Act carefully preserves traditional checks and balances that safeguard civil liberties.

For that reason, after 4 years of constant review by the Justice Department's Inspector General and a host of hostile advocacy groups, not a single abuse of power has been found or even alleged.

Now I've observed four rhetorical strategies used to discredit the Act. I call them hide the judge, invent new rights, conceal legal precedents and oppose secrecy. I want to review these strategies in the context of the two most controversial provisions of the PATRIOT Act—section 215, the business records provision, and 213, delayed notice.

215 allows the government to get records in third party hands for terrorist investigations. It's been attacked as a massive viola-

tion of free speech. It's the librarians' hysteria provision. The librians are all convinced that the section is all about them, even though the Act doesn't mention libraries. What you never hear in the attacks on 215 is that the government cannot get any records without prior approval of the FISA Court. These are Article III judges who have pledged to protect our civil rights. They are not going to approve a search of somebody's records simply because the FBI doesn't like your reading habits, as the ACLU has alleged.

It's also been blasted as a violation of Fourth Amendment privacy rights. Now we're getting into my second strategy, which is to invent new rights. Courts have long held there is no Fourth Amendment privacy rights in records held by third parties. For that reason, prosecutors or grand juries—your fellow citizens—can get those same records without any judicial review whatsoever. Section 215 is actually more protective of rights than the criminal powers that pre-existed it.

Now the furor over section 213, the delayed notice provision, illustrates my third rhetorical strategy, which is concealing legal precedent. 213 allows the government to delay notice of a search—delay, not permanently put it off—if notice would have an adverse result such as witness intimidation, evidence tampering or jeopardizing an investigation.

This has been portrayed by the ACLU and other groups as a radical new power that's going to unleash government tyranny. The gall of this claim, frankly, astounds me, because 213 merely codifies two decades of existing judicial precedent. If delayed notice was the threat that its critics have made it out to be, we would have already heard about abuses that such a power leads to.

As with every other provision of the Act, the critics have not been able to bring forth a single example of abuse over the last 20 years of the delayed notice authority.

213 attacks also take advantage of the hide the judge strategy. You'll never hear that in order to even delay notice of a search first you need to go through your traditional probable cause hearing to justify a warrant and you need to persuade the judge that there is a necessity to delay notice.

Ultimately what drives much of the criticism is a deep suspicion of government secrecy, the fourth strategy—deny the need for secrecy. I constantly hear the FISA Court disparaged as a mere rubber stamp because its proceedings are closed to the public. Opponents of 213 and other provisions apparently believe that if the government is investigating Mohammad Atta, for example, he should be notified in advance that the government wants to search his hard drive. This line of attack shows a complete obliviousness to the fact that what we're doing here is not a criminal investigation after the fact but we're trying to pre-empt a terrorist attack before it happens. Speed and secrecy are of the essence in preventing an attack.

In conclusion, the PATRIOT Act is balanced. It's a reasonable response to the new threat of catastrophic terrorism. It has not led to a single abuse of civil rights. And it should be renewed.

Thank you very much for your attention.

Chairman ROBERTS. Ms. MacDonald, thank you very much for your statement.

Members will have 5 minutes in the first round and we will go to a second round if necessary.

I have a question in reference to section 218 and "significant purpose." I think everybody seems to agree with the Foreign Intelligence Surveillance Court review that the "significant purpose" certification standard was not really needed to tear down the information-sharing walls—and that's my word—created by the Department of Justice and adopted by the Foreign Intelligence Surveillance Court.

Nonetheless, the provision was the catalyst for policy changes that have greatly improved the FBI's ability to consult with prosecutors in national security investigations and share information both within the FBI and among other members of the intelligence community.

Now, Mr. Nojeim, as I read your recommendations, it appears that you want to—this are my words, probably not your description—rebuild the walls between the FBI and national security investigators and prosecutors and restore the Foreign Intelligence Surveillance Court, what I think is a misinterpretation of the law. Why do you think it's a bad idea for the FBI agents conducting national security investigations to be able to consult with prosecutors to the same extent as the FBI agents who are conducting the domestic criminal investigation? How is it an end run around the Fourth Amendment to use FISA to pursue a terrorist group like the al-Qa'ida or spies like Robert Hansen?

Mr. NOJEIM. I never said in my testimony that they shouldn't be allowed to consult. What I did say was that the risk to the Fourth Amendment is this: FBI agents believe that such-and-such a person has committed a terrible crime. They want to search the person's home and they want to wiretap the person to get evidence of that crime, and to put him behind bars.

Normally they would have to go in front of a judge and show probable cause of crime. Under the "significant purpose" test, if they also have an intelligence rationale they no longer have to do that. Eventhough they are looking for evidence of a crime, they never have to show probable cause of crime because they can go around that requirement, search the home or eavesdrop on the telephone conversation if they meet the intelligence rationale under the PATRIOT Act and that intelligence gathering is a significant purpose of the surveillance.

There is a problem. We have to admit that there is a problem about going around the Fourth Amendment. The issue is how do we deal with that problem. We suggest three things. The first I hope is easy. It's increased public reporting. We're not asking for the FBI to disclose sources and methods of intelligence gathering. Even the raw numbers of searches that involve the use of this power is not disclosed. Even whether the person who is being surveilled is a U.S. person, a citizen, or a lawful permanent resident, that's not disclosed either. So disclosure is one thing that needs to happen.

Another thing that needs to happen——

Chairman ROBERTS. If you can do the two real quickly, I've got a yellow light and I want to turn to Ms. MacDonald.

Mr. NOJEIM. Another thing that needs to happen is making it so that the person who is accused of a crime based on that information that's gathered in that intelligence surveillance can get access to the application that was used to gather that information. There's a ready process under the Classified Information Procedures Act that could be grafted onto the statute to make it work better.

Ms. MACDONALD. Can I just respond?

Chairman ROBERTS. Ms. MacDonald.

Ms. MACDONALD. Mary Jo White, who before 9/11 was the most seasoned al-Qa'ida prosecutor, told me that there was no greater barrier to fighting terrorism than the wall. She said it was something that they beat their heads against all the time. The idea that the process of going before the FISA Court is some flippant, easy way to have a run around the Fourth Amendment is absurd.

You need massive clearance within the FBI. Then you have to persuade the Office of Intelligence and Policy Review to bring your case before the FISA Court. I believe it was the Senate Select Committee itself that, several years before 9/11, was extremely concerned with the hurdles that were being placed by OIPR on FISA requests from the field.

I think we also forget that there has been a massive sea change in law enforcement culture. For the civil liberties advocates, it's always 1968. We always have J. Edgar Hoover trampling civil rights. In fact, let's be honest. Law enforcement, the FBI, has internalized norms of restraint. As General Hayden told you last week, his challenge within the NSA was to try and persuade his agents to use their powers, not to pull them back from an abuse of power.

The FISA process is basically, as the first head of OIPR, Mr. Bass, Kenneth Bass, said, it's basically a probable cause warrant.

Chairman ROBERTS. Senator Rockefeller. Thank you, Ms. MacDonald.

Vice Chairman ROCKEFELLER. Thank you, Mr. Chairman.

Perhaps I could ask this question of each of you and then have you rebut each other, all in 5 minutes. The liveliest part of this controversy is what we've just been talking about, and that's 215 on access to records. It's about the librarians, named, unnamed. Booksellers have been concerned about it. It's not limited to libraries and books.

Now we have read and we have heard your separate arguments about that section. It would be helpful to each of us to hear those arguments side by side. Would you each take a minute to state your main point about section 215 and then a half minute to rebut what others say about that—a side-by-side approach.

Ms. MACDONALD. 215 gives the government access to business records that a criminal prosecutor already had access to for the mere after-the-fact investigation of a crime. This allows terrorism investigators to have access to those same records. It requires FISA Court approval. The fact that it removed the four narrow categories merely acknowledges the fact that we cannot predict the next terror attack.

Who would have known that it would have been nice to have had flight school records before 9/11? Under 215 the government can get flight school records and it's not confined to storage lockers.

Mr. NOJEIM. Prior to the PATRIOT Act and after the PATRIOT Act the government had the power to, when it was investigating a crime, get a criminal subpoena. It could do that for terrorism crimes; it could do that for other crimes. It's inaccurate to imply that it couldn't do it for terrorism crimes.

What we would like to see on section 215 is an increase in the standard of review. In particular, the notion that when the records are "sought for" an investigation is a very, very low standard. In addition, we suggest that these records requests be limited to records that pertain to an agent of a foreign power. We say that we want to restore the "agent of a foreign power" standard, and again this has nothing to do with information-sharing, which we do not oppose, when we say restore the "agent of a foreign power" standard, we say that because it protects records about people who have nothing to do with terrorism, and they are mostly Americans.

Vice Chairman ROCKEFELLER. Mr. Dempsey.

Mr. DEMPSEY. Senators, as I said in my opening remarks, there's not a category of records that I can think of that the FBI shouldn't have access to in intelligence investigations. The expansion of 215 from some limited categories of records to any records, including library records, was appropriate. Libraries aren't really the issue, as we all know, and if there is something at a library that's valid and useful, the government should have access to that as well.

The question is, shouldn't there be some factual basis for the government's request. I think the one-to-one comparison between the criminal side, where there are lots and lots of checks and balances all the way to right to counsel and the adversarial process, you get a subpoena, you can scream bloody murder about it, but these are secret. We have to have something compensating for that.

The judge right now is a rubber stamp. If the government says we want them and signs a piece of paper, the judge has to approve it and does approve it, and there's——

Vice Chairman ROCKEFELLER. Do you disagree with that, Ms. MacDonald?

Ms. MACDONALD. I disagree. The language in 215 is identical to the pre-PATRIOT language on the standard of review. Under that standard pre-PATRIOT, there was still the months-long vetting on OIPR. In fact, there is basically, in practice, a factual predicate. That certification language is no different. Either there was the same problem pre-PATRIOT and we didn't know about it, or it's not a problem at all.

As for restoring the "agent of a foreign power" standard, I think that would be a great mistake, for the same reason that I mentioned why we're expanding the documents. We can't predict in advance what the contours of a terror investigation are going to be. Somebody may have unwittingly bought fertilizer for a suspected terrorist. Under the agent of a foreign power standard, you're not going to be able to get those records of a farm supply store because it's not his records that you're looking for. It's a third party that's bought them.

Finally, again there's no Fourth Amendment interest in records in third party hands. A prosecutor can already get them. They are no more available under the PATRIOT Act than they were before the PATRIOT Act.

Vice Chairman ROCKEFELLER. My time is up, Mr. Nojeim, but I will come back to you on the second round because I excluded you and I didn't mean to.

Mr. DEMPSEY. Senator, could I have just one quick clarification?

Vice Chairman ROCKEFELLER. No, because we're being very strict about time. We will have a second round.

Mr. DEMPSEY. Of course.

Chairman ROBERTS. See, I was going to grant that, but this man is just an absolute tyrant with time, as you can see.

[Laughter.]

Chairman ROBERTS. Actually, he's a heavy-handed despot, but I'm not going to get into that any further.

Senator Lott.

Senator LOTT. Thank you, Mr. Chairman. Thank you for your restraint that you've been exercising throughout this hearing. I thank the panel for being here.

I must say to you, Ms. MacDonald, how impressed I am with your credentials and your resume and your testimony here today. I'm glad to hear somebody take the position that I agree with very strongly.

The PATRIOT Act is coming up for reauthorization. We need to listen to complaints. We need to review how it has worked. I found it completely telling when you note, for instance, after constant monitoring by the Justice Department Inspector General and all kind of hostile advocacy groups horrified at what might happen, not a single abuse has occurred or been seriously alleged.

That is what you're saying.

Ms. MACDONALD. That is what I'm saying. We've heard none today either. It's not just under the PATRIOT Act. Again, the most interesting issue for me is the delayed notice provision. We've had 20 years of delayed notice power that is now causing the public to fear that the FBI's going to be rummaging around their underwear drawer and not a single abuse has occurred for the last 20 years.

Again, I think what this speaks to is the sea change in law enforcement culture and the fact that the checks and balances that exist before the PATRIOT Act and certainly exist after the PATRIOT Act are working.

Senator LOTT. Let me ask you to do this, then. As we look at this Act, let's not just look at some of the complaints about it. Let's look at are there some ways that maybe we could strengthen it even further, that would be helpful in trying to provide additional surveillance or investigative authorities that might help us to combat terrorism.

Have you thought about that?

Ms. MACDONALD. I'm not going to take that on, Mr. Lott. It's hard enough to defend what exists. I know that the FBI has been asking for administrative subpoena power. I'm basically agnostic on that.

Senator LOTT. Well, with your presentation and with your credentials, I hope you'll meditate about that and think about it and see how maybe we can make it even better by making it stronger in some areas where maybe there are some weaknesses.

Ms. MACDONALD. I would say probably what would be more important is the political branches sending a message to law enforce-

ment that they will be supported, if they are acting in good faith, that they don't need to worry about the hypothetical trumping up of civil liberties concerns, that the government, people like yourself, will support them in the full exercise of their power.

Senator LOTT. You know, you cannot be agnostic about privacy issues and protecting individual citizens' privacy rights. My question is, I guess, are there sufficient safeguards in this Act as it now exists?

Ms. MACDONALD. We have no stronger safeguard in our Constitutional system than judicial review. The FISA Court operates in secret, that's true, as it must. There is simply no way that you can conduct a pre-emptive terror investigation in public. You cannot have C-SPAN and CNN covering the proceedings before the FISA court and think that we're going to be able to beat this enemy.

There is judicial review throughout the PATRIOT Act, whether it's before the FISA Court or before a regular Article III court. Again the results speak for themselves.

Mr. DEMPSEY. Senator, may I respond?

Senator LOTT. Mr. Dempsey, I was going to ask if you have any comment on either of my two questions.

Mr. DEMPSEY. Yes, sir. First of all, in terms of the abuses, when a provision says that the government gets anything they want just for asking for it, I don't see how that can be abused. I honestly don't. A standardless law, it's hard to say there's an abuse, and that is some of what we're talking about here.

Now I think there have been what I would call abuses. I think using the PATRIOT Act to break into a judge's chambers and conduct a secret search in a non-terrorism case involving no threat of life and no intimidation or likelihood of intimidating witnesses, I don't think that that's what members of this body thought they were voting for when they approved the PATRIOT Act. I think that's an abuse.

It's within the four corners of the law, but I think that's an abuse of the concept of this emergency legislation that was passed to address a compelling national security threat. I think that other of these provisions are so broadly written that they cannot be abused. I think they should be narrowed.

Ms. MacDonald was referring to the judges. This law says that if an FBI agent comes in with a signed piece of paper saying—actually, it's interesting. It doesn't even say it has to be in writing. It doesn't even say that the officer has to name himself. If you compare this to some of the other laws on our books, some of the subpoena laws or the pen register statute for criminal cases, it has to be in writing. This doesn't even say it has to be in writing. It doesn't say he has to even name the case.

All he has to do is come in and say, "I want these records for an intelligence investigation," and the law says upon application, oral application probably, the judge shall enter an ex parte order as requested or as modified, period. Why even have the judge in that case? That's a rubber stamp.

Now one thing that's interesting—and Ms. MacDonald referred to this earlier—if you actually look at the FBI's guidance on how to interpret this, it's actually better than the text of the law. The FBI guidance on this does say that they always have, internally at

least, a factual basis and they always have, it seems, some particularized suspicion.

Chairman ROBERTS. Mr. Dempsey, I'm going to have to interrupt at this point, and I do appreciate your point of view.

Could you clarify for the Committee which judge we're talking about in terms of the chambers?

Mr. DEMPSEY. I honestly don't know. It was in a letter that the FBI sent to Senator Stevens describing the use of the sneak and peek legislation.

Chairman ROBERTS. All right. We can find that.

Senator Bond.

Senator BOND. Thank you very much, Mr. Chairman. I thank the panel. I think we've had a very good discussion of what has been widely abused and misused and misrepresented, as we now hear people with differing points of view agreeing that there is justification for this. I happen to be a strong supporter of the PATRIOT Act. For better or for worse, I, with my colleague from Maine, Senator Snowe, authored the Visa Integrity and Security Act provisions which have caused a lot of heartburn. We understand that any law like this should be reviewed and we very much appreciate the thoughtful comments.

I go back to Mr. Dempsey and ask him briefly, you say on section 213 it was used to expand government powers with respect to delayed notice searches and that the section lacks suitable checks and balances. It was my understanding the PATRIOT Act merely codified pre-existing judicial precedent that allowed investigators to execute delayed notice criminal search warrants under certain limited circumstances.

To what extent was 213 an expansion of authority? Why aren't the current limits unreasonable? If you have to have approval of a judge, why isn't it appropriate to delay notice in certain circumstances?

Mr. DEMPSEY. Senator, a good question. Let me give you an example of how the provision failed in its stated goal of codifying existing practice.

Senator BOND. All right.

Mr. DEMPSEY. Two circuit courts had specifically ruled on the question of delayed notice. Each of them had come down in favor of a 7-day delay rule as the basic timeframe for which delay could be permitted, renewable for successive 7-day periods upon a good showing.

The PATRIOT Act, rather than codifying that case law, says the delay can be for any reasonable period. Well, what are the judges of the Ninth Circuit supposed to do now? They had come up with a 7-day rule. The Congress has not taken up the 7-day rule and adopted a reasonable period rule.

If you look at the Justice Department guidance, they say that up to 90 days would be a reasonable delay. That's an example of where we could have given specificity and clear standards and in fact failed to do so.

Senator BOND. Maybe Congress thought that the judges should determine in the particular circumstances what is reasonable and that if you are looking at a multi-faceted investigation, as some of the ones that we have heard about here, there's no way you're

going to get it finished in 7 days. I would think that the judge would have to be presented. They've said seven. Time's up. I want Ms. MacDonald to comment on that.

Mr. DEMPSEY. If I could, Senator, just 1 second.

Senator BOND. I want Ms. MacDonald to comment when Mr. Dempsey finishes his thought before we yellow light goes off.

Chairman ROBERTS. Mr. Dempsey, please proceed.

Mr. DEMPSEY. If we were going to leave it to the judges, we should have left it to the judges. We didn't need 213 at all. I think that the reason why the Justice Department pushed for 213 is because they had come to the conclusion that that legal authority that everybody cites was on shaky ground, because if you look at those cases, there are some older cases that said that the Fourth Amendment has nothing to do with notice or says nothing about notice. Then the Supreme Court later came along and said that notice is part of the Fourth Amendment determination.

Ms. MACDONALD. Subsequent to that case itself, there's been a Seventh Circuit case that said that you can delay notice for reasonable periods of time. To my mind, reading the case law, there is no question that delayed notice is fully constitutional.

I think it was wise of Congress to give judges and investigators the leeway to determine what a reasonable period of delay is. One of the problems that we had pre-PATRIOT Act was short time limits on warrants that were creating an enormous amount of paperwork.

You know, again, we're fighting terrorism here. We're not trying to prosecute——

Mr. DEMPSEY. Then let's limit this one to terrorism.

Ms. MACDONALD. OK. I want to respond as well to Mr. Dempsey's point about 215 when he asks, "Why have a judge?" Again, let's remember that these documents are available without a judge. A prosecutor can get them on his own request. Why 215 is more problematic is a mystery to me. The standard by which the FISA Court decides a 215 request under the PATRIOT Act is the same standard as under FISA. It required a factual showing before the PATRIOT Act and it still requires it now.

Chairman ROBERTS. Senator Wyden.

Senator WYDEN. Thank you, and thank all of you. We've got a good cross-section of views at this table.

This Act is going to be renewed. There's just no question about that. I would be interested in just going right down the row—and we can start with you, Mr. Dempsey—and have each of you say what you think the most important areas are with respect to what the Congress should require in the way of reporting. In other words, take two items each, the two most important areas to you in terms of what is most important for reporting so as to strike this balance between protecting the public good and individual liberties.

Mr. Dempsey.

Mr. DEMPSEY. Recognizing that reporting is one aspect of the sort of checks and balances we're talking about.

Senator WYDEN. Right. I think one of the most important ones.

Mr. DEMPSEY. I think reporting should apply to a couple of the sections that we haven't talked about yet, which are the emergency disclosure of e-mail section, which is section 212, again a relatively

uncontroversial provision in some ways. I've been hearing that there have been a lot of requests. Again, these are non-terrorism cases. These are by and large criminal matters, and there's absolutely no reporting now for those extrajudicial disclosures where the government goes to the service provider, says there's an emergency, the service provider, without a court order, turns over the e-mail. We really don't have any kind of a handle on how often that's happening.

In terms of FISA reporting, both on the electronic surveillance, physical surveillance and on 215, I think the issue there is to find a way to bring some of that more detailed information into the public light. I know this Committee receives the classified information. I would certainly urge you to look carefully at the applications, particularly the U.S. person ones. You may do that.

If you do do that, it would be useful to have a report about that. In the early years of FISA there was a 5-year report on its application which was an unclassified, public report. I think that would be helpful. I think that could be done without compromising any classified information and could talk about what this Committee is doing behind the scenes as an oversight matter.

I think there could be some more public reporting on FISA.

Mr. NOJEIM. To summarize, sections 215 and 505, the FISA records provisions, there ought to be reports under those provisions. In fact, AG Gonzales revealed for the first time just a couple weeks ago that section 215 had been used 35 times. A year before that Attorney General Ashcroft had said it had never been used. It seems to me that if they can disclose selectively the number of times it's been used that an annual reporting requirement probably wouldn't damage national security.

The section 215 reporting notion should be extended to section 505, National Security Letters, as well.

In addition, sections 203(b) and 203(d) about information-sharing, they could be beefed up with additional notice to the court and to Congress about how information is being shared, because right now there aren't sufficient requirements about that.

Then I'd like to follow up for just a second on what Senator Bond was saying earlier about sneak and peek warrants.

Senator WYDEN. My time is short and I want to get Ms. MacDonald in. If you could give us that a little bit later, that would be great.

Ms. MACDONALD. Thank you, Senator Wyden. I'll yield my time back to Mr. Nojeim because I don't feel qualified to answer that question. It's not something that I'd looked at on a section-by-section basis. My impression is, given the past reporting to the Judiciary Committee in the House, that the reporting requirements are very extensive.

I'm not aware, really, of any gaps in reporting requirements that exist.

Senator WYDEN. I may have time for one additional question. I was going to ask about National Security Letters, because I have been troubled by the fact that there really isn't any court review on it. What I'm most interested in to start with is, do any of you know how frequently they've been used? Because if this is not a frequently used tool, that makes it a matter of lesser importance.

Do any of you three know about how frequently they've been used?

Mr. DEMPSEY. Not currently. The staff knows; it's reported, I think, to the Committee.

Mr. NOJEIM. It ought to be something that's reported to the public, the frequency of the use of those.

Senator WYDEN. Are they widely used? Ms. MacDonald, do you know?

Mr. DEMPSEY. Oh, they are very widely used. It's a classic investigative technique.

Senator WYDEN. My time is up. I would only ask, if that's the case—and I was not aware of that, Mr. Chairman—I would like to work with both of you on that.

Chairman ROBERTS. Senator Wyden, we do have that information that you requested. We will share that with you.

Senator WYDEN. My understanding, then, is, Mr. Chairman, that there are very few rules with respect to National Security Letters and if it's a widely used tool I would like to work with both of you and see if we can flesh out a bipartisan change there that would strike the right balance between security and individual rights, because as far as I can tell there's no standard for it.

I thank you.

Ms. MACDONALD. Can I just make one response? The National Security Letter law was 1986 law, and it was Patrick Leahy that believed that they should be secret. Again, this is something we've had a very long time to look at whether it's a power that's been abused. Again, I'm not aware of abuses.

Senator WYDEN. Well, there are a variety of statutes that mandate National Security Letters. Other letters are permissive, Ms. MacDonald. That's why I think we're going to take a look at it.

Thank you, Mr. Chairman.

Chairman ROBERTS. Let the record show that we had a witness before the Committee who actually said that she didn't know about a question. I think that's remarkable.

I want to let my colleagues and everybody be aware of the fact—I know Mr. Dempsey mentioned records and what the Committee might do—this is not our first review of the PATRIOT Act or the Foreign Intelligence Surveillance Act. We regularly hold hearings and conduct briefings and receive information in regard to the activities of the intelligence community.

We conducted a closed hearing on the PATRIOT Act during the last Congress. We receive detailed reports from the Department of Justice every 6 months in regard to FISA, annual reports on the use of other surveillance tools. We're also in the final stages of completing our second audit of the procedures and practices and use of FISA. This comprehensive and classified analysis I think will represent one of the most thorough reviews of the Executive branch activities under FISA since the Act was enacted.

That was in my opening statement and I wanted to make sure that everybody here understood that we are aggressively active.

Senator Feinstein I think is next.

Senator FEINSTEIN. Thank you very much, Mr. Chairman.

As a member of both this Committee and the Judiciary Committee, in our hearings on the PATRIOT Act I have really been

hard-pressed to find any signs of bad use or overuse. I have pressed the Attorney General to provide a specific report. He has provided it. I've been though it. I have a hard time finding any instance of misuse of this Act.

I would like the two people—Mr. Dempsey and Mr. Nojeim—to take their best shot and give me what the misuse has been or bad use and how it should be repaired.

Mr. NOJEIM. We wrote a letter to you about this.

Senator FEINSTEIN. I got that letter, a 12-page letter, I think.

Mr. NOJEIM. Let me just run through some of the points that we made. First, the PATRIOT Act was used to search the home of Brandon Mayfield. He's the Portland, Oregon, attorney who was a suspect in a crime, and that was the Madrid train bombing. It turned out that he was completely innocent and the PATRIOT Act, the "significant purpose" test of the PATRIOT Act was used to get the intelligence warrant to search his home. I could go into that case in a little bit more detail.

Senator FEINSTEIN. Let me stop you there, because I moved the amendment in Judiciary for the "significant purpose." If you were to change it, how would you change it? Because I agree with Ms. MacDonald. I think in this world that we live in, the breaking down of that wall from "primary purpose" to "significant purpose" was really important to do.

Mr. NOJEIM. As we wrote in the letter to you, we're not asking that you support repeal of the "significant purpose" test. We're asking that you increase reporting. We're asking that you——

Senator FEINSTEIN. You mean periodic reporting?

Mr. NOJEIM. Reporting, for example, of how many U.S. persons are searched under FISA. Brandon Mayfield is a native-born American.

Senator FEINSTEIN. I understand that.

Mr. NOJEIM. That's what we're asking for.

Another thing that we're asking is that you put the Brandon Mayfields of the world—and there will be more of them—in a better position if the government doesn't come forward with the evidence showing that it wrongly accused them. Brandon Mayfield could have gone to trial accused of one of the worst crimes in history without getting access to the information that was used to search his home.

What we're suggesting is that the Classified Information Procedures Act provides a good model that the Committee could adopt for giving a person like that, who is accused of a terrible crime, if it actually goes to trial, access to that information.

Another thing that we mentioned, in our letter to you, as an abuse was the use of an unconstitutional statute. The National Security Letter statute has been struck down by a Federal district court. The statute was broadened substantially, rewritten by the PATRIOT Act, and one can't say that repeated use of an unconstitutional power is not a problem. It is a problem.

We suggested a number of changes to the National Security Letter statute that we think would satisfy that court. For example, making it so that a person who gets one of those National Security Letters can talk to a lawyer, making it so that the gag that pre-

vents them from saying they ever got a letter is time-limited, and putting in a meaningful standard of review for that letter.

The other cases that we mentioned in our letter to you include the exclusion of a Muslim scholar under section 411 of the PATRIOT Act that appears to be based on the person's political opinion; in another one, the prosecution of a gentleman, Sammy L. Hussein, for, among other things, posting material to the Internet that he didn't even write. He posted things to the Internet that were links to what other people wrote. He was charged for providing material support for terrorism for doing that and for some other things.

These are problems. We're suggesting that this Committee can deal with those.

Senator FEINSTEIN. Mr. Dempsey, quickly.

Mr. DEMPSEY. I think the cases cited by Mr. Nojeim are real cases of abuse. I had cited in my dialog with Senator Lott others that I thought were not what Congress had intended, although they are within the four corners of the legislation—use of PATRIOT Act authority for nonviolent crimes having nothing to do with terrorism.

I also think, looking at the Justice Department report on the PATRIOT Act sunsets, there's no evidence of abuse; also, for many of the provisions there's no evidence of use, not that they aren't used, but there's nothing one way or the other in this report saying good or bad about how those cases have been used.

I'm not sure that the standards, particularly for intelligence authorities, should be documented abuses. I think we can now take the time, look at the authority, ask does the authority meaningfully advance the national security. I think in almost every case, if not every case, there is an argument that it does. Then ask ourselves what should be the circumstances surrounding that.

Clearly Congress thought it was retaining some limits. Witnesses today have emphasized the role of the judiciary, for example. The fact that the government needs information doesn't mean that all the rules are off. We now have the time to go back. We've made what I think are significant proposals, relatively modest, but they would help focus the FBI and other intelligence agencies.

Ms. MACDONALD. Can I quickly respond?

Senator FEINSTEIN. My time is up, but could Ms. MacDonald comment?

Chairman ROBERTS. Well, I certainly would like to recognize Ms. MacDonald for her quick-draw best shot.

Ms. MACDONALD. OK. Thank you.

I think we've had a case of bait and switch here. I'm really perplexed by the Brandon Mayfield example. What we were hearing, the doom and gloom scenarios about getting rid of the "primary purpose" test was that you would have a sneaky prosecutor who wants to get some guy for drugs and he uses FISA because it's a lower standard of review.

Brandon Mayfield was being investigated for terrorism. I don't see how that is a misuse of the PATRIOT Act. The problem was the fingerprinting was inaccurate. That was not a PATRIOT Act abuse. The system worked. He was exonerated. He was not prosecuted. I'm very perplexed by the Mayfield example.

If that's all they've got, it's not much. The National Security Letter statute that Mr. Nojeim says was stuck down as unconstitutional, that's true, but they did not strike down the PATRIOT Act provision. They struck down the 1986 Electronic Communications Privacy Act and Senator Leahy's idea that there should be a gag order. Let's not way that the PATRIOT Act has been struck down as unconstitutional.

The exclusion of a Muslim scholar because of his political opinion, I'd need to know the facts about that. Obviously if somebody is preaching jihad, in the worst case scenario, I do not think that we want to admit. There's no constitutional right of a foreigner to be admitted to this country. He has no First Amendment rights. Without knowing more about the case, that would be my initial reaction.

Chairman ROBERTS. Senator Corzine.

Senator CORZINE. Thank you, Mr. Chairman, and I appreciate the hearing.

I'd like to actually continue on this. I come at this by citing a quote in the 9/11 Commission.

> "The burden of proof for retaining a particular governmental power should be on the Executive to explain that the power actually materially enhances security and that there's adequate supervision of the Executive's use of the power to ensure protection of civil liberties."

It goes on.

I embrace that concept, and I think this discussion of abuses actually is one of those elements that maybe some of this needs to be done privately where you delve into it. The idea of a judge's quarters being interdicted into without any kind of authorization——

Mr. DEMPSEY. There was a court order, just to be clear, Senator. There was a court order, but it was a secret search.

Senator CORZINE [continuing]. Strikes me as somewhat overreaching. I'd like to hear the response to Ms. MacDonald's comments about the Mayfield situation, which, if you were Mr. Mayfield, an American citizen, you'd wonder why you were being subjected outside of extraordinary causes, why you were being subject to an investigation without the kinds of checks and balances that American citizens believe that they have under the Constitution.

Mr. NOJEIM. A couple points in response to Ms. MacDonald.

First, in the Mayfield case, the government never had to show probable cause of crime in order to break into his home. It's just a different standard. It's a lower standard. They used the PATRIOT Act to break into his home. They didn't give notice. They wouldn't have to give notice—I'm sorry. Pre-PATRIOT Act, they would have had to give notice. They would have had to, when they broke in and downloaded the computer hard drives, took 355 digital photographs, took 10 samples of DNA, they'd have to leave a notice saying this is what we took from your apartment.

You know what Mayfield's most concerned about now? All this information that was gathered has now been shared. It's been shared under the information-sharing provisions of the PATRIOT Act. There's not a Rule 41 A-type procedure for Mayfield to get it

all back, to get back what was downloaded from his computer. That's one of his concerns.

The other point that Ms. MacDonald made was about the National Security Letter statute. This I need to illustrate. The PATRIOT Act rewrote the National Security Letter statute.

This is 18 USC section 2709, before the PATRIOT Act.

This is what the PATRIOT Act did to the National Security Letter statute. The parts that are in yellow were added by the PATRIOT Act. The parts that are crossed out were deleted by the PATRIOT Act.

Chairman ROBERTS. If you can, Mr. Nojeim, speak up. I apologize that we don't have a rolling mike.

Mr. NOJEIM. This is what the Court did to 18 USC section 2709. It struck the parts that were added by the PATRIOT Act and it struck the parts that were in the statute before the PATRIOT Act amended it that were not deleted by the PATRIOT Act. It struck every single sentence, every phrase, every comma of section 505(a) of the PATRIOT Act. It is simply not accurate to say that it didn't strike a section of the PATRIOT Act.

[The chart referred to follows:]

Section 2709 Before the Patriot Act

18 U.S.C. § 2709 Counterintelligence access to telephone toll and transactional records

(a) Duty to provide.--A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) Required certification.--The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director, may--

(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee in a position not lower than Deputy Assistant Director) certifies in writing to the wire or electronic communication service provider to which the request is made that--

(A) the name, address, length of service, and toll billing records sought are relevant to an authorized foreign counterintelligence investigation; and

(B) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801); and

(2) request the name, address, and length of service of a person or entity if the Director (or his designee in a position not lower than Deputy Assistant Director) certifies in writing to the wire or electronic communication service provider to which the request is made that--

(A) the information sought is relevant to an authorized foreign counterintelligence investigation; and

(B) there are specific and articulable facts giving reason to believe that communication facilities registered in the name of the person or entity have been used, through the services of such provider, in communication with--

(i) an individual who is engaging or has engaged in international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States; or

(ii) a foreign power or an agent of a foreign power under circumstances giving reason to believe that the communication concerned international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States. (footnote omitted)

(c) Prohibition of certain disclosure.--No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(d) Dissemination by bureau.--The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) Requirement that certain congressional bodies be informed.--On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

Section 2709 As Amended By the Patriot Act

18 U.S.C. § 2709 -- Counterintelligence access to telephone toll and transactional records

(a) Duty to provide.--A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) Required certification.--The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, may--

(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee ~~in a position not lower than Deputy Assistant Director~~) certifies in writing to the wire or electronic communication service provider to which the request is made that -

~~(A)~~ the name, address, length of service, and toll billing records sought are relevant to an authorized ~~foreign counterintelligence~~ investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; and

~~(B) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801)~~

(2) request the name, address, and length of service of a person or entity if the Director (or his designee ~~in a position not lower than Deputy Assistant Director~~) certifies in writing to the wire or electronic communication service provider to which the request is made that--

~~(A)~~ the information sought is relevant to an authorized ~~foreign counterintelligence~~ investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States;

~~(B) there are specific and articulable facts giving reason to believe that communication facilities registered in the name of the person or entity have been used, through the services of such provider, in communication with--~~

~~(i) an individual who is engaging or has engaged in international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States; or~~

~~(ii) a foreign power or an agent of a foreign power under circumstances giving reason to believe that the communication concerned international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States.~~

(c) Prohibition of certain disclosure.--No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(d) Dissemination by bureau.--The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) Requirement that certain congressional bodies be informed.--On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

Section 2709 After Doe v. Ashcroft

709 -- Counterintelligence access
l and transactional records

(a) wire or electronic communication service
provida request for subscriber information and tail
billing reco tronic communication transactional
records in its c made by the Director of the Federal
Bureau of Investig (b) of this section.

(b) Required certificat Federal Bureau of
Investigation, or his designee than Deputy
Assistant Director of Bureau head Agent in Charge
in a Bureau field office designated b

(1) request the name, address, le al and
long distance tol billing records of a p irector
(or his designee ~~in a position not lower tha~~
~~Director~~) certifies in writing to the wire or elec
service provider to which the request is made tha

~~(A)~~ the name, address, length of service, and to
records sought are relevant to an authorized ~~foreign~~
~~counterintelligence~~ investigation to protect against
international terrorism or clandestine intelligence acti
provided that such an investigation of a United Sta
not conducted solely on the basis of activities
first amendment to the Constitution of the U
~~(B) there are specific and articulable fa~~
~~to believe that the person or entity~~ tion
~~sought pertains is a foreign pow~~ oreign
~~power as defined in section~~ elligence
~~Surveillance Act of 1978~~

(2) request the name of service of a person
or entity if the Dir ~~n a position not lower~~
~~than Deputy~~ ies in writing to the wire or
electronic e provider to which the request is
made

ought is relevant to an authorized
~~elligence~~ investigation to protect against
terrorism or clandestine intelligence activities
that such an investigation of a United States person
conducted solely on the basis of activities protected by
the first amendment to the Constitution of the Uni
~~(B) there are specific and articulable facts gi~~
~~to believe that communication facilities re~~
~~name of the person or entity have bee~~
~~services of such provider, in comm~~

~~(i) an individual who is engag~~ ~~(c) of the~~
~~international terrorism as~~
~~Foreign Intelligence S~~ ~~ndestine~~
~~intelligence activi~~ ~~y involve a~~
~~violation of the~~ ~~the United States; or~~
~~(ii) a foreig~~ ~~of a foreign power~~
~~under~~ ~~reason to believe that the~~
~~ce~~ ~~ned international terrorism as~~
~~(c) of the Foreign Intelligence~~
~~or clandestine intelligence activities that~~
~~y involve a violation of the criminal statutes of~~
~~d States.~~

n of certain disclosure.--No wire or electronic
ation service provider, or officer, employee, or agent thereof,
lose to any person that the Federal Bureau of Investigation
or obtained access to information or records under this

bureau.--The Federal Bureau of Investigation
n and records obtained under this section
approved by the Attorney General for
foreign intelli foreign counterintelligence
investigations co al Bureau of Investigation, and,
with respect to dissem y of the United States, only if
such information is clear horized responsibilities of
such agency.

(e) Requirement that certain con informed.--On a
semiannual basis the Director of the Fe igation
shall fully inform the Permanent Select Com e of the
House of Representatives and the Select Com of
the Senate, and the Committee on the Judiciary
Representatives and the Committee on the Judiciary
concerning all requests made under subsection (b) of this

Mr. NOJEIM. In his opinion striking this National Security Letter statute, Judge Morero repeatedly, repeatedly referred to amendments made by section 505(a) of the PATRIOT Act. He noted as examples of abuses conduct that could not have been conducted prior to the PATRIOT Act changes. In particular with respect to the gag in section 505(a), he said that the requirement of the tie to an agent of a foreign power limits the potential for abuse and cited that as one of the reasons he was striking down this statute.

Ms. MACDONALD. I read that opinion very differently. The ACLU was challenging the 1986 law on the fact that there was a gag order in the National Security Letter 1986 law that was put there by Patrick Leahy. The PATRIOT Act changed the 1986 law to this extent: it removed the agent of a foreign power requirement. That is not the issue that was before the Court.

The issue before the Court was the constitutionality of the gag order which was in 1986. Yes, it struck down the entire section because the PATRIOT Act merely amended that section. The PATRIOT Act changes were not what was at stake. It really is more accurate to say it struck down the 1986 law.

On the Mayfield case, again they were breaking into his house because he was under investigation for terrorism, not for a garden variety crime. Pre-PATRIOT Act they would have had to have given notice. Do we want to be giving notice to suspects in terrorism cases? I don't think so. Now, are there going to be cases in the future, perhaps, where other American citizens are suspected of terrorism. Could be. I wish we knew that no American is ever going to be tempted to join into a terrorist plot.

We don't have a rule to that effect. I think that the power to investigate terror suspects is properly limited by the PATRIOT Act. That was a terrorism investigation, not a criminal investigation.

Chairman ROBERTS. Senator Rockefeller.

Vice Chairman ROCKEFELLER. Thank you, Mr. Chairman. I just have one question. Over the months, years of its history, it seems to me to have always been the core question. That is, I'm not sure which one said it, but one of you said that the FISA judges are nothing more than a rubber stamp.

I think that there are those who oppose the PATRIOT Act or want to see it changed because they accept that. I'm not a lawyer and I would wish to hear each of you say why you think or what you think about that statement.

Mr. DEMPSEY. Senator, that was my statement, so if I could first—let me make it clear. I don't think that the FISA judges are rubber stamps in reviewing the content interception orders or the physical search orders, and they have proven that because they have clearly pushed back against the FBI and against the Office of Intelligence Policy Review, which presents the orders to them. Absolutely, I don't think that they are rubber stamps.

I think under 215 they don't want to be rubber stamps, but as I read the statute it sort of makes them function as rubber stamps. It basically says, there will be no facts in front of you and you cannot ask for facts or asking for facts is outside the scope of the statute. I think that court is an important institution. I think they may ultimately, as we go forward, be given additional responsibilities.

I don't want them to be rubber stamps. The PATRIOT Act, at least 215, as adopted, and probably the pen register changes, if adopted, do pretty much make them into that.

Vice Chairman ROCKEFELLER. How would you respond to that, Ms. MacDonald?

Ms. MACDONALD. That was actually my statement. I said that in my impression I hear critics accusing the FISA court of being a rubber stamp because it's in secret. I think that is an insult to Article III judges who rotate in and out of that court. I have to assume that they are taking their responsibilities extraordinarily seriously.

Let's not forget that FISA, the original law, was already a radical civil libertarian idea that a judge should be involved in foreign intelligence investigations in the first place. The whole wisdom of constitutional assumptions up to that point was that anything involving foreign espionage, foreign terrorism, was within the Executive branch's discretion, because judges don't have the knowledge to pass on such matters. The very fact that we have a court at all basically issuing warrants for foreign intelligence investigations I think is already a significant check on executive power.

The idea that anything should be public about that court to me is preposterous.

Vice Chairman ROCKEFELLER. That I'm not questioning.

Mr. Dempsey said that they have no facts before them. When you say that to the average American they say, "Well, they must just be operating automatically or on automatic pilot."

Ms. MACDONALD. They have the record that is presented to take a request before the FISA court.

Vice Chairman ROCKEFELLER. The facts that they do have reflect on the decision that they will proceed to make.

Ms. MACDONALD. That the records are relevant to a terrorism investigation.

Vice Chairman ROCKEFELLER. And, Mr. Dempsey, you would say?

Mr. DEMPSEY. Well, I guess I have to say, Mr. Chairman, at some level I don't know, since I haven't seen a 215 or post-PATRIOT pen register application to the FISA court. As I read the statute, it says nothing about the factual determination. If there is one and if there is a factual showing—and, by the way, internally the FBI does prepare, internally, a factual basis for both the National Security Letters and 215, and I assume for the pen registers—if they do, I think that should be part of the statute.

If they don't, then I think they are operating on autopilot, and that's where it would be good if this Committee could say something publicly about what it has seen, that 215 and pen register applications do or do not have a factual predicate to them, and it is or is not something that would show relevance in the particularity of that request.

National Security Letters, of course, never are presented to a judge. I think they should be. I think everything should be rolled into 215.

Ms. MACDONALD. if you have a judge, it's not enough, and if you don't have a judge, then it's not enough. The identical language was what was governing the FBI before 9/11 when this Committee

raised the alarm that the FISA process was taking months and that the OIPR was putting probable cause standards that were completely unjustified by the statute.

The practice is clearly to develop a substantial record to take to the court.

Vice Chairman ROCKEFELLER. You think that the necessity of getting—as you pointed out, I think very effectively, this is about terrorism and our Nation's security—that there is a certain rush to get decisions made for purposes of looking or not looking or whatever, and that some then would interpret that as, in and of itself, being avoiding their particular practices, which would not apply to a national security type situation, an ordinary law situation. Shakespeare could have said that better.

Ms. MACDONALD. Again let's just remember that your peers can get those records. A grand jury can subpoena those records with no judge involved at all. The PATRIOT Act gives you a judge. FISA gives you a judge. Those records are not protected by the Fourth Amendment. You do not need a probable cause warrant to get them. A prosecutor can say give me those records right now.

Vice Chairman ROCKEFELLER. Would you disagree with that, Mr. Nojeim?

Mr. NOJEIM. I would say that she's gone a little too far in saying that the records are completely unprotected by the Fourth Amendment because they're in the hands of a third party. For example, when I send an e-mail to you, that e-mail is in the hands of an Internet service provider. The content of that e-mail, I believe, is protected by the Fourth Amendment. So this notion that everything that's in the hands of a third party is unprotected I don't know that I would go that far.

Ms. MACDONALD. The PATRIOT Act does not make the content of that e-mail available. That is protected First Amendment information. Third party records——

Mr. NOJEIM. Actually, if I could just follow up on that, what happened in the PATRIOT Act was the pen register and trap and trace language that used to apply only to telephone records and was interpreted to apply to Internet records was explicitly applied to Internet records. It wasn't clarified that that language doesn't include, for example, content type information that might be in a person's search request when they make a search request under Google, for example.

One of the things that we're suggesting that this Committee or Congress do is to clarify that that kind of information, which is content, would not be available under pen registers and trap and trace devices.

Ms. MACDONALD. That's fine. This is minutiae. The fact is, *U.S.* v. *Miller*, a Supreme Court case of 1976, said no Fourth Amendment privacy interest in records in third party hands. That's why a prosecutor can subpoena them.

Vice Chairman ROCKEFELLER. This has been enlightening and helpful. I thank you all.

Chairman ROBERTS. Senator Corzine.

Senator CORZINE. I really just need to ask for the facts in the Mayfield case. Can someone give me the chronology about what authorizations occurred, didn't occur, and how soon the individual

was made aware? What was the flow. I apologize if I didn't get through all my briefings, but actually looking at some of these individual cases——

Chairman ROBERTS. Senator, could I make a suggestion, that we go into that in a closed session, as to chronological order that you requested? I want the witnesses to respond, if in fact you have something to say, but let me just say that I think you should raise that question again during the closed session so we can get a better answer.

I would only say that at the time, I think it was Ms. MacDonald, indicated that it was a fingerprint mistake. We thought this gentlemen had the same fingerprint as was located on a bomb in Madrid. As you remember, we were going through quite a time here in regard to a consensus threat analysis that, as it turned out—I'll just stop right there.

We did a lot in terms of security measures and everybody was very intense at that particular time, very concerned. As it turned out, that was not the case in regard to the level that perhaps was acted upon. I probably ought to quit talking about it.

At any rate, it was at that particular time. We had officers around here, as you well remember, with gas masks and automatic weapons and security moved away, and parents of my staffers calling. One Senator just left. It was all based on the Madrid syndrome. You had a situation where you had a fingerprint mistake.

I don't think that that's an abuse of the PATRIOT Act. That was a mistake by the FBI and the fingerprint. Now that didn't answer your question, and I apologize. At least I wanted to bring that up.

If you would like to pursue that.

Senator CORZINE. I respect the idea that we ought to parse this, if we were to parse this, in private. What is in the public domain, if someone had a comment on it.

I have a simple question. Was there a FISA request.

Mr. NOJEIM. Yes. There was a FISA request. The simple two-sentence explanation is, Mayfield enlisted in the Army and submitted a fingerprint. It was that fingerprint that was mistakenly matched with a fingerprint on some detonators of undetonated bombs that were found in Madrid. The government used that match to detain Mayfield on a material witness warrant, but prior to that it had secretly broken into his home, apparently a number of times, and also conducted electronic surveillance using the Foreign Intelligence Surveillance Act, as amended by the PATRIOT Act.

Mr. DEMPSEY. Mr. Chairman.

Chairman ROBERTS. Yes, Mr. Dempsey.

Mr. DEMPSEY. Could I just make one brief comment, not on the Mayfield question but going back to the discussion of abuse and sort of what's the burden of proof, so to speak, on the PATRIOT Act. In November 2001 the National Security Law unit at the FBI sent a field memo out to agents explaining the National Security Letter provisions, pointing out that the National Security Letters are powerful investigative tools. However, they just be used judiciously. It said that the USA PATRIOT Act greatly broadened the FBI's authority to gather this information; however, the provisions in the Act relating to the NSLs are subject to a sunset provision that calls for the expiration of those provisions in 4 years. In decid-

ing whether or not to reauthorize the broadened authority, Congress certainly will examine the manner in which the FBI exercised it.

Now in that sense I think that the sunsets worked. The sunsets have required the government to be careful. There may be abuses, either in the Mayfield case or in some of the cases I cited, abuses may yet come to light, but because of the sunsets we did have this exercise of caution implicitly recommended by FBI headquarters.

I think we need to either have another sunset or we need to find some checks and balances that will serve the same purpose and ensure that these are exercised carefully. Because if the sunsets go away, then I'm not sure what there is left.

Chairman ROBERTS. Senator Chambliss. You are like Shane; you come back.

Senator CHAMBLISS. When you page me, Mr. Chairman, I come. I apologize for having to come and go, but this is too interesting a subject and too important a subject to not come back and dialog on a couple of issues.

First of all, Mr. Dempsey, in your opening comments you talked about sneak and peek and the use of it relative to a couple of instances that you pointed out, one going into a judge's chamber to look for whatever I guess the FBI in that case was looking for and, second, in the office of a health care provider. In both those cases they used the PATRIOT Act.

How could you use the PATRIOT Act in a non-terrorist situation in the two examples that you gave?

Mr. DEMPSEY. Isn't that a fascinating question? That would perplex most people, Senator. The fact is that there are provisions in the PATRIOT Act that have nothing to do with terrorism. Sneak and peek is No. 1. Remember, for terrorism investigations the FBI has sneak and peek authority under FISA. If sneak and peek authority were needed for criminal investigations of terrorism, some Senators, including Senator Leahy, said, "Well, OK, let's have a sneak and peek for terrorism cases."

"Uh-uh", said the Justice Department. We want it for all cases. We want it for student loan cases. We want it for Medicare fraud cases. We want it for judicial corruption cases. We want it for check-kiting cases. That's what was enacted and that's how it's being used. I think most people would be astonished to realize that the PATRIOT Act is being used for sneak and peek searches in non-terrorism, non-violent cases.

Senator CHAMBLISS. Is there a specific authorization for sneak and peek to be used in non-terrorist cases within the PATRIOT Act?

Mr. DEMPSEY. Well, the section was generic in nature. It was a generic exception to the rule which generally requires notice in the execution of warrants. It was sort of shoehorned in there. It's a little bit of an odd provision.

Senator CHAMBLISS. Of course, sneak and peeks have been used, particularly in organized crime cases, drug cases, I know for years. Are you telling me that this was something different, that there was some additional authority given in the PATRIOT Act that allowed them to use this versus the previous sneak and peek authority?

Mr. DEMPSEY. My own view is that the Justice Department was trying to bootstrap the existing authority, which I think was a little bit shaky, it couldn't be pushed too far, it had to be used with care, in my view it had to be confined to cases where there was risk of destruction of the evidence or risk of intimidation of witnesses or flight from prosecution or risk of loss of life or some violent act.

What happened in the PATRIOT Act was that basically the Justice Department invoked the authority of the Congress to bolster that authority, expand the kind of cases in which it could be used, and in essence give a green light to the judges, backed up by Congress. Judges have allowed sneak and peeks in criminal cases before the PATRIOT Act.

I think the Justice Department was a little worried about what ground that stood upon. Some Supreme Court cases had said that notice is more important than we had thought when the original sneak and peek cases were decided, and I think the Justice Department was trying to get Congress to sort of bolster that authority and expand it in the sense of putting it on what seemed to be a firmer foundation, although, of course, it's the Constitution that's the final test.

I think that there was an effort by the Justice Department to take some somewhat uncertain, often used but still uncertain and cautiously exercised, judicial common law authority and bolster that with this emergency legislation. I think they shouldn't have done it for cases, non-terrorism-related. I think that is somewhat surprising, that it turned out that way.

I think that now the judges, if anything, are probably more confused about what are the standards for sneak and peek searches. It looks a little bit like the constraints are off.

Senator CHAMBLISS. Ms. MacDonald, according to your opening comments, I don't think you agree with that. Am I right?

Ms. MACDONALD. That's a good supposition. The theory that somehow the authority to delay notice of a search was in any constitutional jeopardy before the PATRIOT Act I disagree with 100 percent. The cases had upheld sneak and peek authority. In fact, I don't see how you can conduct any kind of pre-emptive investigation, be it criminal or terrorism, with notice. You can't.

If sneak and peek hadn't existed, somebody would have had to invent it, because if you are trying to limn out the extent of a criminal conspiracy, you need secrecy up until the point when you have evidence. You need secrecy. Remember, the other point about this authority, which pre-existed the PATRIOT Act and which the PATRIOT Act merely codified, is that notice is only delayed.

There is no authority to withhold notice for eternity. All that the PATRIOT Act did was change, in one case, a 7-day rule of thumb to the phrase "reasonable period of delay." Courts all the time operate under that type of language, and we don't have a problem with it. It is in fact, in case law, quite rare to have specific numerical barriers on anything. This is why we have the common law system, because courts like to look at facts and use their own judgment.

As far as getting rid of the limits that Mr. Dempsey said, that's not true. The PATRIOT Act points to the exact set of circumstances that he just enumerated—witness intimidation, destruction of evidence, jeopardizing a trial or unduly delaying a trial, putting some-

body's life in jeopardy. Those existed pre-PATRIOT Act, they exist post-PATRIOT Act.

I don't think the Justice Department was in any fear of the power being taken away from them. I think what they wanted was a uniform national standard for complex criminal or terror investigations so they didn't have to worry about what the Second Circuit's specific details were versus the Ninth Circuit's. Because we have national investigations, be they criminal or terror.

Mr. DEMPSEY. Then let's write those standards. What the Congress did in the PATRIOT Act was to refer to a list of circumstances not drawn up for sneak and peek searches, not drafted for the PATRIOT Act but drafted a number of years ago in a law having to do with delayed notice of access to stored e-mail. The PATRIOT Act simply references those circumstances by referral—the risk of loss of life, absolutely, intimidation of witnesses, destruction of evidence, flight from prosecution. They also include otherwise unduly jeopardizing an investigation or delaying a trial.

It turns out that the Attorney General report just last week that the majority of the sneak and peeks that have been approved under the PATRIOT Act in non-terrorism cases since it was adopted have been in that catch-all category of unduly delaying a trial or otherwise jeopardizing an investigation.

If we want to give standards, if we want to give uniformity, if we want to give guidance to the courts, let's give them guidance. Let's think about what are the circumstances in which this technique is appropriate and write them and not reference some other circumstances developed for another purpose.

I think it would be useful to actually look back at the cases. I'm not sure that any case has ever said that a delay in a trial is a reason to break secretly into somebody's house. I don't think there is a case on that.

Chairman ROBERTS. I want to thank all the witnesses for a very challenging and intellectually stimulating hearing and for your advice and counsel as we go through the reauthorization of the Act. You have been most helpful and been patient and you have persevered, and we thank you very much for your attendance.

The hearing is concluded.

[Whereupon, at 4:44 p.m., the hearing adjourned.]

THE HISTORY AND APPLICATION OF THE USA PATRIOT ACT AND THE IMPORTANCE OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 (FISA)

DAY TWO

WEDNESDAY, APRIL 27, 2005

UNITED STATES SENATE,
SENATE SELECT COMMITTEE ON INTELLIGENCE,
Washington, DC.

The Committee met, pursuant to notice, at 9:37 a.m., in room SH–216, Hart Senate Office Building, Hon. Pat Roberts (Chairman of the Committee) presiding.

Committee Members Present: Senators Roberts, DeWine, Snowe, Rockefeller, Levin, Wyden and Mikulski.

OPENING STATEMENT OF HON. PAT ROBERTS, CHAIRMAN

Chairman ROBERTS. The Committee will come to order.

The Senate Select Committee on Intelligence today continues its ongoing oversight of the USA PATRIOT Act. This is the third in a series of three hearings designed to educate Members and the public as the Senate considers the repeal of the sunset provision, and modification to other intelligence authorities.

Last week, the Committee heard from a panel of outside experts with regard to the authorities contained in the PATRIOT Act. Later in the week, the Committee held a very informative closed hearing on the use by the intelligence community field operatives of the tools provided by the PATRIOT Act, and today it is my opinion that I have heard nothing to substantiate the allegations that abuses of the tools that are provided by the USA PATRIOT Act have led to violations of the civil rights of American citizens. I have, however, heard testimony and received other information that clearly demonstrates how the PATRIOT Act has been instrumental in helping our intelligence community agencies, in particular the FBI, identify and interdict terrorists and other national security threats.

The purpose of today's hearing is to receive testimony concerning the Administration's position on the authorities provided in the PATRIOT Act, including those provisions subject to sunset. We have a distinguished panel—the Honorable Alberto Gonzales, Attorney General of the United States; the Honorable Robert Mueller, the Director of the Federal Bureau of Investigation; and the Honorable Porter Goss, the Director of the Central Intelligence Agency. The

Committee thanks all of our witnesses for being here today, and for taking time out of your very valuable schedule.

This series of hearings is not the Committee's first review of the USA PATRIOT Act or the Foreign Intelligence Surveillance Act, also known as FISA. The Committee regularly holds hearings and conducts briefings and receives information in regard to activities of the intelligence community. The Committee conducted a closed hearing on the PATRIOT Act during the last Congress. We receive detailed reports from the Department of Justice every 6 months in regard to FISA collection, and annual reports on the use of other surveillance tools.

The Committee is also in the final stages of completing its second audit of the procedures and practices in the use of FISA. This comprehensive classified analysis will represent one of the most thorough reviews of the executive branch activities under FISA since the USA PATRIOT Act was enacted.

Now, before I recognize the Vice Chairman, I want to reiterate some fundamental principles that will inform our consideration of the USA PATRIOT Act reauthorization and any other modifications to law or policy governing intelligence activities. First, our intelligence agencies need flexible authorities to confront terrorists, spies, and proliferators and other national security threats.

Second, as we seek to protect the national security, we must also ensure that civil liberties and privacy are not sacrificed in the process. This is not a zero sum game, however. As former Supreme Court Justice Arthur Goldberg noted, while the Constitution does protect against invasions of individual rights, it is not a suicide pact.

Third, these are not matters of first impression. During their interpretation of the Constitution and the President's responsibility to protect national security, Federal courts have wrestled with many of these issues before. And the courts have recognized the authority of the President to conduct warrantless electronic surveillance of foreign powers and their agents. Well established judicial precedents also make clear that certain records, even of the most private information, lose their constitutional protection when voluntarily exposed publicly or to a business or to a third party.

Finally, I will support reasonable modifications to the USA PATRIOT Act provisions or other authorities that clarify legal uncertainties, but I will oppose modifications that place unnecessary hurdles in the path of lawful intelligence investigations.

Now, the Senate's consideration of modifications to section 215 of the US PATRIOT Act will serve as a good example of how I intend to apply these fundamental principles. I had previously expressed my support for the modifications made to FISA by section 215. The "business records" that our investigators now have access to, following a review by a Federal judge, are very important pieces of the intelligence puzzle. They form the basis for further investigation of national security threats.

Despite all of the talk that has been directed at section 215, and obvious concern, I have heard of no substantial allegation of abuse or misuse. There may have been some mistakes, but it certainly didn't have anything to do with the PATRIOT Act. In fact, I believe the FBI's use of the authority may have been a little bit too judi-

cious. While I recognize that some clarifying modifications to section 215 may be necessary, I will oppose any modification that increased the standard for a business record order above "relevance" or alterations that place unreasonable barriers between these records and the intelligence officials.

Those provisions of the USA PATRIOT Act, including section 215, that will expire at the end of the year must be reauthorized. The alternative is a return to a failed, outdated, and illogical limit on national security investigations that tied our hands prior to the 9/11 attacks. The dangers are real, and we should give our people every constitutional tool available to fight and defeat terrorism.

I now recognize the distinguished Vice Chairman for any remarks he might wish to make.

OPENING STATEMENT OF HON. JOHN D. ROCKEFELLER IV

Vice Chairman ROCKEFELLER. Thank you, Mr. Chairman.

I greet all three of you distinguished leaders of your agencies and express embarrassment that there are only four Members of our Committee here. If there are any that choose to listen to this on in-Senate television, we would welcome their coming in and participating in this Committee meeting. This is not an impressive display of government oversight.

I do welcome you. Our principle focus has been on one title of the PATRIOT Act, which is Title II on enhanced surveillance procedures. That has, as we discussed before, 16 provisions that will cease to have effect or sunset on December 31st of this year. In addition, the recently enacted Intelligence Reform Act authorizes the use of the FISA, the Foreign Intelligence Surveillance Act, in the case of so-called lone wolf terrorists. That new authority is also subject to sunset at the end of this year.

So these hearings and related hearing before the Senate Judiciary Committee and in the House also will help Congress to resolve two basic questions. First, on the basis of experience and further reflection since September 11, 2001, should any of the expiring authorities be amended? And second, as originally enacted or as amended, should the expiring provisions be made, in fact, permanent?

From last week's hearings it appears that there is broad support for the proposition. Even a critic of parts of the PATRIOT Act conceded that, "we see not a single power in the Act that needs to sunset or go away entirely." Rather, the issue is whether several sections of the Act should be amended to provide additional checks and balances. It's my hope that we can now begin to focus on the suggestions for improving several of the provisions that are now scheduled to expire at the end of this year.

In the Senate there is a bipartisan bill, S. 737, the Security and Freedom Enhancement Act, or SAFE Act, introduced by Senator Craig. Senator Corzine of our Committee is one of the 10 bipartisan cosponsors of this Act. The SAFE Act would make permanent most of the PATRIOT Act's investigative tools without change and amend several other PATRIOT Act tools to provide additional safeguards. I have reached no conclusions myself about the particulars of the SAFE Act, or I choose not to at this point, which has been

referred to the Judiciary Committee and also will be studied by our colleagues very carefully in that body.

I do believe on the basis of the breadth of its sponsorship and the supporting testimony that we have heard that the legislation merits our serious consideration. I look forward to hearing from our witnesses today about the proposals in the SAFE Act, including any objections or alternative suggestions that you may have for ensuring both sufficient focus on suspected terrorists and sufficient judicial and congressional oversight.

We need effective investigative tools against terrorism. Nobody can argue that. We need to be mindful of our Constitution and our values. And we need to build a broad public consensus that sustains our efforts against a war on terrorism which I think will last for decades, in those years to come. This will require intensive effort by the executive and legislative branches, to give the American public additional confidence that powerful investigative tools will be used effectively and that they will be used judiciously. I think this can be done, but the American public is not easily sold on such matters. On the other hand, fighting a war on terrorism has its own requirements by themselves.

Today's witnesses head the three organizations that are responsible, along with the Department of Defense, for developing, issuing and carrying out the legal and operational guidance at the heart of our interrogation program, and that is another matter for another day.

Mr. Chairman, I thank you, and again I welcome the witnesses.

Chairman ROBERTS. We are pleased to have the Attorney General and the Director of the FBI and the Director of the CIA with us. And in the following order they will be recognized—the Attorney General, and the FBI Director, and the CIA Director. So General Gonzales, if you would like to proceed, sir, you are most welcome to do so at this time.

[The prepared statement of Attorney General Gonzales and Director Mueller follows:]

PREPARED STATEMENT OF ALBERTO R. GONZALES AND ROBERT S. MUELLER III

Chairman Roberts, Vice Chairman Rockefeller, and Members of the Committee:

We are pleased to be here today to discuss the government's use of authorities granted to it by Congress under the Foreign Intelligence Surveillance Act of 1978 (FISA). In particular, we appreciate the opportunity to have a candid discussion about the impact of the amendments to FISA made by the USA PATRIOT Act and how critical they are to the government's ability to successfully prosecute the war on terrorism and prevent another attack like that of September 11 from ever happening again.

As we stated in our testimony to the Senate Judiciary Committee, we are open to suggestions for strengthening and clarifying the USA PATRIOT Act, and we look forward to meeting with people both inside and outside of Congress who have expressed views about the Act. However, we will not support any proposal that would undermine our ability to combat terror ism effect ively.

I. FISA STATISTICS

First, we would like to talk with you about the use of FISA generally. Since September 11, the volume of applications to the Foreign Intelligence Surveillance Court (FISA court) has dramatically increased.

• In 2000, 1,012 applications for surveillance or search were filed under FISA. As the Department's public annual FISA report sent to Congress on April 1, 2005 states, in 2004 we filed 1,758 applications, a 74 percent increase in 4 years.

• Of the 1,758 applications made in 2004, none were denied, although 94 were modified by the FISA court in some substantive way.

II. KEY USES OF FISA AUTHORITIES IN THE WAR ON TERRORISM

In enacting the USA PATRIOT Act, the Intelligence Authorization Act for Fiscal Year 2002, and the Intelligence Reform and Terrorism Prevention Act of 2004, Congress provided the government with vital tools that it has used regularly and effectively in its war on terrorism. The reforms contained in those measures affect every single application made by the Department for electronic surveillance or physical search of suspected terrorists and have enabled the government to become quicker and more flexible in gathering critical intelligence information on suspected terrorists. It is because of the key importance of these tools to the war on terror that we ask you to reauthorize the provisions of the USA PATRIOT Act scheduled to expire at the end of this year. Of particular concern is section 206's authorization of multipoint or "roving" wiretaps, section 207's expansion of FISA' s authorization periods for certain cases, section 214's revision of the legal standard for installing and using pen register/trap and trace devices, and section 215's grant of the ability to obtain a Court order requesting the production of business records related to national security investigations.

In addition, the Intelligence Reform and Terrorism Prevention Act of 2004 includes a "lone wolf' provision that expands the definition of "agent of a foreign power" to include a non-United States person, who acts alone or is believed to be acting alone and who engages in international terrorism or in activities in preparation therefor. This provision is also scheduled to sunset at the end of this year, and we ask that it be made permanent as well.

A. Roving Wiretaps

Section 206 of the USA PATRIOT Act extends to FISA the ability to "follow the target" for purposes of surveillance rather than tie the surveillance to a particular facility and provider when the target's actions may have the effect of thwarting that surveillance. In the Attorney General's testimony at the beginning of this month before the Senate Judiciary Committee, he declassified the fact that the FISA court issued 49 orders authorizing the use of roving surveillance authority under section 206 as of March 30, 2005. Use of roving surveillance has been available to law enforcement for many years and has been upheld as constitutional by several Federal courts, including the Second, Fifth, and Ninth Circuits. Some object that this provision gives the FBI discretion to conduct surveillance of persons who are not approved targets of court-authorized surveillance. This is wrong. Section 206 did not change the requirement that before approving electronic surveillance, the FISA court must find that there is probable cause to believe that the target of the surveillance is either a foreign power or an agent of a foreign power, such as a terrorist or spy. Without section 206, investigators will once again have to struggle to catch up to sophisticated terrorists trained to constantly change phones in order to avoid surveillance.

Critics of section 206 also contend that it allows intelligence investigators to conduct "John Doe" roving surveillance that permits the FBI to wiretap every single phone line, mobile communications device, or Internet connection the suspect may use without having to identify the suspect by name. As a result, they fear that the FBI may violate the communications privacy of innocent Americans. Let me respond to this criticism in the following way. First, even when the government is unsure of the name of a target of such a wiretap, FISA requires the government to provide "the identity, if known, or a description of the target of the electronic surveillance" to the FISA Court prior to obtaining the surveillance order. 50 U.S.C. §§ 1804(a)(3) and 1805(c)(l)(A). As a result, each roving wiretap order is tied to a particular target whom the FISA Court must find probable cause to believe is a foreign power or an agent of a foreign power. In addition, the FISA Court must find "that the actions of *the target* of the application may have the effect of thwarting" the surveillance, thereby requiring an analysis of the activities of a foreign power or an agent of a foreign power that can be identified or described. 50 U.S.C. § 1805 (c)(2)(B). Finally, it is important to remember that FISA has always required that the government conduct every surveillance pursuant to appropriate minimization procedures that limit the government's acquisition, retention, arid dissemination of irrelevant communications of innocent Americans. Both the Attorney General and the FISA Court must approve those minimization procedures. Taken together, we believe that these provisions adequately protect against unwarranted governmental intrusions into the privacy of Americans. Section 206 sunsets at the end of this year.

B. Authorized Periods for FISA Collection

Section 207 of the USA PATRIOT Act has been essential to protecting the national security of the United States and protecting the civil liberties of Americans. It changed the time periods for which electronic surveillance and physical searches are authorized under FISA and, in doing so, conserved limited OIPR and FBI resources. Instead of devoting time to the mechanics of repeatedly renewing FISA applications in certain cases—which are considerable—those resources can be devoted instead to other investigative activity as well as conducting appropriate oversight of the use of intelligence collection authorities by the FBI and other intelligence agencies. A few examples of how section 207 has helped arc set forth below.

Since its inception, FISA has permitted electronic surveillance of an individual who is an agent of foreign power based upon his status as a non-United States person who acts in the United States as "an officer or employee of a foreign power, or as a member" of an international terrorist group. As originally enacted, FISA permitted electronic surveillance of such targets for initial periods of 90 days, with extensions for additional periods of up to 90 days based upon subsequent applications by the government. In addition, FISA originally allowed the government to conduct physical searches of any agent of a foreign power (including United States persons) for initial periods of 45 days, with extensions for additional 45-day periods.

Section 207 of the USA PATRIOT Act changed the law as to permit the government to conduct electronic surveillance and physical search of certain agents of foreign powers and nonresident alien members of international groups for initial periods of 120 days, with extensions for periods of up to 1 year. It also allows the government to obtain authorization to conduct a physical search of any agent of a foreign power for periods of up to 90 days. Section 207 did *not* change the time periods applicable for electronic surveillance of United States persons, which remain at 90 days. By making these time periods equivalent, it has enabled the Department to file streamlined combined electronic surveillance and physical search applications that, in the past, were tried but abandoned as too cumbersome to do effectively.

As the Attorney General testified before the Senate Judiciary Committee, we estimate that the amendments in section 207 have saved OIPR approximately 60,000 hours of attorney time in the processing of applications. Because of section 207's success, we have proposed additional amendments to increase the efficiency of the FISA process. Among these would be to allow coverage of all non-U.S. person agents for foreign powers for 120 days initially with each renewal of such authority allowing continued coverage for 1 year. Had this and other proposals been included in the USA PATRIOT Act, the Department estimates that an additional 25,000 attorney hours would have been saved in the interim. Most of these ideas were specifically endorsed in the recent report of the WMD Commission. The WMD Commission agreed that these changes would allow the Department to focus its attention where it is most needed and to ensure adequate attention is given to cases implicating the civil liberties of Americans. Section 207 is scheduled to sunset at the end of this year.

C. Pen Registers and Trap and Trace Devices

Some of the most useful, and least intrusive, investigative tools available to both intelligence and law enforcement investigators are pen registers and trap and trace devices. These devices record data regarding incoming and outgoing communications, such as all of the telephone numbers that call, or are called by, certain phone numbers associated with a suspected terrorist or spy. These devices, however, do not record the substantive content of the communications, such as the words spoken in a telephone conversation. For that reason, the Supreme Court has held that there is no Fourth Amendment protected privacy interest in information acquired from telephone calls by a pen register. Nevertheless, information obtained by pen registers or trap and trace devices can be extremely useful in an investigation by revealing the nature and extent of the contacts between a subject and his confederates. The data provides important leads for investigators, and may assist them in building the facts necessary to obtain probable cause to support a full content wiretap.

Under chapter 206 of title 18, which—has been in place since 1986, if an FBI agent and prosecutor in a criminal investigation of a bank robber or an organized crime figure want to install and use pen registers or trap and trace devices, the prosecutor must file an application to do so with a Federal court. The application they must file, however, is exceedingly simple: it need only specify the identity of the applicant and the law enforcement agency conducting the investigation, as well as "a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted—by that agency." Such applications, of course, include other information about the facility that will be tar-

geted and details about the implementation of the collection, as well as "a statement of the offense to which the information likely to be obtained . . . relates," but chapter 206 does not require an extended recitation of the facts of the case.

In contrast, prior to the USA PATRIOT Act, in order for an FBI agent conducting an intelligence investigation to obtain FISA authority to use the same pen register and trap and trace device to investigate a spy or a terrorist, the government was required to file a complicated application under title IV of FISA. Not only was the government's application required to include "a certification by the applicant that the information likely to be obtained is relevant to an ongoing foreign intelligence or international terrorism investigation being conducted by the Federal Bureau of Investigation under guidelines approved by the Attorney General," it also had to include the following: information which demonstrates that there is reason to believe that the telephone line to which the pen register or trap and trace device is to be attached, or the communication instrument or device to be covered by the pen register or trap and trace device, has been or is about to be used in communication with:

(A) an individual who is engaging or has engaged in international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States; or

(B) a foreign power or agent of foreign power under circumstances giving reason to believe that the communication concerns or concerned international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States.

Thus, the government had to make a much different showing in order obtain a pen register or trap and trace authorization to find out information about a spy or a terrorist than is required to obtain the very same information about a drug dealer or other ordinary criminal. Sensibly, section 214 of the USA PATRIOT Act simplified the standard that the government mast meet in order to obtain pen/trap data in national security cases. Now, in order to obtain a national security pen/trap order, the applicant must certify "that the information lkely to be obtained is foreign intelligence information not concerning a United States person, or is relevant to an investigation to protect against international terrorism or clandestine intelligence activities." Importantly, the law requires that such an investigation of a United States person may not be conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

Section 214 should not be permitted to expire and return us to the days when it was mare difficult to obtain pen/trap authority in important national security cases than in normal criminal cases. This is especially true when the law already includes provisions that adequately protect the civil liberties of Americans. I urge you to re-authorize section 214.

D. Access to Tangible Things

Section 215 of the USA PATRIOT Act allows the FBI to obtain an order from the FISA Court requesting production of any tangible thing, such as business records, if the items are relevant to an ongoing authorized national security investigation, which, in the case of a United States person, cannot be based solely upon activities protected by the First Amendment to the Constitution. The Attorney General also declassified earlier this month the fact that the FISA Court has issued 35 orders requiring the production of tangible things under section 215 from the date of the effective date of the Act through March 30th of this year. None of those orders was issued to libraries and/or booksellers, and none was for medical or gun records. The provision to date has been used only to order the production of driver's license records, public accommodation records, apartment leasing records, credit card records, and subscriber information, such as names and addresses, for telephone numbers captured through court-authorized pen register devices.

Similar to a prosecutor in a criminal case, issuing a grand jury subpoena for an item relevant to his investigation, so too may the FISA Court issue an order requiring the production of records or items that are relevant to an investigation to protect against international terrorism or clandestine intelligence activities. Section 215 orders, however, are subject to judicial oversight before they are issued—unlike grand jury subpoenas. The FISA Court must explicitly authorize the use of section 215 to obtain business records before the government may serve the order on a recipient. In contrast, grand jury subpoenas are subject to judicial review only if they arc challenged by the recipient. Section 215 orders arc also subject to the same standard as grand jury subpoenas—a relevance standard.

Section 215 has been criticized because it does not exempt libraries and booksellers. The absence of such an exemption is consistent with criminal investigative practice. Prosecutors have always been able to obtain records from libraries and

bookstores through grand jury subpoenas. Libraries and booksellers should not become safe havens for terrorists and spies. Last year, a member of a terrorist group closely affiliated with al Qaeda used Internet service provided by a public library to communicate with his confederates. Furthermore, we know that spies have used public library computers to do research to further their espionage and to communicate with their co-conspirators. For example, Brian Regan, a former TRW employee working at the National Reconnaissance Office, who was convicted of espionage, extensively used computers at five public libraries in Northern Virginia and Maryland to access addresses for the embassies of certain foreign governments.

Concerns that section 215 allows the government to target Americans because of the books they read or websites they visit are misplaced. The provision explicitly prohibits the government from conducting, an investigation of a U.S. person based solely upon protected First Amendment activity. 50 U.S.C. § 1861(a)(2)(B). However, some criticisms of section 215 have apparently been based on possible ambiguity in the law. The Department has already stated in litigation that the recipient of a section 215 order may consult with his attorney and may challenge that order in court. The Department has also stated that the government may seek, and a court may require, only the production of records that are relevant to a national security investigation, a standard similar to the relevance standard that applies to grand jury subpoenas in criminal cases. The text of section 215, however, is not as clear as it could be in these respects. The Department, therefore, is willing to support amendments to Section 215 to clarify these points. Section 215 also is scheduled to sunset at the end of this year.

E. The "Wall"

Before the USA PATRIOT Act, applications for orders authorizing electronic surveillance or physical searches under F1SA had to include a certification from a high-ranking Executive Branch official that "*the* purpose" of the surveillance or search was to gather foreign intelligence information. As interpreted by the courts and the Justice Department, this requirement meant that the "primary purpose" of the collection had to be to obtain foreign intelligence information rather than evidence of a crime. Over the years, the prevailing interpretation and implementation of the "primary purpose" standard had the effect of sharply limiting coordination and information sharing between intelligence and law enforcement personnel. Because the courts evaluated the government's purpose for using FISA at least in part by examining the nature and extent of such coordination, the more coordination that occurred, the more likely courts would find that law enforcement, rather than foreign intelligence collection, had become the primary purpose of the surveillance or search.

During the 1980's, the Department operated under a set of largely unwritten rules that limited to some degree information sharing between intelligence and law enforcement officials. In 1995, however, the Department established formal procedures that more clearly separated law enforcement and intelligence investigations and limited the sharing of information between intelligence and law enforcement personnel even more than the law required. The promulgation of these procedures was motivated in part by the concern that the use of FISA authorities would not be allowed to continue in particular investigations if criminal prosecution began to overcome intelligence gathering as an investigation's primary purpose. The procedures were intended to permit a degree of interaction and information sharing between prosecutors and intelligence officers while at the same time ensuring that the FBI would be able to obtain or continue FISA coverage and later use the fruits of that coverage in a criminal prosecution. Over time, however, coordination and information sharing between intelligence and law enforcement personnel became more limited in practice than was allowed in reality. A perception arose that improper information sharing could end a career, and a culture developed within the Department sharply limiting the exchange of information between intelligence and law enforcement officials.

Sections 218 and 504 of the USA PATRIOT Act helped to bring down this "wall" separating intelligence and law enforcement officials. They erased the perceived statutory impediment to more robust information sharing between intelligence and law enforcement personnel. They also provided the necessary impetus for the removal of the formal administrative restrictions as well as the informal cultural restrictions on information sharing.

Section 218 of the USA PATRIOT Act eliminated the "primary purpose" requirement. Under section 218, the government may conduct FISA surveillance or searches if foreign intelligence gathering is a "significant" purpose of the surveillance or search. This eliminated the need for courts to compare the relative weight of the "foreign intelligence" and "law enforcement" purposes of the surveillance or

search, and allows increased coordination and sharing of information between intelligence and law enforcement personnel. Section 218 was upheld as constitutional in 2002 by the FISA court of Review. This change, significantly, did not affect the government's obligation to demonstrate that there is probable cause to beliew that the target is a foreign power or an agent of a foreign power. Section 504—which is *not* subject to sunset—buttressed section 218 by specifically amending FISA to allow intelligence officials conducting FISA surveillances or searches to "consult" with Federal law enforcement officials to "coordinate" efforts to investigate or protect against international terrorism, espionage, and other foreign threats to national security, and to clarify that such coordination "shall not" preclude the certification of a "significant" foreign intelligence purpose or the issuance of an authorization order by the FISA court.

The Department moved aggressively to implement sections 218 and 504. Following passage of the Act, the Attorney General adopted new procedures designed to increase information sharing between intelligence and law enforcement officials, which were affirmed by the FISA court of Review on November 18, 2002. The Attorney General has also issued other directives to further enhance information sharing and coordination between intelligence and law enforcement officials. In practical terms, a prosecutor may now consult freely with the FBI about what, if any, investigative tools should be used to best prevent terrorist attacks and protect the national security. Unlike section 504, section 218 is scheduled to sunset at the end of this year.

The increased information sharing facilitated by the USA PATRIOT Act has led to tangible results in the war against terrorism: plots have been disrupted; terrorists have been apprehended; and convictions have been obtained in terrorism cases. Information sharing between intelligence and law enforcement personnel, for example, was critical in successfully dismantling a terror cell in Portland, Oregon, popularly known as the "Portland Seven" as well as a terror cell in Lackawanna, New York. Such information sharing has also been used in the prosecution of several persons involved in al Qaeda drugs-for-weapons plot in San Diego, two of whom have pleaded guilty; nine associates in Northern Virginia of a violent extremist group known as Lashkar-e-Taiba that has ties to al Qaeda, who were convicted and sentenced to prison terms ranging from 4 years to life imprisonment; two Yemeni citizens, Mohammed Ali Hasan Al-Moayad and Molishen Yahya Zayed, who were charged and convicted for conspiring to provide material support to al Qaeda and HAMAS; Khaled Abdel Latif Dumeisi, who was convicted by a jury in January 2004 of illegally acting as an agent of the former government of Iraq as well as two counts of perjury; and Enaam Arnaout, the Executive Director of the Illinois-based Benevolence International Foundation, who had a long-standing relationship with Osama Bin Laden and pleaded guilty to a racketeering charge, admitting that he diverted thousands of dollars from his charity organization to support Islamic militant groups in Bosnia and Chechnya. Information sharing between intelligence and law enforcement personnel has also been extremely valuable in a number of other ongoing or otherwise sensitive investigations that we arc not at liberty to discuss today.

While the "wall" primarily hindered the flow of information from intelligence investigators to law enforcement investigators, another set of barriers, before the passage of the USA PATRIOT Act, often hampered law enforcement officials from sharing information with intelligence personnel and others in the government responsible for protecting the national security. Federal law, for example, was interpreted generally to prohibit Federal prosecutors from disclosing information from grand jury testimony and criminal investigative wiretaps to intelligence and national defense officials even if that information indicated that terrorists were planning a future attack, unless such officials were actually assisting with the criminal investigation. Sections 203(a) and (b) of the USA PATRIOT Act, however, eliminated these obstacles to information sharing by allowing for the dissemination of that information to assist Federal law enforcement, intelligence, protective, immigration, national defense, and national security officials in the performance of their official duties, even if their duties arc unrelated to the criminal investigation. (Section 203(a) covers grand jury information, and section 203(b) covers wiretap information.) Section 203(d), likewise, ensures that important information that is obtained by law enforcement means may be shared with intelligence and other national security officials. This provision does so by creating a generic exception to any other law purporting to bar Federal law enforcement, intelligence, immigration, national defense, or national security officials from receiving, for official use, information regarding foreign intelligence or counterintelligence obtained as part of a criminal investigation. Indeed, section 905 of the USA PATRIOT Act requires the Attorney General to expeditiously disclose to the Director of Central Intelligence foreign intelligence

acquired by the Department of Justice in the course of a criminal investigation unless disclosure of such information would jeopardize an ongoing investigation or impair other significant law enforcement interests.

The Department has relied on section 203 in disclosing vital information to the intelligence community and other Federal officials on many occasions. Such disclosures, for instance, have been used to assist in the dismantling of terror cells in Portland, Oregon and Lackawanna, New York and to support the revocation of suspected terrorists' visas.

Because two provisions in section 203: sections 203(b) and 203(d) are scheduled to sunset at the end of the year, we provide below specific examples of the utility of those provisions. Examples of cases where intelligence information from a criminal investigation was appropriately shared with the Intelligence Community under Section 203(d) include:

• Information about the organization of a violent jihad training camp including training in basic military skills, explosives, weapons and plane hijackings, as well as a plot to bomb soft targets abroad, resulted from the investigation and criminal prosecution of a naturalized United States citizen who was associated with an al-Qaeda related group;

• Travel information and the manner that monies were channeled to members of a seditious conspiracy who traveled from the United States to fight alongside the Taliban against U.S. and allied forces;

• Information about an assassination plot, including the use of false travel documents and transporting monies to a designated State sponsor of terrorism resulted from the investigation and prosecution of a naturalized United States citizen who had been the founder of a well-known United States organization;

• Information about the use of fraudulent travel documents by a high-ranking member of a designated foreign terrorist organization emanating from his criminal investigation and prosecution revealed intelligence information about the manner and means of the terrorist group's logistical support network which was shared in order to assist in protecting the lives of U.S. citizens;

• The criminal prosecution of individuals who traveled to, and participated in, a military-style training camp abroad yielded intelligence information in a number of areas including details regarding the application forms which permitted attendance at the training camp; after being convicted, one defendant has testified in a recent separate Federal criminal trial about this application practice, which assisted in the admissibility of the form and conviction of the defendants; and

• The criminal prosecution of a naturalized U.S. citizen who had traveled to an Al-Qaeda training camp in Afghanistan revealed information about the group's practices, logistical support and targeting information.

Title Ill information has similarly been shared with the Intelligence Community through section 203(b). The potential utility of such information to the intelligence and national security communities is obvious: suspects whose conversations arc being monitored without their knowledge may reveal all sorts of information about terrorists, terrorist plots, or other activities with national security implications. Furthermore, the utility of this provision is not theoretical: the Department has made disclosures of vital information to the intelligence community and other Federal officials under section 203(b) on many occasions, such as:

• Wiretap interceptions involving a scheme to defraud donors and the Internal Revenue Service and illegally transfer monies to Iraq generated not only criminal charges but information concerning the manner and means by which monies were funneled to Iraq; and

• Intercepted communications, in conjunction with a sting operation, led to criminal charges and intelligence information relating to money laundering, receiving and attempting to transport night-vision goggles, infrared army lights and other sensitive military equipment relating to a foreign terrorist organization.

Section 203 is also critical to the operation of the National Counterterrorism Center. The FBI relies upon section 203(d) to provide information obtained in criminal investigations to analysts in the new National Counterterrorism Center, thus assisting the Center in carrying out its vital counterterrorism missions. The National Counterterrorism Center represents a strong example of section 203 information sharing, as the Center uses information provided by law enforcement agencies to produce comprehensive terrorism analysis; to add to the list of suspected terrorists on the TIPOFF watchlist; and to distribute terrorism-related information across the Federal Government.

In addition, last year, during a series of high-profile events—the G–8 Summit in Georgia, the Democratic Convention in Boston and the Republican Convention in New York, the November 2004 Presidential election, and other events—a task force used the information sharing provisions under Section 203(d) as part and parcel of

performing its critical duties. The 2004 Threat Task Force was a successful interagency effort where there was a robust sharing of information at all levels of government.

F. Protecting Those Complying with FISA Orders

Often, to conduct electronic surveillance and physical searches, the United States requires the assistance of private communications providers to carry out such court orders. In the criminal context, those who assist the government in carrying out wiretaps arc provided with immunity from civil liability. Section 225, which is set to sunset, provides immunity from civil liability to communication service providers and others who assist the United States in the execution of FISA orders. Prior to the passage of the USA PATRIOT Act, those assisting in the carrying out of FISA orders enjoyed no such immunity. Section 225 simply extends the same immunity that has long existed in the criminal context to those who assist the United States in carrying out orders issued by the FISA court. Providing this protection to communication service providers for fulfilling their legal obligations helps to ensure prompt compliance with FISA orders.

CONCLUSION

It is critical that the elements of the USA PATRIOT Act subject to sunset in a matter of months be renewed. Failure to do so would take the Intelligence Community and law enforcement back to a time when a full exchange of information was not possible and the tools available to defend against terrorists were inadequate. This is unacceptable. The need for constant vigilance against terrorists wishing to attack our Nation is real, and allowing USA PATRIOT Act provisions to sunset would damage our ability to prevent such attacks.

We thank the Committee for the opportunity to discuss the importance of the USA PATRIOT Act to this nation's ongoing war against terrorism. This Act has a proven record of success in protecting the American people. Provisions subject to sunset must be renewed. We look forward to working with the Committee in the weeks ahead. We appreciate the Committee's close attention to this important issue. We would be pleased to answer any questions you may have. Thank you.

STATEMENT OF THE HONORABLE ALBERTO R. GONZALES, ATTORNEY GENERAL OF THE UNITED STATES

Attorney General GONZALES. Thank you, Mr. Chairman.

Chairman Roberts, Vice Chairman Rockefeller, Members of this Committee, I am pleased to be here to talk about reauthorization of the PATRIOT Act. I really appreciate this opportunity to come before Congress to discuss our successes in the war on terror and to find new ways to fight for freedom more effectively and consistent with the values that we all cherish as Americans.

As the distinguished Members of this Committee know, the threat of terrorism remains very serious and it is critical that Congress continues to provide tools that enable prosecutors and law enforcement to both confront terrorism and investigate and prosecute other serious crimes.

I believe the authorities in the PATRIOT Act have enabled us to better protect America. But, the exercise of government authority is always worthy of respectful and accurate discussion. I'm open to suggestions for strengthening and clarifying the Act, but I cannot support amendments that will weaken our ability to protect our nation.

The PATRIOT Act, as we know, has helped dismantle the wall that used to separate law enforcement from intelligence officials. Prior law, as interpreted and implemented, sharply limited the ability of law enforcement and intelligence officers to share information and connect the dots in terrorism and espionage investigations.

As we know, section 203 and section 218 of the PATRIOT Act, which are scheduled to sunset at the end of this year, brought down this wall. And together these provisions have reduced the statutory and cultural barriers to information sharing. And it is information sharing, as the 9/11 Commission and the WMD Commission made clear, and as this Committee knows full well, that will make the difference in our ongoing efforts to prevent terrorism.

This Committee is familiar with the successful use of section 218, including investigation of the Portland Seven and the Virginia Jihad. Section 203 along with section 218 was used extensively during the investigation of the Holy Land Foundation in 2004. Law enforcement professionals tell me that allowing sections 203 and 218 to expire would discourage information sharing, making it more difficult for us to disrupt terrorist plots.

There are other similar commonsense PATRIOT Act provisions that also will expire if Congress does not take action. Section 206, which provides national security investigators with an authority long possessed by criminal investigators, authorizes the use of multi-point or roving wiretaps, tied to a specific target rather than a specific communications facility. Before the PATRIOT Act these orders were not available for a national security investigation under FISA, a gap in the law that we believe sophisticated terrorists or spies could easily exploit. Although specific examples of the use of multi-point wiretaps under section 206 remain classified, I can represent in this open hearing that this authority has been very valuable.

As of March 30 this year we have used this authority 49 times. Importantly, 206 contains numerous safeguards to protect civil liberties. The FISA court can only issue a roving wiretap order upon a finding of probable cause, the order must always be connected to a particular target, and minimization procedures must be followed concerning the collection, the retention and dissemination of information about U.S. persons.

Section 215 also filled a gap in the law. It granted national security investigators authority to seek a court order for the production of records relevant to a foreign intelligence investigation, similar to a prosecutor's authority to use grand jury subpoenas as the building blocks of criminal investigations. Use of this provision has been judicious. We have used this authority 35 times as of March 30 of this year. Moreover, we have not sought a Section 215 order to obtain library or bookstore records, medical records, or gun sale records. Let me be clear, the reading habits of ordinary Americans are of no interest to those investigating terrorists or spies.

Section 213, although not scheduled to sunset is another valuable provision of the PATRIOT Act. Section 213 codified one consistent process and standard for delayed notice search warrants, which can be used in limited circumstances, with judicial approval, to avoid tipping off criminals who otherwise might flee, destroy evidence, intimidate or kill witnesses, cutoff contact with associates, or take other action to evade arrest.

Now the portion of Section 213 that has received the most attention is the provision allowing a court to authorize delayed notice if immediate notice would "seriously jeopardize" an investigation. I

would like to describe one actual case where immediate notice would have seriously jeopardized an investigation.

In this case, the Justice Department obtained a delayed notice search warrant for a Federal Express package that contained counterfeit credit cards. At the time of the search it was very important not to disclose the existence of a Federal investigation, as this would have exposed a related Title III wiretap that was ongoing for major drug trafficking activities. An organized crime drug enforcement task force, which included agents from the DEA, the IRS, the Pittsburgh police department and other State and local agencies was engaged in a multi-year investigation that resulted in the indictment of the largest drug trafficking organization ever prosecuted in the western district of Pennsylvania.

While the drug trafficking investigation was ongoing it became clear that several leaders of the drug trafficking conspiracy had ties to an ongoing credit card fraud operation. An investigation into the credit card fraud was undertaken and a search was made of a Federal Express package that contained fraudulent credit cards. Had notice of the Federal Express search tied to the credit card fraud investigation been immediately given, it could have revealed the ongoing drug trafficking investigation prematurely and the drug trafficking investigation might have been seriously jeopardized. Even modest delay would not have been available if this provision of section 213 were deleted. It is critical that law enforcement continue to have this vital tool for those limited circumstances where a court finds good cause to permit the temporary delay of notification of a search.

Finally, I'd like to close by addressing a common question that must be answered by this Committee and this Congress—the issue of whether we should continue to impose sunset provisions on critical sections of the PATRIOT Act. The PATRIOT Act was a swift and decisive response to the attacks of September 11. In the weeks and months following the attacks in Washington, Pennsylvania, and New York, Democrats and Republicans came together to address the vulnerabilities in our nation's defenses.

Both Congress and the administration worked with experienced law enforcement, intelligence and national security personnel to design legislation to better protect the American people. Although there was extensive consideration in 2001, and although it is unusual to impose sunsets on statutory investigative tools, Congress included sunsets for certain provisions of the PATRIOT Act because Members wanted to ensure that we were not risking the very liberties we were setting out to defend. And I think today we can all be proud.

The track record established over the past 3 years has demonstrated the effectiveness of the safeguards of civil liberties put in place when the Act was passed. There has not been one verified case of civil liberties abuse. Our Nation is stronger and safer; our bipartisan work has been a success.

The Department of Justice has exercised care and restraint in the use of these important authorities because we are committed to the rule of law. We have followed the law because it is the law, not because it is scheduled to sunset. With or without sunsets, our dedication to the rule of law will continue. The Department will

strive to continue to carry out its work lawfully and appropriately, and as a citizen I expect Congress will continue its active oversight over our use of the PATRIOT Act, not because it sunsets but because oversight is a constitutional responsibility of Congress.

So, given the Department's record in using these authorities, the obvious effectiveness of these tools in stopping violent crimes and protecting our nation, and the authority of Congress to re-examine these provisions at any time to correct abuses, the sunset provisions are, in my judgment, no longer necessary and should be repealed.

The authorities in the PATRIOT Act are critical to our nation's efforts in the war against terrorism. The Act has a proven record of success in protecting the security of the American people while simultaneously respecting civil liberties. And I question how we can afford to allow its most important provisions to sunset. The efforts of the terrorists to strike our country surely will not sunset.

I look forward to continuing to work with this Committee in the period ahead, listening to and responding to your concerns, and joining together again to protect the security of the American people.

Thank you, Mr. Chairman.

Chairman ROBERTS. Thank you, General.

We now recognize Director Mueller. Welcome back to the Committee, Bob.

STATEMENT OF THE HONORABLE ROBERT S. MUELLER, III, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

Director MUELLER. Thank you, and good morning, Mr. Chairman. Senator Rockefeller, and other Members of the Committee, good morning. I'm also pleased to be here today to talk about the PATRIOT Act and how it has assisted us in the war on terror.

Indeed, the PATRIOT Act has changed the way the FBI operates, and I will say that many of our operational counterterrorism successes since September 11 are the direct result of the changes incorporated in the PATRIOT Act. The formal statement that was submitted by the Attorney General and myself focuses on the key areas and the key uses of the FISA authorities in the war on terrorism. And as is set forth in that statement, I share the Attorney General's belief that these vital tools that have been used regularly and effectively in our efforts to prevent another attack should be renewed.

This morning I would like to emphasize the importance of a portion of the PATRIOT Act, that portion that relates to information-sharing, and address the fundamental manner in which those provisions have changed the way we do business.

Last week I know this Committee heard directly from our operational personnel, who provided in a classified setting specific examples of how the PATRIOT Act information-sharing provisions have altered the landscape for conducting terrorism investigations. The Committee heard not only from FBI headquarters and FBI field office personnel but also from our partners in the CIA and our partners at the NSA about the coordinated teamwork approach that has guided our operations over the past 3 years.

Such interagency teamwork has successfully foiled terrorist-related operations and cells from Seattle to Detroit to Lackawanna, New York. And while the law prior to the PATRIOT Act provided for some exchange of information, that law was complex and, as a result, agents often erred on the side of caution and refrained from sharing information.

Our current integrated approach, which grew from the PATRIOT Act's information-sharing provisions, eliminated that hesitation and now allows agents to more openly work with other governmental agencies, whether they be at the Federal, the State or the local level.

Prior to the PATRIOT Act, the Federal law was interpreted to limit the ability of our criminal investigators to disclose criminal wiretap or grand jury information to counterparts working on intelligence investigations. Sections 203(a) and (b) of the PATRIOT Act eliminated these barriers to information sharing, allowing for the routine sharing of information derived from these important criminal tools. And section 203(b) ensures that information developed through law enforcement methods other than grand jury subpoenas or criminal wiretaps can also be shared with our intelligence partners at the Federal, State and local levels, as well as our partners overseas.

Although information does not flow between agencies with a PATRIOT Act label on it, it is quite clear that information derived from the FBI's investigations is now assisting other agencies in performing their missions, principally overseas. As an example, an FBI field office obtained information of intelligence value while conducting a criminal investigation and shared this information with the CIA and other intelligence entities. In this particular investigation, a Title III intercept showed that the subject of the investigation was in contact with an overseas number.

Taking that number, investigation undertaken by the CIA and others determined links between this number and a number associated with a subject of a terrorism investigation who had been captured. This sharing of information permitted additional investigation by each of the intelligence community components, integrating information that had been found and put together in the United States with information that had been found and put together overseas.

This sharing of information is absolutely fundamental to the safety of the American public in the future. And while section 203 removed barriers to sharing criminally-derived information with our intelligence community partners, section 218 of the PATRIOT Act was the first step in dismantling the wall between the criminal and our intelligence investigators. It eliminated the primary purpose requirement that arose from statutory interpretation by the FISA court and replaced it with a "significant purpose" test. As a result, FBI agents working on intelligence and counterintelligence matters now have greater latitude to consult criminal investigators or prosecutors without putting their investigations at risk.

The increased coordination and information sharing between intelligence and law enforcement agents facilitated by the PATRIOT Act has allowed us, the FBI, to approach our cases as a single integrated investigation using all of its tools, both criminal and intel-

ligence, as long as the requirements for each of those tools are properly met. The successes of these cases are entirely dependent on the free flow of information between respective investigators and analysts.

Mr. Chairman, I would like to close with making one point that I do think has been not fully amplified in the debate, in the public debate, on the PATRIOT Act and its tools, and that is the role of the Federal judiciary. For example, the FBI must seek authority from a Federal judge to utilize a roving wiretap and that judge must find that there is probable cause to believe that the target of the surveillance is either a foreign power or an agent of a foreign power, such as a terrorist or a spy.

If the name of the individual on whom we are seeking roving surveillance is not known to us, we must provide a description of the individual and that person's activities to satisfy a Federal judge that, again, there is probable cause to believe that this person is a terrorist or a spy and that his actions may have the effect of thwarting surveillance.

Similarly, under 215, the FBI does not write a warrant authorizing access to business records; rather, it is a Federal judge that issues the order upon a certification by the government that the items requested are relevant to an ongoing national security investigation. And finally a judge authorizes the government to conduct a search, and only the Federal judge can then authorize the government to delay notification, upon making of a showing—delay notification to the subject of that search.

Mr. Chairman, the role of the Federal judiciary is vital to protecting the rights of individuals, particularly where more intrusive means of investigation are utilized. In addition to the oversight by Federal judges, the activities of the FBI and DOJ prosecutors are always tethered to the Constitution, and we take our responsibility exceptionally seriously.

As the Attorney General has already noted, I as well am unaware of any substantiated allegation that the government has abused its authority under the PATRIOT Act. This is a tribute to the men and women in Federal law enforcement and the men and women in the intelligence community as well as the Federal prosecutors, all of whom are committed to responsibly using the statutes provided by Congress. In renewing these provisions scheduled to sunset at the end of this year, Congress will ensure that the FBI will continue to have the tools we need to combat the very real threat to America posed by terrorists and their supporters.

Thank you for the opportunity to appear here today. I'm happy to answer any questions.

Chairman ROBERTS. Mr. Director, we thank you very much for a comprehensive statement.

We now recognize Director Goss.

[The prepared statement of Director Goss follows:]

PREPARED STATEMENT OF PORTER J. GOSS

Good morning, Mr. Chairman, Mr. Vice Chairman, and Members of the Committee.

I appreciate the opportunity to appear before you today to discuss the important role the USA PATRIOT Act has played in improving the ability of the Intelligence Community to fight the global war on terrorism. As you recall, in October 2001,

Members of Congress worked together in a united effort to create legislation that would give Federal law enforcement and intelligence officials the additional legal authorities needed to combat the terrorist threat to our country. I can assure you that the tools you provided in the PATRIOT Act have greatly assisted intelligence officials in the on-going effort to interdict and disrupt terrorist groups and individuals who seek to do harm to our country and our citizens. I will now briefly discuss how the PATRIOT Act has been most helpful to intelligence officers, and, along with my colleagues, the Attorney General, and the Director, FBI, urge you to renew permanently those provisions of the Act due to expire at the end of this year.

INFORMATION SHARING

The PATRIOT Act has played a large role in an information-sharing transformation throughout the Federal law enforcement and intelligence communities, permitting a cultural shift in previously unshakeable paradigms. Today, intelligence officers have the ability to receive foreign intelligence information from Federal law enforcement officials that has been obtained during the course of criminal investigations, and the PATRIOT Act makes it clear that this information may include information obtained from grand jury proceedings and criminal investigative wiretaps. If the various provisions of the PATRIOT Act that authorize this foreign intelligence information sharing are permitted to sunset, we will lose some of the essential weapons used to counter the grave threats posed by al-Qaeda and other terrorist groups. Now is not the time to engage in unilateral disarmament.

Of particular concern is the "wall" that served to limit the sharing of information between intelligence and law enforcement officers. The wall was a barrier against full and discerning dialog and greatly impinged on the effective use of critical tools necessary to fight terrorism. Continuation of the PATRIOT Act information sharing provisions ensures while we do not hamstring ourselves in this vital area of intelligence and law enforcement collaboration we will also take the appropriate steps to protect the privacy rights and civil liberties of Americans.

If the information sharing provisions of the PATRIOT Act are permitted to expire, currently robust information sharing relationships may be adversely impacted as officials seek guidance on what information sharing is permitted absent the PATRIOT Act authorities, because the clarifying and instructive benefits of the PATRIOT Act will be lost. As any war-fighter will tell you, a necessary tool in fighting the battle is the ability to share information freely to get the job done expeditiously and effectively. Constructs that otherwise preclude information sharing had to be torn down, and the PATRIOT Act provisions accomplished that end. Resurrection of these obstacles will significantly impede the war effort.

If, however, the provisions scheduled to sunset are renewed, ongoing efforts by government officials to use the PATRIOT Act authorities to improve information sharing, to utilize highly valuable limited resources most effectively, and to continue the cooperation between agencies, will continue. One of the most positive illustrations of this collaborative environment may be found in the National Counterterrorism Center (NCTC).

• NCTC is a specific example of how the information-sharing authorities of the PATRIOT Act have been leveraged to benefit the Federal Government as a whole.

- NCTC personnel assigned from multiple Federal law enforcement and intelligence community entities receive foreign intelligence information from the FBI that is obtained by the Bureau during criminal investigations and disseminated to NCTC under authorities granted by the PATRIOT Act.
- This information is compiled with other foreign intelligence information obtained through traditional intelligence collection methods and is used to produce all-source terrorism analysis that is subsequently disseminated throughout the Intelligence Community and to officers within the Department of Homeland Security and the FBI.
- NCTC officials also use terrorist identity information disseminated by Federal law enforcement officials under PATRIOT Act authorities to maintain TIPOFF, a data base used to prevent known and suspected terrorists from entering the United States. NCTC officials estimate that the number of known or suspected terrorists that have been intercepted at US borders, based on FBI reporting alone, has increased due to the information sharing provisions of the PATRIOT Act.

In addition to talking about the information sharing provisions that are due to expire in a few months, I wanted to also highlight the importance of another information sharing authority in the PATRIOT Act. This provision, section 905 of the Act, not only permits, but also generally requires the Attorney General to expeditiously disclose to the DCI, and now to the DNI under the Intelligence Reform Act

of 2004, foreign intelligence information acquired by the Department of Justice during the course of criminal investigations. This provision, like the expiring information sharing provisions, encourages the free flow of intelligence information by removing any doubt from the minds of Federal law enforcement officials that sharing is authorized.

FISA PRIORITIZATION

My colleagues from the Department of Justice will discuss with you how Federal law enforcement officials have benefited from amendments made to the Foreign Intelligence Surveillance Act (FISA) by the PATRIOT Act. I would like to advise you how authority granted by the PATRIOT Act has enabled the DCI to improve the process for submitting FISA requests to the Attorney General and the Foreign Intelligence Surveillance Court.

The PATRIOT Act called upon the DCI to establish requirements and priorities for foreign intelligence information to be collected under the FISA and to assist the Attorney General with the dissemination of FISA-derived intelligence. The DNI is now charged with these responsibilities under the Intelligence Reform and Terrorism Prevention Act of 2004.

In June 2003, the DCI implemented this provision of the PATRIOT Act by creating an interagency panel to prioritize requests seeking authorization to engage in foreign intelligence collection operations under the FISA. The panel, coordinated by the ADCI for Collection, includes representatives from the CIA, DOJ, FBI, and NSA. The prioritization mechanisms established by the panel are working well and have enabled intelligence officials to carefully weigh and accommodate competing priorities for FISA-authorized collection operations, making the best use of the limited resources of the FBI, NSA, CIA, and the Department of Justice, and most specifically, the FISA Court.

CONCLUSION

Let me conclude my comments today by saying that the PATRIOT Act has improved the ability of intelligence officials to fight the war on terrorism by removing legal and cultural impediments that previously prohibited or discouraged the sharing of foreign intelligence obtained by Federal law enforcement officials during the course of criminal investigations, and by enhancing the ability of the intelligence and law enforcement communities to collect and analyze vital information to wage an effective and continuing effort to disrupt international terrorist activities. Failure to renew the provisions due to sunset will ill-serve the national security of the United States.

I thank you for inviting me to speak with you today, and for your continued support.

STATEMENT OF THE HONORABLE PORTER J. GOSS, DIRECTOR, CENTRAL INTELLIGENCE AGENCY

Director GOSS. Thank you, Mr. Chairman. Good morning. Good morning, Mr. Vice Chairman, Members of the Committee.

I would propose that I ask, in the interest of time and not to repeat some things that I would like to say that have already been said, that you would accept my full statement and allow me to abbreviate it.

Chairman ROBERTS. Without object it is so ordered, and your request is gladly approved.

Director GOSS. I thank you.

I do associate myself very much with the statements made by the Attorney General and the Director of the FBI. There are a couple points I would like to make as the Director of the Central Intelligence Agency, although I would also be very happy to answer questions as the DCI, which I was when some of this material was going on, and I have had the responsibility of signing FISA requests and a somewhat different role in that position, which now Ambassador Negroponte, of course, has assumed.

I would simply say that it is extremely important for us not to under-emphasize the information sharing, the coordination, cooperation, change of cultures, breaking down of walls, breaking of stovepipes, if you will. Remember how much time was spent by Members of Congress and various Committees, oversight boards, specially set-up commissions, independent commissions, and so forth, after 9/11 that said we must work better together.

And there is no question that the manifestation of that has been made possible by the PATRIOT Act in enterprises such as TTIC, the Terrorist Threat Integration Center, which has now graduated into the National Counterterrorism Center, which is probably a showcase of where we can point out how we bring information together and how it works well for the safety of our country in dealing with the terrorist threat.

Obviously I am here today representing the national foreign intelligence program as seen through the CIA's eyes and there is a lot I will not be able to say in open session but I am very happy to talk about in closed session.

Certainly, sources and methods are involved in the PATRIOT Act, in our programs, but authorities are appropriate for us to discuss. These authorities are particularly essential for the intelligence community, in particular 203(d) and 214. These represent areas in sharing, breaking down the "wall" that has been referred to already—and talk a little bit about modernization, of being able to keep up with the advantages we have to deal with terrorists using technology as it exists today, which, of course, the terrorists are taking advantage of. We need to be able to deal with that, counter that, and get ahead of it for our own purposes.

I think those two provisions, from our perspective, are critically important, although I would suggest that the PATRIOT Act has served this country extremely well across the board. And I also am not aware of any serious problems with it in terms of invasion of rights or liberties.

I do admire the safeguards that Director Mueller has referred to. I have spent some time coming in and signing FISA requests as the DCI. There is a clear need to prioritize and understand each request, understand what is going on. I think that process works well. I'm not sure what other testimony has been on that, but my testimony on it is that it works timely; it works well. It deals with the crush of business, as it were, on a prioritization basis, which is very important. And it does provide fresh eyes.

In my case, I must have looked at a couple of dozen things that I hadn't seen before because somebody else had signed them or they had come in under a different channel, and I was very satisfied that this process was working exactly the way any American would want it, which would be to stay out of their business but to be applied to people who are trying to infringe our liberties and damage our people, innocent people, from far shores—people we call terrorists.

So I think this is a very good use of time, Mr. Chairman, to be reviewing this matter and being suggestive of the position that we've got a success here; perhaps we could make it a little better. But I certainly don't want to give away the tools that, I can assure you, the intelligence community is using well.

Thank you, sir.

Chairman ROBERTS. Senators will be recognized for 5 minutes in the order of their arrival and there will be a second round, if needed.

I have a question in regards to administrative subpoenas. In the past, the President and Director Mueller have asked Congress to authorize the FBI to issue what's called an administrative subpoena in international terrorism investigations. If the government can use administrative subpoenas in health care fraud investigations and in drug cases, then the obvious question is why can't we use them in the international terrorism investigations. It seems to me that the administrative subpoena tool should be available for all authorized national security investigations that are conducted in accordance with the Attorney General guidelines, not just terrorism cases.

I was surprised, however, that the prepared statement by the Department of Justice and the FBI does not echo these earlier requests for administrative subpoenas. Has the President changed his mind on this issue? That's my first question.

Attorney General Gonzales, are you in favor of Congress authorizing the administrative subpoena in national security investigations? And I would also pose the same question to Director Mueller.

General.

Attorney General GONZALES. Mr. Chairman, the President has not changed his position. We believe administrative subpoenas would be an additional valuable tool to deal with the terrorist threat. And so I want to reassure the Committee that we continue to believe that that is a necessary tool and would respectfully request a serious consideration of that request.

Chairman ROBERTS. Director Mueller.

Director MUELLER. Certainly, yes, we believe that it would be an exceptionally helpful tool in filling the gaps in getting us the information we need in our national security investigations. I will say that I spent a substantial amount of time on that in our prepared statement before the Judiciary Committee. It was in looking at a sense of brevity that I did not mention it in my opening remarks.

But yes, we continue to press for administrative subpoenas. We think it is a very useful tool. As you have pointed out, Mr. Chairman, if it is available in health care fraud cases, child pornography cases, narcotics cases—I think there are approximately 300 separate statutes to provide for the utility or the use of administrative subpoenas—it makes very good sense for us to have that tool available when it comes to national security investigations.

Chairman ROBERTS. I thank you both for your responses.

We're in the process of finishing up our audit report on the FISA process. One of the things that we have found out was that the Department of Justice and the FBI—I don't know what grade I would give it, but it's not a 92; it doesn't rate that high; maybe 70, passing, I'm not quite sure—of implementing the FISA business records provisions, section 215 of the PATRIOT Act, took more than 2½ years to issue the first application.

Regardless, your joint statement indicates that approximately 35 FISA—I think maybe you said 39—business record court orders have been issued since then, and most of these were issued for tele-

phone numbers captured through the court-authorized pen registers. My question to you is, why isn't this technique being used more?

Director MUELLER. Well, we have the possibility in some areas of using National Security Letters, as you're well aware.

Chairman ROBERTS. Yes.

Director MUELLER. We have, in those cases where it's being handled jointly as an intelligence as well as perhaps a grand jury investigation, it may well be that we're using grand jury subpoenas. But in those areas where 215 fills the void, we have gone through the 215 process.

If you're comparing on the one hand the use of the 215 process and the administrative subpoena process, they're night and day. The fact of the matter is, the 215 process is somewhat burdensome. Nonetheless, that is the way the PATRIOT Act established it. It does go before a judge. So we have had, particularly in the last couple of years, occasions where we have utilized that tool.

Attorney General GONZALES. Mr. Chairman, I think one message that we would like to leave with the Committee today is that we take all these authorities very seriously and we try to act responsibly and judiciously in exercising these authorities. If we need to exercise a 215 authority, it will be exercised. If we don't need to exercise it, because there are other ways of getting information, we'll pursue other avenues.

Chairman ROBERTS. I have a yellow light here, but I'm going to try to sneak the last question in, with apologies to my colleagues.

Mr. Attorney General and Director Mueller, at a hearing we held last week, the FBI's investigation of Brandon Mayfield was cited as an abuse of the PATRIOT Act. I know that your answer might be circumscribed somewhat by the fact that there's a pending lawsuit over this case. But could you please respond to that allegation?

Attorney General GONZALES. I'd be happy to, Mr. Chairman.

You're right; I am limited in what I can say. We have done an exhaustive review of the allegations made by communication from the ACLU to Senator Feinstein specifically about Brandon Mayfield. I am told there was not an abuse of the PATRIOT Act. There are misimpressions about what authorities were in fact used in connection with that investigation. People have the mistaken belief that the section 213 authority, delayed notification search warrant, was used there, but that's not the case. It was a straightforward FISA application in connection with that case.

I think we all need to understand, though, when people ask the question, was the PATRIOT Act implicated or used at all in connection with that investigation, sure it was, to the extent that FISA was amended by the PATRIOT Act in areas of information sharing like 218.

And so to the extent that the PATRIOT Act caused changes in FISA, then clearly it was implicated. But from what we can tell, there was no abuse or misuse of the PATRIOT Act in connection with that investigation.

Chairman ROBERTS. So if somebody makes a mistake on a fingerprint, that isn't the fault of the PATRIOT Act?

Attorney General GONZALES. That was not the fault of the PATRIOT Act, that's correct, sir.

Chairman ROBERTS. Senator Rockefeller.

Vice Chairman ROCKEFELLER. Thank you, Mr. Chairman.

In section 206—I address this to both of you in that you gave joint testimony—section 206 of the PATRIOT Act authorizes roving wiretaps under the Foreign Intelligence Surveillance Act. As it has been explained to us, the SAFE Act would retain roving wiretaps, allowing surveillance where the target, for example, uses multiple cell phones in order to evade detection. And the SAFE Act would retain John Doe wiretaps where the target cannot be named. But the SAFE Act would eliminate the combination of the two—John Doe, roving wiretaps—where neither the location of the surveillance nor the identity of the target is known.

So my question is, what would be the impact of this provision on the activities of the Bureau? And second, would the elimination of the John Doe roving wiretaps increase the protection of innocent Americans from unnecessary surveillance? And third, what protection against unnecessary surveillance exists in the statute as written?

Attorney General GONZALES. Senator, let me begin by emphasizing that we have to go before a Federal judge in order to get a search warrant under 206. There has to be probable cause that the target is in fact a foreign power or an agent of a foreign power. In addition, 206 does include extensive minimization procedures so that we do ensure that steps are taken to protect the rights of innocent Americans.

I believe that under 206 we have to go to a Federal judge and provide sufficient information to identify a specific target. There may be instances where we don't know the exact identity of someone we believe is a terrorist. Nonetheless, we have to provide sufficient information for the judge to identify that person. If we discover later on that we've made a mistake, that in fact we should be conducting surveillance on Person B as opposed to Person A because we were wrong in our identification, we'd have to go back to a Federal judge and get a new court order.

Additionally, I'd like to add that we also have to have probable cause that the facility that we want to target or place that we want to target, that the terrorist is either using or about to use. And so we believe that 206 contains an abundant number of safeguards to ensure that we've got a limited search under the supervision of a Federal judge and that there are adequate safeguards to protect the privacy interests of Americans.

Director MUELLER. The recommended change does not make much sense to me. As was pointed out by the Attorney General, if we have an individual whom we accurately can describe, to differentiate that individual from everybody else, and the person is an individual which would satisfy the requisite specificity so that a judge can issue the order allowing us to intercept his conversations, and the person is roving—in other words, utilizing a number of cell phones over a period of days—what this statute would mean is that we would have to go back when we identify another device that he's using and get another court order.

If we satisfy the prerequisites of 206 as it is written now, in my mind that is certainly an adequate safeguard to protect the innocent. Again, I'd emphasize, it goes before a judge; you have to be

specific in terms of the individual, and you have to be specific in terms of the usage of that individual of various devices. And persuading a judge that you have probable cause to satisfy those prerequisites in my mind satisfies the need to protect the innocent.

Vice Chairman ROCKEFELLER. OK. I'll save my next questions for the next round.

Thank you very much.

Chairman ROBERTS. Senator Levin.

OPENING STATEMENT OF HON. CARL LEVIN

Senator LEVIN. Thank you, Mr. Chairman. Let me add my welcome to all three of you and my thanks for your service.

The morning paper tells us that the State Department has decided to drop from its annual report the number of serious international terrorist incidents that occurred during the previous year. It's a very disturbing report to us.

This law requiring an annual report on terrorist incidents has been on the books for a long time, long before 9/11. But suddenly we read the State Department has decided they're no longer going to tell the American people what the numbers of those incidents were in the previous year; they're going to drop that information.

I'm wondering whether—and I'll ask each of you—whether or not you were consulted by the State Department prior to this important information being dropped, or at least the decision being made by them to drop it and to suppress information which is really significant in many people's eyes to understanding whether or not we are making progress.

So General, let me start with you. Were you consulted by the State Department on that issue?

Attorney General GONZALES. Senator, I was not personally consulted; whether or not the department was consulted, I'd have to find out. But I was not personally consulted.

Senator LEVIN. Fair enough.

Director Mueller.

Director MUELLER. I was not. I was not involved in the issue. But I'm not certain I would agree with the predicate of the question.

Senator LEVIN. I understand.

Director Goss.

Director GOSS. I believe my role was pretty much limited to making sure that whatever the NCTC had was made available to the State Department.

Senator LEVIN. Thank you.

Let me first thank you, General Gonzales, for your strong statement of support for oversight by Congress, calling it a constitutional responsibility. You disagree on whether or not sunset was needed. But nonetheless, in terms of the importance of oversight, you made a very ringing endorsement of that and we appreciate that.

And Director Mueller, let me thank you for your endorsement of the role of the courts.

Both of those endorsements are significant. We appreciate them.

On section 206, let me ask you, Mr. Attorney General, about the roving wiretaps issue. I understand that, under existing criminal law, in addition to identifying the target and the location so that

a court is satisfied to grant a roving wiretap, before the wiretap is triggered that there must be an authentication that the person involved in the conversation is the subject of the authorized wiretap, but that that requirement of authentication is not present in the Act that we're reviewing. Is that accurate?

Attorney General GONZALES. If I understand your question as to whether or not there is an ascertainment requirement in the criminal context, my understanding, Senator, is that the ascertainment requirement in the criminal context only applies or only is there with respect to oral communications, like bugging. It does not exist in a criminal context in connection with electronic surveillance. And so I think that in that respect 206 would be consistent with the current requirements in the criminal context.

Senator LEVIN. In terms of bugging, is it consistent?

Attorney General GONZALES. I do not—it's my understanding that with respect to oral communications there is an ascertainment requirement in the criminal code.

Senator LEVIN. What about in the PATRIOT Act?

Attorney General GONZALES. There is no ascertainment requirement per se. But again, let me emphasize that we do have to show probable cause as to two very important facts—No. 1, that the target is a foreign power or agent of a foreign power, and No. 2, probable cause that the facility or place which you're targeting, that the target is in fact using or about to use that facility.

Senator LEVIN. No, I got that. But why should there not be the same ascertainment requirement in the PATRIOT Act that there is in criminal law, just the way there is for electronic communications?

Attorney General GONZALES. I don't believe that there is such a similar requirement.

Senator LEVIN. Should there not be?

Attorney General GONZALES. I don't know if I can answer that question, Senator.

Senator LEVIN. Let me ask Director Mueller.

Is there any reason why we shouldn't have that same ascertainment to protect privacy of American citizens to make sure that in fact the ascertainment occurs, to make sure that it's not somebody who should not be the subject who in fact is being bugged?

Director MUELLER. I would have to go and check the statute more clearly, more carefully on that particular proviso and look at the import.

I will say generally, though, that the FISA statute relates to finding probable cause that we're dealing with a foreign power and we're dealing and looking at and undertaking investigative techniques of a foreign power or an agent of a foreign power. And that, in my mind, is a different set of concerns than one would have when we are investigating individuals for their possible breaking of the criminal laws.

There are a number of areas that are different because of the different subjects we're looking at under the FISA statute than those subjects we're looking at under Title III of the criminal statutes.

Senator LEVIN. My time's up. So why don't you just expand for the record, after reviewing the law, as to whether we should not

have that same ascertainment requirement for the bugging as we do in criminal law when it comes to the PATRIOT Act?

Thank you.

Chairman ROBERTS. Senator Wyden. Let's try Senator Mikulski.

OPENING STATEMENT OF HON. BARBARA A. MIKULSKI

Senator MIKULSKI. Thank you very much, Mr. Chairman, and good morning to our panelists.

I think we all remember what it was like in October 2001 after America had been attacked and we knew that 19—or maybe even more—people had come into our own country and had planned the most despicable and dastardly deeds against us. And out of that came the PATRIOT Act, because we knew we needed to get more information and that we had old rules based on old thinking about old technology.

So out of this came the PATRIOT Act, but yet the great idea of sunset, because I think we were all concerned that in our zeal to protect the country we would not be overzealous and then create a set of rules we either found dysfunctional or not in keeping with our Constitution. So I think this is why this debate is important now.

Let me get to my questions.

There are a lot of concerns, as you know, among the American people about jealously guarding their right of privacy. There's a built-in tension between the right of privacy and our national security. This is what we're trying to resolve—how to protect both.

One of the questions that people have when they talk to me is they think anybody in the Federal Government, under the PATRIOT Act, can now spy on them. So I'm going to ask a series of questions, and perhaps, Mr. Gonzales, you can answer this.

No. 1: What agencies within the Federal Government can,"spy" or place American citizens under surveillance—Federal agencies?

Attorney General GONZALES. I mean, the FBI. The Department of Justice is the agency that has——

Senator MIKULSKI. So can the CIA spy on the American people?

Attorney General GONZALES. The primary responsibility falls upon the Department of Justice, not the CIA.

Senator MIKULSKI. Can the CIA spy on the American—I'll get to another question about the so-called wall.

Attorney General GONZALES. No.

Senator MIKULSKI. Can the National Security Agency, the great electronic snooper, spy on the American people?

Attorney General GONZALES. There are limits upon the NSA in terms of what they can do in spying upon the American people.

Let me just emphasize one additional thing, Senator. Even with respect to the authorities that are granted, many of the authorities——

Senator MIKULSKI. These are not hostile questions.

Attorney General GONZALES. No. And I understand——

Senator MIKULSKI. These are clarifying. Clarify after I ask my next question.

Then let's go to the wall that Mr. Goss talked about in his written statement. That was the whole issue. And then it goes into the information sharing that Director Mueller talked about.

Everybody's working together; let's say it's in the Counterterrorism Center. The NSA picks up something—say a foreign agent.

They're a person of interest, even a person of suspicion. They're coming into the United States. They're mingling with people who are already in the United States. They're communicating. NSA has picked all of this up. They're following these people with their computer, their cell phone, whatever techno stuff they have.

Then when they're there, do they stop and hand it over to the FBI, and the FBI keeps on doing it? Or do they keep on following these persons of interest or suspicion? And what are they allowed to do under the law?

Attorney General GONZALES. Well, they are always——

Senator MIKULSKI. And clarify anything you want. But see, these are the questions, which is, who does what, when?

Attorney General GONZALES. There are minimization requirements under law on Federal agencies that engage in surveillance to ensure that the privacy interests of all Americans are protected. In addition to requirements under the statute, there are additional guidelines within the Department of Justice to ensure that the privacy interests of Americans are protected.

Senator MIKULSKI. Well, Mr. Mueller, how would this work from a practical standpoint? Do you see what I'm getting at? Because people really worry that everybody can spy on them—the DOD, et cetera—and that they can come in carte blanche.

Director MUELLER. Surveillance of American citizens for national security matters is in the hands generally of the FBI. The investigation or development of intelligence overseas is in the hands of the CIA and NSA. And I would say generally they are not allowed to spy or to gather information on American citizens, but there are limited exceptions to that. Depending on the type of investigation, there would be, thanks to the PATRIOT Act and additional rulings of the FISA court, we would now have the ability to share the information that may have been, pursuant to its authorities, obtained by the NSA, maybe overseas, maybe between somebody overseas and somebody in the United States, or obtained by the CIA overseas, and now be able to use it in the United States.

Senator MIKULSKI. Did you need the PATRIOT Act to be able to do that?

Director MUELLER. The PATRIOT Act and changes to the FISA statute—not changes to the FISA statute, but a reinterpretation of the FISA statute by the FISA appellate court in order to do that, yes.

Senator MIKULSKI. And had those changes not occurred, would you or your agents have felt shackled in some way or discouraged from pursuing certain things?

Director MUELLER. Absolutely. I think if you look at the—go back and read the report of the 9/11 commission, it was well pointed out there the constraints under which we were operating prior to September 11 that stymied, cutoff the flow of information between the agencies whose responsibility is protecting the security within the United States and those agencies whose responsibility of protecting the security of the United States outside the United States. And the PATRIOT Act and the interpretation of the FISA statute has broken down that wall.

Senator MIKULSKI. Mr. Gonzales, you wanted to clarify, and then I have another question I just want to put in, which is, has the PATRIOT Act had any constitutional challenges directed at it through the court system? And have any parts of the PATRIOT Act been struck down as unconstitutional?

Attorney General GONZALES. The only clarification I wanted to make, Senator, was to repeat one thing that Director Mueller said in his opening statement. And that is, of course, that many of the authorities exercised by the Federal Government in the area of surveillance are done oftentimes under the supervision of a Federal judge, and also that there are strong minimization requirements imposed by statute and by regulation to protect the privacy interests of Americans.

There have been numerous challenges to the PATRIOT Act, and to my knowledge they have all withstood challenge—successful challenges in the courts.

Senator MIKULSKI. Mr. Chairman, I think I'll wait for my next round of questions to go to another set. Thank you.

Chairman ROBERTS. The questions you had were follow-on questions, which is why the Chairman thought it would be perhaps a good thing to let you get to the end of that chain of questions in regards to the understandability of the answers and the questions. But we will have a second round.

Senator MIKULSKI. Well, and, Mr. Chairman, I think some of those questions, knowing the colleagues before us, have to almost go into a closed session to get more detail and get more of the mechanics of how it works and so on that, again, we have privacy concerns here.

But I appreciate the answers.

Chairman ROBERTS. Senator Snowe will be now recognized.

Let me point out the Committee did hold a closed hearing on the use by the intelligence community field operatives in regard to the tools provided by the PATRIOT Act. These same questions were brought up at that particular time, and their responses were very helpful in regards to the questions that the Senator has asked.

Senator Snowe.

OPENING STATEMENT OF HON. OLYMPIA S. SNOWE

Senator SNOWE. Thank you, Mr. Chairman. And I thank all of you for being here today.

I think one of the fundamental issues surrounding the PATRIOT Act as we consider its reauthorization is a lack of public reporting with respect to the way in which it's applied. And I'd really like to hear from all of you, given your perspectives and the different positions that you represent, as to how we could do a better job, how you could do a better job in informing the public in which instances the PATRIOT Act is applied because I think so often now what I hear from my constituents is a concern that it's used for domestic investigations, that there is excessive secrecy with respect to how it's used.

And I think we need to have more public disclosure in examining and assessing its impact. I think it would enhance the public's confidence in the way in which this additional and broader authority is being used.

So could you give us some ideas as to how we could improve upon the public reporting dimensions without compromising, obviously, valuable investigations concerning terrorists and terrorism?

Mr. Gonzales, proceed.

Attorney General GONZALES. Well, I agree with you. I think that we have a responsibility to not only use these tools wisely, but to reassure the American people that we're using these tools wisely, and to provide as much information as we can without compromising our ability to effectively deal with this threat, to do the best we can to provide information not only to the Congress but to the American people.

In the past few weeks we have tried to be more open about providing additional numbers about how many times these authorities have been used. As you know, some of these provisions do impose reporting requirements upon the Executive branch as to how these authorities are being used.

I must tell you, Senator, based on my very short stint at the Department of Justice, there are a lot of folks at the department who spend a great deal of time gathering up information to provide to Congress. And I understand that sometimes it takes a little longer than some Senators like. We want to be very careful. We want to be very accurate in providing good information to the Congress.

And so there already is a lot of information that's being provided to the Congress. We provide reports twice a year regarding the use of FISA, and I'm beginning to learn that sometimes some Members of Congress don't take advantage of the opportunity to review that report, and they don't understand what information is already being provided to the Congress.

So we're always happy to see what we can do more, but I would just emphasize that I think there is a lot of information that is currently being shared about how these authorities are being used.

Senator SNOWE. You don't think we should do anything further than those additional reports? I mean, I think you provide them biannually.

Attorney General GONZALES. Senator, I'm happy to sit down with you and your staff and consider additional ways that we could better educate the Congress and the American people. I'm happy to do that.

I just want to—I don't need to remind you, but there is in my judgment a lot of information that is currently being provided already by the Executive branch.

Senator SNOWE. Well, somehow I think that we really have to do a better job in conveying that to the American people so that it doesn't undermine the integrity of the process and how it's being applied, I think, in the final analysis, and its impact. I mean, we understand to what extent you—you know, obviously, certain activities have to remain secret. We understand that. But on the other hand, I think we have to go the extra mile whenever we can to convey to the public that this is being used in the most appropriate way and we're not encroaching on people's civil liberties.

Attorney General GONZALES. I couldn't agree more, Senator.

Senator SNOWE. Mr. Mueller.

Director MUELLER. Following up on what the Attorney General said, the information that's been provided I think should be helpful

in allaying some of the concerns, particularly of individual groups, about the abuse of the PATRIOT Act. For instance, the fact that we have not used the PATRIOT Act 215 to obtain records from a library should allay some of the concerns.

We have provided a great deal of information to Congress. I have here a letter of October 24, 2003, to the Honorable Ted Stevens, as chairman of the Committee on Appropriations. In it, it lists something like 15 instances where we've utilized the delayed notification in various of our cases, indicating how important that particular provision is and how it has not been abused.

Part of the problem that we have is the fact that to disclose our successes, we have to do it in closed session. The closed session I believe you had a couple of weeks ago, I believe was informative in showing you exactly how we're using those provisions, but to disclose much of that material would educate the terrorists, would educate those whom we're investigating. But my hope is that through hearings such as this, continued scrutiny from Congress, that much of the concern will be allayed.

Director GOSS. Senator, I have a great deal of empathy for your question because I have participated from the situation you find yourself in as responsible to a constituency. And I think it's very important that we reassure the constituency that we have safeguards in place in our government.

I certainly think that the Oversight Committee role is very, very important in that. And I think, therefore, a frequent, very candid exchange on matters of concern needs to be undertaken just to make sure that we do assuage those concerns that might be out there, so that people who are respected in their communities can get up and say, I've examined this, I'm on top of this, and I can understand your concerns, but I think everything is working OK and, on balance, in fact, this is helping us catch terrorists or prevent terrorist acts from happening.

I think that is the system that we have embraced in our form of representative government for dealing with these kinds of problems, and it's one that I think does work pretty darn well, but I certainly am aware of the balance problem.

I know right now that there are people who have terrorist concerns, terrorist thoughts, may be associated with terrorists, actually people maybe in terrorist organizations, who are probably watching this discussion. I am very concerned that we understand that in the audience these days, because of technology, we have not only the people we're trying to reassure and we want to go out there and tell them how wisely we're employing these tools, it would be not helpful to tell the terrorists that.

There is a huge amount of denial and deception and cleverness going on in the terrorist community, as loosely as it is organized. But it is good. They are smart, clever people. They take benign things like aircraft that we use to fly around for our commerce and our comfort in this country and they turn them into weapons of doom and tragedy. They can do that with other simple things that we count on every day, like going to the store and buying aspirin or things like that. It doesn't take much imagination.

So I am very concerned that we draw a line with all the American people to understand we may have to be looking into things

from time to time that terrorists are trying to take advantage of and use against us, things that we consider benign in our daily life. And those explanations have to be credible and they have to be accurate. And we need all the partners in our great enterprise to do that, both legislative, executive, and I would add the media would help too, if we could have accuracy in what's actually going on.

I do think we have the things in place. The last thing any of us want in the intelligence community—and again, we are overseas, so I speak from that point of view—is a feeding frenzy over a poster child because we abused the authority. This authority is too important. We don't want to lose it. We are very careful not to abuse it.

Senator SNOWE. Thank you. Thank you, Mr. Chairman. Thank you all.

Chairman ROBERTS. Senator Rockefeller. I'm sorry, Senator Wyden is next, and he has returned.

OPENING STATEMENT OF HON. RON WYDEN

Senator WYDEN. Thank you very much, Mr. Chairman, and thank all of you for your cooperation.

I want to begin with you, Director Mueller, and also express my thanks to you. You've always been responsive whenever I've called and whenever I've had concerns, and I'm very appreciative of that.

I want to start with the library provision of the PATRIOT Act and the debate about 215. You all constantly say there has never been a case where you forced a library to turn over records. I've heard that again and again and again. But my understanding is that you get cooperation from libraries by using what you call—these are your words, not mine—a "discreet inquiry" by a member of the Bureau. And I'd like to know, No. 1, what a discreet inquiry of a library is and, No. 2, how many of them have there been since the PATRIOT Act? Because I constantly hear from my libraries, you know, about this.

I think Porter Goss is absolutely right. We need to strike a balance here. We ought to be fighting terrorism ferociously without gutting civil liberties. And I really want to get on top of this library issue. So tell me what you mean when you say you get cooperation from libraries through discreet inquiries.

Director MUELLER. Let me start off by saying that I have not, I don't believe, ever said that we have never forced libraries to give records. We have never used 215 as a vehicle to get records from libraries. In the past, in criminal investigations we have used grand jury subpoenas. So I want to make certain that we're clear that I was talking about 215 we have not used to ask libraries to provide records to us.

In terms of discreet inquiries, and I'm not certain of the context in which I may have——

Senator WYDEN. You said it to the Judiciary Committee.

Director MUELLER [continuing]. Said that. But I think what was in my mind is we've had a couple of occasions at least in which we have been contacted by persons who believe that they have information that needs to come in the hands of the FBI, and these are librarians. And in colloquy with these individuals, they've decided to provide us records. Now, it may have been with some paper. But

when I'm talking about discreet inquiries, it has been triggered—in my mind it's been triggered on those occasions by librarians themselves that have come forward to us and said this is something you ought to look into.

Senator WYDEN. So, since the PATRIOT Act was enacted, there has not been an increase in discreet inquiries that the department has initiated with libraries?

Director MUELLER. Not to my knowledge, no.

Senator WYDEN. All right. Would you——

Director MUELLER. Now let me just make one——

Senator WYDEN. Would you check on that and give me the numbers with respect to times when the department initiated what you all call this discreet inquiry?

Director MUELLER. Well, I wouldn't put a tag on discreet inquiries. I may have used the word "discreet inquiries" to describe what I believe were two situations in which librarians had come to us and we had a colloquy with the librarians. It never got to the point of 215s because the librarians believed we needed the information.

I would be happy to try to go back and look at the number of occasions where we have utilized—we have not used 215—the number of occasions that we have utilized process on libraries. But it would be very difficult for me to go back and say, "OK, when has one of our agents talked to a librarian?"

Senator WYDEN. I understand. I think you get my point as well. These librarians are very fearful. They're patriotic Americans. They want to assist their government and at the same time, like the rest of us, they're concerned about fishing expeditions. And I want to make sure I understand what these issues are all about. And why don't we say I intend to go into this more in the closed session as well to make sure I'm on top of that.

Director MUELLER. Can I make one last point in this regard?

Senator WYDEN. Of course.

Director MUELLER. I am quite certain that had we engaged in fishing expeditions with libraries that it would have come—attention would have been brought to that fishing expedition by either the librarian society or the ACLU. And we have not had brought to our attention an abuse of our role in interacting with libraries.

Senator WYDEN. Director, what I'm concerned about is that it may not be getting to that point because essentially people show up from the Bureau, ask these kinds of questions, and these librarians say, "Look, we don't want to be seen as disloyal; we're just going to cooperate." I want to know more about this. I'm not making any allegations here. All I know is I saw you say the words "discreet inquiry," and I'm hearing from these librarians. I want to get on top of this.

Question for you, if I might ask, General Gonzales. You said that there had not been an instance where a court has found any abuses under the PATRIOT Act. Are you aware of *Doe* v. *Ashcroft*? That was the case where the Federal judge struck down the authority for National Security Letters for customer records of communication service providers which had been expanded by the PATRIOT Act.

Now the court held that the government had failed to provide any explicit right for a recipient to challenge the letter, a search

order, and that violated the Fourth Amendment, and that the automatic secrecy rule violated the First Amendment, and the department has appealed the decision to the 2nd Circuit. Are you aware of that, or——

Attorney General GONZALES. I am generally aware of that case. You are correct; the courts had indicated that there were problems under the First and Fourth Amendment, even though the Department of Justice conceded that this request by the government could be disclosed and could in fact be challenged in the courts. Nonetheless, the court chose to disregard our concession and issue its ruling.

My understanding of that case, Senator, is that the court specifically, though, focused on a provision that predated the PATRIOT Act, and that was the provision that was in fact struck down. And it did not reflect a decision by a Federal judge to strike down a particular provision created by the PATRIOT Act. But I will confirm that and get back to you.

Senator WYDEN. Why not require a judge to approve these National Security Letters? I mean, that could be done electronically, it could be done quickly. My concern about these National Security Letters is that there would be a way to strike the balance that Porter Goss has talked about, a view that I share, relatively simply—that, you know, you could have judges approve the National Security Letters electronically and quickly. I'm concerned that a lot of these recipients aren't given notice of their right to challenge search orders. And it would seem to me that this would be something consistent with this balance that we've been talking about that we could do.

Do you have any concern about what I've just described?

Attorney General GONZALES. My understanding, Senator, with respect to the use of National Security Letters, I mean, one of the benefits of it is speed. There may be instances where you need to get them so quickly that you might lose valuable information if, in fact, you have to track down a Federal judge.

I would also emphasize that the use of National Security Letters is limited to certain types of entities that you can gather information from, and it's limited as to certain types of information you can try to get under National Security Letters.

Senator WYDEN. Well, again, what is hard for us to address here is that we're to some extent doing oversight in the dark. We are trying to figure out how to strike this balance. Director Mueller and I are going to talk a bit more in closed session about the library provisions.

The Department of Justice is required to report to this Committee on the use of National Security Letters by the FBI. We haven't gotten the report for 2004. We haven't gotten it. So that makes it hard for us to do oversight, which is why Members of this Committee show up and ask these questions.

So I hope that all of you will work with us on this because in an area like this, National Security Letter, I sort of operate under the Ronald Reagan theory, "trust but verify." And what I do know is that we haven't gotten the report that was supposed to be filed on these National Security Letters, so we come here and ask these questions.

And if we have a second round, Mr. Chairman, I'll ask some more. Thank you.

Chairman ROBERTS. Senator Rockefeller.

Vice Chairman ROCKEFELLER. Thank you, Mr. Chairman.

This is a specific question about FISA orders for business records, "any tangible things." In 215 in the PATRIOT Act it authorizes FISA orders issued by the FISA court for "any tangible things" from any entity. Under section 215 the government only needs to make, with respect to terrorism investigations, a showing that the records in question are for "an authorized international terrorism investigation." In your joint statement you indicated that the department would support an amendment that requires that the records be "relevant" to a national security investigation.

Section 215 also provides that no person shall disclose to any other person that the FBI has sought or obtained records except for persons necessary to producing, obviously, the records. In your statement you indicated that the department would support an amendment that the recipient of a section 215 order may consult with an attorney and may challenge the order in court. The questions I have are twofold.

Would you support limiting the scope of section 215 to those records for which there was at least some specific information for believing that the records related to a suspected terrorist or other agent of a foreign power, No. 1, yes/no?

Secondly, your statement indicates that you support modification of section 215 to give the recipient of the FISA order the right to consult an attorney and to challenge the order in court. Do you support the provisions of the SAFE Act that would require the government to show why nondisclosure is necessary and place a time limit on a nondisclosure requirement? Why or why not?

Attorney General GONZALES. I think that the "relevant" standard is the appropriate standard with respect to 215 business order requests. We have indicated that we believe that it is a relevant standard. The words are not used in the statute, but we believe it is implicit. But nonetheless, we would support making it clear that the appropriate standard is a relevance standard.

I think to go above that to require a higher standard would make the use of 215 sort of a dead letter. I don't think investigators would use 215.

We look at 215 orders as a search for—not a search, but a request for information, much like a grand jury subpoena, where the standard there is also relevance. It's part of the building block of the case in order to get information to see whether or not there is sufficient information to develop probable cause that would support a search. And my own judgment is that if the standard were changed, that 215 would no longer continue to be useful.

And I'm sorry, sir, I don't remember the second part of your question.

Vice Chairman ROCKEFELLER. That was the SAFE Act would require government to show why nondisclosure is necessary and place a time limit on nondisclosure requirements.

Attorney General GONZALES. Well, I think in this case we'd be talking about information that is classified. And it just sort of turns the presumption on its head that classified information—the

presumption is is that it would become public unless you showed certain things. I mean, it is classified information, and I think there's a reason it is classified information and should remain classified information.

Vice Chairman ROCKEFELLER. Well, then help me understand. You would say, then, that a nondisclosure requirement is not desirable?

Attorney General GONZALES. I would not support it. I mean, I think we all understand that these investigations involve very sensitive matters. Talking about in the FISA context, this is the most sensitive information. And to disclose information to a target or someone who's not a target of an investigation but someone who then shares the information unknowingly to the target may jeopardize a very important, serious investigation. And so we would have concerns about such a requirement.

Vice Chairman ROCKEFELLER. OK. One more. This is on "significant purpose," about those requirements.

Section 218 of the PATRIOT Act amended the certification requirement of FISA such that the collection of foreign intelligence must be "a significant purpose" of the surveillance or the search. Prior to the PATRIOT Act, the certification requirement had to be interpreted to require that foreign intelligence collection be, quote, "the primary purpose" of a surveillance or search. Section 218 has been credited with "helping to bring down the wall separating intelligence agencies from law enforcement agencies."

Other provisions of the PATRIOT Act such as section 203 allow information to flow from law enforcement officials to national security officials and to members of the intelligence community, as we know.

The question is, in terms of protecting the United States from another attack, what difference have these information-sharing acts made, in your judgment? Second, can you describe the relative use and importance of, first, a provision allowing the sharing of criminal investigative information with intelligence officials, the importance of that, and second, in the other direction, provisions allowing the sharing of intelligence information with law enforcement agencies at a lower level?

Attorney General GONZALES. Well, I think it is probably one of the most important aspects of the PATRIOT Act, provisions like sections 218 and 203, which have made it clear for law enforcement and the intelligence community that it is OK to share information. And, as the 9/11 commission and the WMD commission, the reports from those commissions, both indicated, part of the reasons for the attack on September 11 and the problems we've had is the fact that the government has been unwilling because of a perception that they're unable to share information. And section 218 and other provisions like 203 have made it clear that it's OK to share information.

So, it's very, very important. I think sharing of information, to be successful in that, is so important in winning the war on terror.

Vice Chairman ROCKEFELLER. General, I'm in agreement with that, but the question was, has it made a difference?

Attorney General GONZALES. It has made a difference. Yes, sir.

Director MUELLER. If I could speak to that just for a second, it has made a tremendous difference in our ability to conduct what has been called by the 9/11 commission "transnational intelligence investigations." Terrorists operate, as we saw on September 11—they developed their plans in Afghanistan; they habituate Hamburg, Germany; and launched their plans in the United States.

We've had a number of occasions since September 11 in which we have discovered information in the course of criminal proceedings here that has been passed on to the CIA and enabled the CIA to wrap up persons overseas with the help of their counterparts. That would not be possible without the provisions of the PATRIOT Act.

We had convicted yesterday, in Northern Virginia, an individual by name of Tamimi, who in the wake of September 11 had encouraged a number of individuals to go to Pakistan to obtain training in order to fight against the troops in Afghanistan. He was convicted as a result of the ability to share information that may have come from the intelligence side of the house but can be used in the criminal side of the house.

Last year, in the spring of last year, I believe it was, there was an individual by the name of al-Hindi, who was arrested by the British authorities. He is the individual who had undertaken surveillance of The Prudential and a number of financial institutions in the United States. If we had not been able to look at some of his co-conspirators, both criminally as well as from the intelligence perspective, we would not have been successful in obtaining the plea of a principal member here in the United States, nor would we have been half as successful in coordinating and cooperating with our counterparts overseas in terms of exchanging information with them that enabled them to wrap up and prosecute al-Hindi.

One can talk about the successes due to breaking down the walls for a good several hours. I'm sure you heard in the closed session last week a number of instances where breaking down the wall by the PATRIOT Act and the rulings of the FISA court has made a tremendous difference in our ability to protect the American public.

Vice Chairman ROCKEFELLER. I happen to agree with that, and I think it's important that the public hear that clearly.

Chairman ROBERTS. Senator Levin.

Senator LEVIN. Thank you, Mr. Chairman.

Director Goss, I welcome—I think all of us do—your strong support for congressional oversight which you have made in your testimony. I think we've fallen short in Congress of carrying out those responsibilities and I very much welcome your statement of support.

And, more importantly, I welcome your following through with documents which you have supplied to me, which I have been waiting for from the former CIA Director for a year. You came to office, said you would be cooperative. You have come through, followed through with the actual documents I've been waiting for. I can only say I wish the Department of Defense were as forthcoming with documents as you have been, but I don't expect you to comment on that.

[Laughter.]

Senator LEVIN. Thank you.

The money-laundering provisions in the PATRIOT Act. Title III contains provisions that Congress enacted to strengthen our laws against money laundering and terrorist financing. They're not subject to sunset, but nonetheless we should be reviewing these provisions, whether they're sunsetted or not, as you said, General. I agree with that.

Have they been useful to you, the anti-money laundering provisions in the PATRIOT Act?

Attorney General GONZALES. I'm told that they've been very useful to the department. I don't have specific examples. Perhaps Direct Mueller does. But money laundering and those kinds of schemes to finance terrorist activities is so very important in our ability to deal with this threat. Without financing, it's very difficult for terrorists to attack this country. But, to respond, yes, it's been very important.

Senator LEVIN. And, Director Mueller, have the provisions of the PATRIOT Act relative to anti-money laundering in general been useful to you, without getting into too many specifics because of the time limit on our questions?

Director MUELLER. Yes. Let me just mention a couple of provisions that were incorporated in the PATRIOT Act that were tremendously important.

Money transmitting businesses, which have become a mechanism for exchanging funds around the world, the PATRIOT Act gave us provisions helping us to address those. The provisions relating to treasuries, the rules and regulations with regard to banks, so that banks, not only in the United States but around the world, adopt "know-your-customer" rules are tremendously important.

So just to mention two of those provisions, I'm sure we have other examples from Treasury in which the ability to forfeit funds in interbank accounts has been useful, but I'd have to get you details on that.

Senator LEVIN. That's fine. That's very helpful, thank you.

General, section 214 is the subject of the next question. You've made reference to the fact that there's got to be a certification of the information that you seek authority to obtain being relevant to an ongoing investigation. And my question is, do you think it is appropriate in that request for that judicial authority that the way in which the information is expected to be relevant should be set forth?

Attorney General GONZALES. Senator, I'm not sure I understand your question.

Senator LEVIN. Well, you said that there's a requirement in section 214 that when agencies install pen registers, tap and trace devices through FISA procedures, that there's a requirement that you allege, you certify, that what you are seeking authority to do is relevant to an ongoing counterterrorism or counterespionage investigation.

My question to you is, do you think it would unreasonable to require that you state in that request how it is relevant to your investigation—not just the conclusion that it is relevant, but how it is relevant. If you could just give me a yes or no, or expand for the record, I'd appreciate it.

Attorney General GONZALES. Senator, it's hard for me to plead ignorance, but it may be the fact that we do have to explain how it's done. I don't know that.

Senator LEVIN. If not, I would hope you would consider supporting an amendment to the statute which would require that you state how it's relevant, if it's not already required. Could you give us that for the record?

Attorney General GONZALES. I will look at that.

Senator LEVIN. Now, in section 215, we've got a situation where the application—this is on the records we've been talking about, including library records—the application to the court goes, as I understand it, to the institution, the business, or whatever. Is that correct?

Attorney General GONZALES. No, it's the order. The application goes to the court and then an order is issued, and then we seek the records pursuant to that order.

Senator LEVIN. To an institution or an entity?

Attorney General GONZALES. The entity holding the record that is being pursued.

Senator LEVIN. My question is, do you think it's reasonable that when the entity is ordered to provide records, that the specific target of the investigation be the subject of the records being sought rather than a general "we want all your records" relating to some subject? Is there any reason why the law should not require you, if you're not already required, to identify whose records it is that you seek and that it is not an American's record, and that the records are not connected to First Amendment rights?

Attorney General GONZALES. Well, there is, of course, a requirement under 215 that the information sought is relevant to an intelligence investigation.

Senator LEVIN. Right.

Attorney General GONZALES. I worry about the additional requirement that you have suggested. I'd have to look at it, but I'd worry about going beyond what's already within 215.

Senator LEVIN. All right.

Director MUELLER. Can I add something on that? I would be opposed to that.

Senator LEVIN. All right.

Director MUELLER. I think the court should review the application. The court issues the order. If it's overly broad, the court can make a finding and require additional information. There will be occasions where to, as you say, specify in the order the individual who is the target of the investigation where that would be akin to alerting the person and risking the investigation as a whole.

Senator LEVIN. How would that be alerting the person?

Director MUELLER. Well, if it goes to an institution, the institution can well turn around and alert the person if they know a particular target. There may be circumstances where we look for discreet groups of records. In those records may be records we want on a particular target or targets. And I believe we ought to have the ability and capability to present to the judge the circumstances where we want a broader order for those records from a particular institution.

Senator LEVIN. Thank you. Thank you, Mr. Chairman.

Chairman ROBERTS. Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman.

I want to follow up on an area that Senator Levin was touching on and see if I can go at it a different way, and I'll do this with you, Director Mueller.

The PATRIOT Act, of course, eliminated, with respect to the National Security Letters and the FISA warrants, the requirement that you meet what was called the specific articulable fact test. And what was put in place was a requirement that when you want records, it has to be relevant to an open investigation. That's, I think, where we are in terms of the law.

What I am interested in knowing is, what is necessary at this point, Director Mueller, to initiate an investigation within the FBI?

Director MUELLER. Well, it can be an allegation. It could be information provided to us by another agency, and we will generally open what's called a preliminary investigation. And the preliminary investigation enables us to do some limited work in terms of verifying the information, following up on the information before we can go to a full investigation. And the full investigation enables us to use a variety of additional tools.

So it is a staged development of information where we have to make a showing in our files of what is warranting the use of additional investigative techniques. It is based on predication. In other words, the initial predication for opening an investigation can come anywhere from an e-mail from an anonymous source saying that somebody's going to commit an attack in New York tomorrow, and then we'll do whatever is necessary to either corroborate that information or disprove that information.

Senator WYDEN. Is it fair to say then, Director, that this staged development of information, as you describe it, is in fact the new standard of proof for issuing a FISA warrant and a National Security Letter?

Director MUELLER. No.

Senator WYDEN. All right, then tell me why not, because you just said that to initiate an investigation within the FBI, you can do it, essentially, with an allegation. Then you said that there is this—I guess you call it the process of proof, sort of a ladder kind of arrangement. And that, based on an absence of any other information, strikes me as something pretty close to the new standard of proof, and I'm just trying to find out what the standard of proof is.

Director MUELLER. It's not a standard of proof. The evaluation of information has a number of purposes. One is, is it worth opening a file? Is it worth documenting the allegation that's come in? We have a number of allegations that come in we don't open a case on because it may be an anonymous e-mail message that comes in to our website. But for our practical purposes in terms of what we need to do to further the investigation, we are limited at the preliminary stage to documenting and furthering——

Senator WYDEN. But what is the standard of proof, then?

Director MUELLER. There is no particular standard of proof. We don't have to prove to anybody. It's not probable cause. It's is there information that leads us to believe—if you want to say, leads us to believe—that further investigation is warranted in a particular case?

Senator WYDEN. I think that's a pretty sweeping comment that there really isn't any standard of proof, that there isn't any, to your terminology, no particular standard of proof.

And I'm going to want to follow up with you on this, Director, because I think we used to have one. It was, you know, the specific, articulable fact requirement. Then we said that it's got to be relevant to an open investigation. Then you told me you can do an investigation on the basis of an allegation. I'd like now to know what the standard of proof is for these warrants and National Security Letters, and you said there really isn't any particular standard.

Director MUELLER. Well, there's a standard for issuance of a grand jury subpoena, for instance: it's relevance. There's a standard for issuance of a National Security Letter. In order to get a particular process there is a standard. But for us to conduct investigations internally, we don't have to meet any particular standard of proof. What I'm saying is, this is the process we have adopted over the years to assure that we have predication for each step of an investigation.

Senator WYDEN. With all due respect, Mr. Director, as I've said, you've worked very well with me. This is not what we've done over the years. Over the years, we had this specific articulable fact standard. We don't have it anymore, and that's why I'm pursuing this.

Director MUELLER. Happy to pursue with it you, Senator.

Senator WYDEN. Good. I want to ask this. Could I ask an additional question? Are we on the third round?

Chairman ROBERTS. Well, of course.

Senator WYDEN. Third round, or do you want me to proceed now, Mr. Chairman?

Chairman ROBERTS. No, right now.

Senator WYDEN. Thank you.

I want to ask this of General Gonzales, and it involves the privacy and the Civil Liberties Oversight Board with respect to domestic intelligence. The Senate had a different view with respect to how the board would work than ended up in the final law. And the board, by the Senate version, would be in a position to issue subpoenas. That's not how the law came out.

I'm curious whether you would be supportive of a request, General Gonzales, from the board, to issue a subpoena? It seems to me that if they, right from the get-go, don't have that kind of authority, the kind of authority that was envisioned by the Senate, that you limit some of their powers. And I'm just interested in how you would view a request from them.

Attorney General GONZALES. Well, if we got such a request, then obviously we would seriously consider it. But there are certain standards that the department would feel would have to be met in connection with the issuance of any subpoena. And simply because this privacy board requested a subpoena, no one should walk away from this hearing——

Senator WYDEN. If the privacy board met the constitutional standards, what you're telling me is you would not rule out giving them a subpoena.

Attorney General GONZALES. If we believe that a subpoena should be issued, we would issue a subpoena.

Senator WYDEN. Very good.

One last question, if I might, for you, Director Goss, on an area I think that involves a matter we both have a great interest in.

When you were here the last time, I asked about information sharing between the Counterterrorism Center and various intelligence agencies. It was based on my understanding that while information can be shared among the analysts assigned to the terrorism center, analysts have to seek special approval to share this information with their home agencies.

And this approval is required, despite the fact that there is this finite number of people working on terrorism in the intelligence community. All of them have a need to know, all are trained to handle sensitive data on persons and foreign nationals. How do you think this ought to be addressed? And since we talked about it a bit the last time, I thought it made sense to follow it up.

I still think something along the lines of a special terrorism analyst, you know, program, so as to allow all the analysts access to the same data would make sense. But since we talked about it the last time, I just wanted to follow up and get your sense of where we were.

Director GOSS. My sense of where we are is that we are beginning to work better as a team. I don't think it's what I would call a finished product yet. I think it's still a work in progress. Obviously, as you know, I want to be very circumspect in what I respond because Ambassador Negroponte has been given the responsibility for that in his role as DNI, and I no longer have those responsibilities. But when I left the ship, the direction was for more sharing and more compatibility in systems so that the goals that we both have ascribed to about getting information where you need it, when you need it, to the right analyst, would be available.

I cannot assure you that's going to be accomplished immediately. There are still a lot of different systems involved, a lot of different procedures, a lot of concerns about a need to know because need-to-know still is a principle that comes into the business. The trick is sharing with the people who need to know and not having a gratuitous release of information that could be harmful otherwise.

A lot of that is going to have to be worked out on a sort of experiential basis as we go along building the NCTC. We're still a little bit in the dark about what strategic planning actually will entail in the NCTC. As I say, I've left those matters in very good hands with Ambassador Negroponte and we've already had some conversations about some of the efforts that will be necessary out there and that's within the scope of what we've talked about.

Senator WYDEN. My concern is, and I'll wrap up with this Mr. Chairman, that the pre-9/11 set of walls has been replaced with a new set of walls preventing information sharing. And, for the life of me, when we have this limited number of people, all with the need to know, all who are trained to handle sensitive data, it just seems putting them through this kind of water torture exercise to share information is pointless and doesn't serve any of the interests that you three have talked about.

I thank you very much, Mr. Chairman, for the extra time.

Chairman ROBERTS. Senator Levin.

Senator LEVIN. Thank you, Mr. Chairman. I just have one additional question.

Sections 214 and 215 protect American citizens from being investigated, having their phone calls traced, who they're calling, who's calling them, as well as having their records obtained "solely on the basis of activities that are protected by the First Amendment."

So, you cannot be investigated as an American citizen under either 214 or 215 solely on that basis. That's a word which is deeply troubling to me because let's say part of the motivation is your First Amendment activities for being investigated. And I know this isn't your intent. I'm talking about what the law permits. I'm not talking about what you in your practice do.

Why should we suggest in the law, in any way, that if an investigation of an American citizen is based significantly or partly on their First Amendment activities that that would be OK? Or should we?

Attorney General GONZALES. Well, I think that provision was included by Congress to provide additional protections for the lawful activities of American citizens. But if American citizens are involved or have information or are in any way affiliated with terrorist activities, we should have the right to gather additional information through 214 and 215.

Senator LEVIN. Sure. But then the motivation is that participation. The motivation is not, even in part, their First Amendment activities.

Attorney General GONZALES. That would be correct, as far as I'm concerned.

Senator LEVIN. Yeah. Director.

Director MUELLER. Well, I mean, you can take Eric Rudolph, who may claim First Amendment protection for his acts against abortion clinics. It may have some First Amendment motive—protected beliefs. But the fact that he engaged in—we ought to be able to investigate an Eric Rudolph.

Senator LEVIN. Of course.

Director MUELLER. He can sit there and say, "Look, I'm against abortion clinics, but that doesn't mean he has a right to bomb them."

Senator LEVIN. Of course.

Director MUELLER. And so, I think it makes some sense that we cannot investigate someone solely on, but if they're engaged in someway in exercising their First Amendment rights but there is the possibility or the actuality of violence, it makes some sense to me, quite obviously, that we should.

Senator LEVIN. Of course. But the purpose of the investigation is not to investigate his exercise of First Amendments rights, is it?

Director MUELLER. No.

Senator LEVIN. That's what I'm driving at. And I think Americans are concerned about their rights. And we ought to be sensitive to that and you indicate you want to be sensitive to that. We ought to go after any acts of terrorism or support of acts of terrorism with all of our might. But we have to be very clear, as you were in your testimony, I think, that we're not after people for exercise of their constitutional rights. We're after them if they participate, encour-

age, in any way contribute to terrorist acts in some knowing way. Then we're going to go after them with the full weight of the law.

But the word "solely" in there has been troubling to a lot of people. It is to me and I think you ought to give some thought to eliminating that suggestion that we're not—our motivation is not to go after people's exercise of their rights, period. That's not the motivation. It's to go after any illegal activity.

Would you agree with that?

Attorney General GONZALES. I agree with that sir.

Director MUELLER. Yes.

Senator LEVIN. Thanks. Thank you, Mr. Chairman.

Chairman ROBERTS. Thank you, Senator. I have one question but I'm going to opine. I don't know if that's a verb or not but I'll use it.

Attorney General Gonzales, we're going to call you Jericho in terms of these walls. And I noted the discussion of walls in your written testimony. The views of your lawyers, including the lawyers in the Office of Intelligence Policy and Review, basically laid the foundation for and ultimately constructed the walls between law enforcement and intelligence officials which were then adopted by the Foreign Intelligence Surveillance court.

Some would say that these views were overly cautious—and I'm being generous. However, as the Foreign Intelligence Surveillance court, in their view, made clear, these "walls" were not mandated by the Constitution case law or the plain language of the FISA statute. Now that's an opinion upon which I do agree.

Nonetheless, my concern is with the current implementation of FISA. General Hayden testified before this Committee. He indicated the problem was not really preventing NSA employees from stepping over the line. It was getting NSA employees to even come close to the line. It took the FBI and the DOJ more than 2½ years after the passage of the PATRIOT Act to obtain the first FISA business record court order. We've gone over that.

And so the question that I was going to ask, but I'm just going to make it as a statement, is hopefully your attorneys are not still shying away from the line and hopefully they are doing what it takes to fully use the tools we gave you in the PATRIOT Act.

Now the FISA has become one of the nation's most important tools in protecting national security and the Department of Justice, as you know, plays a key role in supporting the intelligence community's use of the Act. The OIPR is at the forefront of this support, whether submitting applications to the Foreign Intelligence Surveillance court or reviewing the Attorney General-approved implementing guidelines. The attorneys at OIPR should be fully cognizant of the important role they play in the intelligence activities of the United States. I think it's extremely important that the OIPR be considered and that they consider themselves to be a full partner with the intelligence community.

The question I had was to you, sir, and for Director Mueller and for Director Goss, do you agree with that statement? Let the record show that you all three said yes.

[Laughter.]

Chairman ROBERTS. While we recognize the role that the OIPR plays in ensuring the integrity of the process, too many times in

this Committee's oversight OIPR has shown itself—this is my words, about 6 months ago during hearings—a rusty gate, if you will, that prevents the full use of intelligence authorities. I think OIPR should focus on enabling collection and ensuring compliance with the applicable laws.

Now, Senator Wyden's pointed out that we have not received your required semi-annual reports—I'm talking to the Attorney General—on the usage of National Security Letters for 2004 and we're here at the last of April. Mr. Gonzales, could you please look into why we haven't received those reports in a timely fashion? I know you will do so, sir.

Finally, I have a copy of the letter from the Attorney General which responds to a number of allegations from the ACLU about the Patriot Act abuses. Without objection, I want to enter this letter in the record.

[The information referred to follows:]

U. S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

April 4, 2005

The Honorable Arlen Specter
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

We have indicated in some of our responses to questions for the record, including those recently submitted on April 1, 2005, that we would supplement our responses to some questions. This letter is intended to supplement previous information we have provided regarding the usage of section 213 of the USA PATRIOT Act ("the Act"), relating to delayed-notice search warrants. We believe the information contained herein completely answers all the Committee's questions submitted to date regarding section 213 and we look forward to working with you on this and other issues related to the reauthorization of the USA PATRIOT Act.

As you know, the Department of Justice believes very strongly that section 213 is an invaluable tool in the war on terror and our efforts to combat serious criminal conduct. In passing the USA PATRIOT Act, Congress recognized that delayed-notice search warrants are a vital aspect of the Department's strategy of prevention: detecting and incapacitating terrorists, drug dealers and other criminals before they can harm our nation. Codified at 18 U.S.C. § 3103a, section 213 of the Act created an explicit statutory authority for investigators and prosecutors to ask a court for permission to delay temporarily notice that a search warrant was executed. While not scheduled to sunset on December 31, 2005, section 213 has been the subject of criticism and various legislative proposals. For the following reasons, the Department does not believe any modifications to section 213 are required.

To begin with, delayed-notice search warrants have been used by law enforcement officers for decades. Such warrants were not created by the USA PATRIOT Act. Rather, the Act simply codified a common-law practice recognized by courts across the country.[1] Section 213 simply created a uniform nationwide standard for the issuance of those warrants, thus ensuring that delayed-notice search warrants are evaluated under the same criteria across the nation. Like any other search warrant, a delayed-notice search warrant is issued by a federal judge only upon a showing that there is probable cause to believe that the property to be searched for or seized constitutes evidence of a criminal offense. A delayed-notice warrant differs from an ordinary search warrant only in that the judge specifically authorizes the law enforcement officers executing the warrant to wait for a limited period of time before notifying the subject of the search that a search was executed.

[1] *See infra* note 4.

In addition, investigators and prosecutors seeking a judge's approval to delay notification must show that, if notification were made contemporaneous to the search, there is reasonable cause to believe one of the following might occur:[2]

1. notification would endanger the life or physical safety of an individual;
2. notification would cause flight from prosecution;
3. notification would result in destruction of, or tampering with, evidence;
4. notification would result in intimidation of potential witnesses; or
5. notification would cause serious jeopardy to an investigation or unduly delay a trial.

To be clear, it is only in these five tailored circumstances that the Department may request judicial approval to delay notification, and a federal judge must agree with the Department's evaluation before approving any delay.

Delayed-notice search warrants provide a crucial option to law enforcement. If immediate notification were required regardless of the circumstances, law enforcement officials would be too often forced into making a "Hobson's choice": delaying the urgent need to conduct a search and/or seizure *or* conducting the search and prematurely notifying the target of the existence of law enforcement interest in his or her illegal conduct and undermine the equally pressing need to keep the ongoing investigation confidential.

A prime example in which a delayed-notice search warrant was executed is Operation Candy Box. This operation was a complex multi-year, multi-country, multi-agency investigative effort by the Organized Crime Drug Enforcement Task Force, involving the illegal trafficking and distribution of both MDMA (also known as Ecstasy) and BC bud (a potent and expensive strain of marijuana). The delayed-notice search warrant used in the investigation was obtained on the grounds that notice would cause serious jeopardy to the investigation (*see* 18 U.S.C. § 2705(a)(2)(E)).

In 2004, investigators learned that an automobile loaded with a large quantity of Ecstasy would be crossing the U.S.-Canadian border en route to Florida. On March 5, 2004, after the suspect vehicle crossed into the United States near Buffalo, Drug Enforcement Administration (DEA) Special Agents followed the vehicle until the driver stopped at a restaurant. One agent then used a duplicate key to enter the vehicle and drive away while other agents spread broken glass in the parking space to create the impression that the vehicle had been stolen. The ruse worked, and the drug traffickers were not tipped off that the DEA had seized their drugs. A subsequent search of the vehicle revealed a hidden compartment containing 30,000 MDMA tablets and ten pounds of BC bud. Operation Candy Box was able to continue because agents were able to delay notification of the search for more than three weeks.

On March 31, 2004, in a two-nation crackdown the Department notified the owner of the car of the seizure and likewise arrested more than 130 individuals. Ultimately, Operation Candy Box resulted in approximately 212 arrests and the seizure of $8,995,811 in U.S. currency, 1,546 pounds of MDMA powder, 409,300 MDMA tablets, 1,976 pounds of marijuana, 6.5 pounds of

[2] *See* 18 U.S.C. § 2705(a)(2).

methamphetamine, jewelry valued at $174,000, 38 vehicles, and 62 weapons. By any measure, Operation Candy Box seriously disrupted the Ecstasy market in the United States and made MDMA pills less potent, more expensive and harder to find. There has been a sustained nationwide eight percent per pill price increase since the culmination of Operation Candy Box; a permanent decrease of average purity per pill to the lowest levels since 1996; and currency seizures have denied traffickers access to critical resources - preventing the distribution of between 17 and 34 million additional Ecstasy pills to our nation's children.

Had Operation Candy Box agents, however, been required to provide immediate notification of the search of the car and seizure of the drugs, they would have prematurely revealed the existence of and thus seriously jeopardized the ultimate success of this massive long-term investigation. The dilemma faced by investigators in the absence of delayed notification is even more acute in terrorism investigations where the slightest indication of governmental interest can lead a loosely connected cell to dissolve. Fortunately though, because delayed-notice search warrants are available, investigators do not have to choose between pursuing terrorists or criminals and protecting the public – we can do both.

It is important to stress that in *all* circumstances the subject of a criminal search warrant is informed of the search. It is simply false to suggest, as some have, that delayed-notice search warrants allow the government to search an individual's "houses, papers, and effects" without notifying them of the search. In every case where the government executes a criminal search warrant, including those issued pursuant to section 213, the subject of the search is told of the search. With respect to delayed-notice search warrants, such notice is simply delayed for a reasonable period of time – a time period defined by a federal judge.

Delayed-notice search warrants are constitutional and do not violate the Fourth Amendment. The U.S. Supreme Court expressly held in *Dalia v. United States* that the Fourth Amendment does not require law enforcement to give immediate notice of the execution of a search warrant.[3] Since *Dalia*, three federal courts of appeals have considered the constitutionality of delayed-notice search warrants, and all three have upheld their constitutionality.[4] To our knowledge, no court has ever held otherwise. In short, long before the enactment of the USA PATRIOT Act, it was clear that delayed notification was appropriate in certain circumstances; that remains true today. The USA PATRIOT Act simply resolved the mix of inconsistent rules, practices and court decisions varying from circuit to circuit. Therefore, section 213 had the beneficial impact of mandating uniform and equitable application of the authority across the nation.

The Committee has requested detailed information regarding how often section 213 has been used. Let us assure you that the use of a delayed-notice search warrant is the exception, not the rule. Law enforcement agents and investigators provide immediate notice of a search warrant's execution in the vast majority of cases. According to Administrative Office of the U.S. Courts (AOUSC), during a 12-month period ending September 30, 2003, U.S. District Courts handled 32,539 search warrants. By contrast, in one 14-month period – between April 2003 and July 2004 –

---

[3] *See Dalia v. United States*, 441 U.S. 238 (1979); *see also Katz v. United States*, 389 U.S. 347 (1967).

[4] *See United States v. Freitas*, 800 F.2d 1451 (9th Cir. 1986); *United States v. Villegas*, 899 F.2d 1324 (2d Cir. 1990); *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000).

the Department used the section 213 authority only 61 times according to a Department survey. Even when compared to the AOUSC data for a shorter period of time, the 61 uses of section 213 still only accounts for less than 0.2% of the total search warrants handled by the courts. Indeed, since the USA PATRIOT Act was enacted on October 26, 2001, through January 31, 2005 – a period of more than three years – the Department has utilized a delayed-notice search warrant only 155 times.[5]

We have been working with United States Attorneys across the country to refine our data and develop a more complete picture of the usage of the section 213 authority. We have manually surveyed each of the 94 United States Attorneys' Offices for this information which, we understand, is not in a database. We are pleased to report our additional findings below.

In September 2003, the Department made public the fact that we had exercised the authority contained in section 213 to delay notification 47 times between October 2001, and April 1, 2003.[6] Our most recent survey, which covers the time frame between April 1, 2003, and January 31, 2005, indicates we have delayed notification of searches in an additional 108 instances. Since April 1, 2003, no request for a delayed-notice search warrant has been denied. It is possible to misconstrue this information as evidence that courts are merely functioning as a "rubber stamp" for the Department's requests. In reality, however, it is an indication that the Department takes the authority codified by the USA PATRIOT Act very seriously. We judiciously seek court approval only in those rare circumstances – those that fit the narrowly tailored statute – when it is absolutely necessary and justified. As explained above, the Department estimates that it seeks to delay notice of fewer than 1 in 500 search warrants issued nationwide. To further buttress this point, the 108 instances of section 213 usage between April 1, 2003, and January 31, 2005, occurred in 40 different offices. And of those 40 offices, 17 used section 213 only once. Looking at it from another perspective over a longer time frame, 48 U.S. Attorneys' Offices – or slightly more than-half – have never sought court permission to execute a delayed-notice search warrant in their districts since passage of the USA PATRIOT Act.

To provide further detail for your consideration, of the 108 times authority to delay notice was sought between April 1, 2003, and January 31, 2005, in 92 instances "seriously jeopardizing an investigation" (18 U.S.C. § 2705(a)(2)(E)) was relied upon as a justification for the application. And in at least 28 instances, jeopardizing the investigation was the sole ground for seeking court approval to delay notification, including Operation Candy Box described above. It is important to note that under S.1709, the "SAFE Act," which was introduced in the 108th Congress, this ground for delaying notice would be eliminated. Other grounds for seeking delayed-notice search warrants were relied on as follows: 18 U.S.C. § 2705(a)(2)(A) (danger to life or physical safety of an individual) was cited 23 times; 18 U.S.C. § 2705(a)(2)(B) (flight from prosecution) was cited 45 times; 18 U.S.C. § 2705(a)(2)(C) (destruction or tampering with evidence) was cited 61 times; and 18 U.S.C. § 2705(a)(2)(D) (intimidation of potential witnesses) was cited 20 times. As is probably

[5] The data reflected in this letter were gathered from paper surveys completed by each U.S. Attorney's Office. While we believe the survey method to be accurate, we cannot completely rule out the possibility of reporting errors.

[6] *See* Letter from Jamie E. Brown, Acting Assistant Attorney General, Office of Legislative Affairs, U.S. Department of Justice to F. James Sensenbrenner, Chairman, House of Representatives Committee on the Judiciary (May 13, 2003).

clear, in numerous applications, U.S. Attorneys' Offices cited more than one circumstance as justification for seeking court approval. The bulk of uses have occurred in drug cases; but section 213 has also been used in many cases including terrorism, identity fraud, alien smuggling, explosives and firearms violations, and the sale of protected wildlife.

Members of the Senate Judiciary Committee have also been concerned about delayed notification of seizures and have requested more detailed explanation of the number of times seizures have been made pursuant to delayed-notice warrants. The Department is pleased to provide the following information.

Seizures can be made only after receiving approval of a federal judge that the government has probable cause to believe the property or material to be seized constitutes evidence of a criminal offense and that there is reasonable necessity for the seizure. (*See* 18 U.S.C. § 3103a(b)(2)). According to the same survey of all U.S. Attorneys' Offices, the Department has asked a court to find reasonable necessity for a seizure in connection with delayed-notice searches 45 times between April 1, 2003, and January 31, 2005. In each instance in which we have sought authorization from a court during this same time frame, the court has granted the request. Therefore, from the time of the passage of the USA PATRIOT Act through January 31, 2005, the Department has exercised this authority 59 times. We previously, in May 2003, advised Congress that we had made 15 requests for seizures, one of which was denied.[7] In total, since the passage of the USA PATRIOT Act, the Department has therefore requested court approval to make a seizure and delay notification 60 times. Most commonly, these requests related to the seizure of illegal drugs. Such seizures were deemed necessary to prevent these drugs from being distributed because they are inherently dangerous to members of the community. Other seizures have been authorized pursuant to delayed-notice search warrants so that explosive material and the operability of gun components could be tested, other relevant evidence could be copied so that it would not be lost if destroyed, and a GPS tracking device could be placed on a vehicle. In short, the Department has sought seizure authority only when reasonably necessary.

The length of the delay in providing notice of the execution of a warrant has also received significant attention from Members of Congress. The range of delay must be decided on a case-by-case basis and is always dictated by the approving judge or magistrate. According to the survey of the 94 U.S. Attorneys' Offices, between April 1, 2003 and January 31, 2005, the shortest period of time for which the government has requested delayed-notice of a search warrant was 7 days. The longest such specific period was 180 days; the longest unspecified period was until "further order of the court" or until the end of the investigation. An unspecified period of time for delay was granted for six warrants (four of these were related to the same case). While no court has ever rejected the government's request for a delay, in a few cases courts have granted a shorter time frame than the period originally requested. For example, in one case, the U.S. Attorney for the District of Arizona sought a delay of 30 days, and the court authorized a shorter delay of 25 days.

Of the 40 U.S. Attorneys' Offices that exercised the authority to seek delayed-notice search warrants between April 1, 2003, and January 31, 2005, just over half (22) of the offices sought

---

[7] *See* Letter from Jamie E. Brown, Acting Assistant Attorney General, Office of Legislative Affairs, U.S. Department of Justice to F. James Sensenbrenner, Chairman, House of Representatives Committee on the Judiciary (May 13, 2003).

extensions of delays. Those 22 offices together made approximately 98 appearances to seek additional extensions. In certain cases, it was necessary for the Offices to return to court on multiple occasions with respect to the same warrant. One case bears note. The U.S. Attorney in the Southern District of Illinois sought and received approval to delay notification based on the fifth category of adverse result – that immediate notification would seriously jeopardize the investigation. The length of the delay granted by the court was 7 days. However, the notification could not be made within 7 days and the office was required to seek 31 extensions. So, each week for almost eight straight months, the case agent was made to swear out an affidavit, and the Assistant United States Attorney (AUSA) then had to reappear before the judge or magistrate to renew the delay of notice.

In the vast majority of instances reported by the U.S. Attorneys' Offices, original delays were sought for between 30 to 90 days. It is not surprising that our U.S. Attorneys' Offices are requesting up to 90-day delays. Ninety days is the statutory allowance under Title III for notification of interception of wire or electronic communications (*see* 18 U.S.C. 2518(8)(d)). In only one instance did a U.S. Attorney's Office seek a delay of a specified period of time longer than 90 days (180 days), and the court granted this request. In another instance, an office sought a 90-day delay period, and the court granted 180 days. In seven instances, the Department sought delays that would last until the end of the investigation. In only once instance was such a request modified. In that matter, the court originally granted a 30-day delay. However, when notification could not be made within 30 days, the U.S. Attorney's Office returned to the judge for an extension, and the judge granted an extension through the end of the investigation, for a total of 406 days. This is, according to our survey, the longest total delay a court authorized. However, most extensions were sought and granted for the same period as the original delay requested.

In one case, a court denied a U.S. Attorney's Office's request for an extension of the delay in providing notice. This matter involved three delayed-notice search warrants – all-stemming from the same investigation. The original period of delay sought and granted was for 30 days on all three warrants. The Office then sought 30-day extensions on all three warrants out of concern that the multiple targets of the investigation might flee to a foreign country if notified. The court denied our request. The judge in the matter reasoned that the need to delay notification warranted only a 30-day stay of service, particularly in light of the fact that one of the targets of the investigation was, by this time, in federal custody in California on an unrelated matter. At some point after notification was made, however, the other targets fled to Mexico.

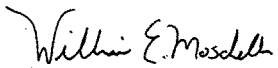
In sum, both before enactment of section 213 and after, immediate notice that a search warrant had been executed has been standard procedure. Delayed-notice search warrants have been used for decades by law enforcement and, as demonstrated by the numbers provided above, delayed-notice warrants are used infrequently and scrupulously – only in appropriate situations where immediate notice likely would harm individuals or compromise investigations, and even then only with a judge's express approval. The investigators and prosecutors on the front lines of fighting crime and terrorism should not be forced to choose between preventing immediate harm – such as a terrorist attack or an influx of illegal drugs – and completing a sensitive investigation that might shut down an entire terror cell or drug trafficking operation. Thanks to the long-standing availability of delayed-notice warrants in these circumstances, they do not have to make that

choice. Section 213 enables us to better protect the public from terrorists and criminals while preserving Americans constitutional rights.

As you may be aware, the Department published a detailed report last year that includes numerous additional examples of how delaying notification of search warrants in certain circumstances resulted in beneficial results. We have enclosed a copy for your convenience.

If we can be of further assistance regarding this or any other matter, please do not hesitate to contact this office.

Sincerely,



William E. Moschella
Assistant Attorney General

Enclosure

cc: The Honorable Patrick J. Leahy
Ranking Minority Member

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

April 26, 2005

The Honorable Dianne Feinstein
United States Senate
Washington, D.C. 20510

Dear Senator Feinstein:

In a letter dated April 4, 2005, the American Civil Liberties Union ("ACLU") responded to your March 25 request for information regarding alleged "abuses" of the USA PATRIOT Act. At your request, the Department of Justice has reviewed the ACLU's allegations. It appears that each matter cited by the ACLU either did not, in fact, involve the USA PATRIOT Act or was an entirely appropriate use of the Act. Thus, the ACLU is mistaken in its assertion in the letter that "the government has abused and misused the Patriot Act repeatedly" and in its press release, entitled "Patriot Act Abuses and Misuses Abound," that accompanied the letter and was released the night before the Attorney General was to appear before the Senate Judiciary Committee.

Our responses to the specific allegations are set forth below.

- **ALLEGATION #1: "Patriot Act [was used] to secretly search the home of Brandon Mayfield, a Muslim attorney whom the government wrongly suspected, accused and detained as a perpetrator of the Madrid train bombings."**

Mr. Mayfield's home was searched with the approval of a federal judge because the available information, including an erroneous finger-print match, gave investigators probable cause to believe that he was involved in the terrorist bombings in Madrid and not on account of any new authority created by the USA PATRIOT Act or any abuse of the Act.

The ACLU's allegation regarding Mr. Mayfield seems to be based in part on the mistaken idea that the search of Mr. Mayfield's home was conducted pursuant to Section 213 of the USA PATRIOT Act. That is not correct. The search was conducted pursuant to the Foreign Intelligence Surveillance Act ("FISA") under an authority that has existed in the FISA statute since 1995.

Because the search was conducted under a FISA court order, some of the USA PATRIOT Act provisions that amended FISA or relate to intelligence investigations may have been implicated or "used" in some sense of that word. For example, information-sharing provisions of the Act may have been used. And the time periods for the duration of FISA orders (Section 207) and the "significant purpose" test (Section 218) were implicated in the sense that those provisions apply to all FISA search applications. That does not in any way mean that these USA PATRIOT Act provisions were misused.

In addition, it would be wrong to suggest that Section 218 of the Act – and the change that provision made in the law – somehow made the search possible. The search could have been conducted just as readily under the standard in FISA in place prior to the USA PATRIOT Act. Under the previous standard in FISA, the government had to certify that "the purpose" of a search was to obtain foreign intelligence information, which is defined to include information necessary "to protect against . . . international terrorism." That standard had been interpreted to require that the "primary" purpose of the search was to obtain such information. In circumstances such as those the FBI encountered in the Mayfield investigation as they were known at the time, we believe that the government could have sought and obtained a FISA search warrant even under the old standard – certifying that the primary purpose of the search was to protect against international terrorism. Therefore, the ACLU is mistaken when it suggests that Section 218 "made the search possible."

Let us be clear: although Section 218 and its "significant purpose" test were not critical to obtaining a FISA search warrant with respect to Mayfield, Section 218 has been essential to the success of many national security investigations and the government's ability to fight terrorism effectively. See, e.g., U.S. Department of Justice, "The Use of Section 218 in Terrorism Investigations" (Apr. 11, 2005) (enclosed). Section 218 has been essential in facilitating information sharing between the intelligence community and the law-enforcement community, and we implore the Congress not to allow a wall to be reconstructed.

- **ALLEGATION #2: "Patriot Act [was used] to serve a National Security Letter (NSL) on an Internet Service Provider (ISP) so coercive under the terms prescribed by the statute that a federal court struck down the entire statute – as vastly expanded by the Patriot Act – used to obtain information about e-mail activity and web surfing for intelligence investigations."**

In Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004), a federal district judge in New York struck down as unconstitutional Section 2709 of Title 18, a statute that authorizes the FBI to request "subscriber information and toll billing records information, or electronic communication transactional records" from a wire or communications service provider, including an Internet service provider (ISP), upon the written certification of a high-level FBI official that such information is

"relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities." 18 U.S.C. § 2709. Such a request is one of several varieties of so-called "national security letters" or "NSLs" authorized by law.

The USA PATRIOT Act did not create the authority contained in Section 2709, nor did the Act create NSLs generally. Rather, Section 2709 was enacted as part of the Electronic Communications Privacy Act of 1986. Although the USA PATRIOT Act amended Section 2709, the amendment was not central to the court's decision striking down the law. The ACLU's suggestion to the contrary is belied by its own attorney, Jameel Jaffer, who has stated in connection with this case: "The provisions that we challenged and that the court objected to were in the statute before the Patriot Act was passed . . . . We could have raised the same objections before the power was expanded." Shaun Waterman, Ashcroft: U.S. will appeal terror-law ruling, UPI, Sept. 30, 2004.

Nor is the ACLU accurate to the extent it implies – in stating that the "statute [is] . . . used to obtain information about e-mail activity and web surfing" – that Section 2709 can be used to obtain the content of electronic communications. It cannot. Section 2709 authorizes the FBI to request only "the name, address, length of service, and local and long distance toll billing records of a person or entity" for telephone service and the "name, address, and length of service" for electronic communications. 18 U.S.C. § 2709(b).

Finally, the ACLU promotes the mistaken impression that Section 2709 and the amendment made to it by the PATRIOT Act were designed, as the ACLU states in its letter, to investigate individuals who "posted a blog critical of the government" or "to obtain a list of people who have e-mail accounts with a given political organization." To the contrary: the USA PATRIOT Act amendments to Section 2709 included specific safeguards to protect the First Amendment rights of United States persons. Section 2709 authorizes the FBI to request the listed information if "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States." (Emphasis added.)

The Department of Justice disagrees with key aspects of the district court's decision in Doe and has filed a notice of appeal with the U.S. Court of Appeals for the Second Circuit.

- **ALLEGATION #3: "Patriot Act [was used] to gag that ISP from disclosing this abuse to the public, and gag the ACLU itself, which represents the ISP, from disclosing this abuse to the public when the ACLU became aware of it, and from disclosing important circumstances relating to this abuse and other possible abuses of the gag, even to this very day."**

The ACLU is referring apparently here to the nondisclosure requirement contained in 18 U.S.C. § 2709 – the subject of the court's decision in Doe v. Ashcroft, discussed above. Again, the statute and its nondisclosure provision have existed since 1986 – long before the USA PATRIOT Act.

Such nondisclosure requirements are entirely appropriate under the circumstances. If information identifying the targets of international terrorism and espionage investigations were revealed, such disclosures would, as the U.S. Court of Appeals for the D.C. Circuit has recognized, "inform terrorists of both the substantive and geographic focus of the investigation[,] . . . would inform terrorists which of their members were compromised by the investigation, and which were not[,] . . . could allow terrorists to better evade the ongoing investigation and more easily formulate or revise counter-efforts . . . [and] be of great use to al Qaeda in plotting future terrorist attacks or intimidating witnesses in the present investigation." Center for National Security Studies v. U.S. Department of Justice, 331 F.3d 918, 928-29 (D.C. Cir. 2003). Indeed, the district court in Doe itself observed:

> [T]he Government's interest in protecting the integrity and efficacy of international terrorism and counterintelligence investigations is a compelling one. The Supreme Court has so acknowledged: "This Court has recognized the Government's 'compelling interest' in withholding national security information from unauthorized persons in the course of executive business." A suspected terrorist or foreign intelligence operative who is alerted that the Government is conducting an investigation may destroy evidence, create false leads, alert others, or otherwise take steps to avoid detection. More generally, such disclosures can reveal the Government's intelligence-gathering methods, from which foreign intelligence operatives or terrorists could learn better how to avoid detection.

Doe, 334 F. Supp. 2d at 513-14 (quoting Department of the Navy v. Egan, 484 U.S. 518, 527 (1988)).

- **ALLEGATION #4: "Patriot Act [was used] to charge, detain, and prosecute a Muslim student in Idaho, Sami al-Hussayen, for providing 'material support' to terrorists because he posted to an Internet website links to objectionable materials, even though such links were available on the websites of the government's own expert witness in the case and on the website of a major news outlet."**

Sami Al-Hussayen was charged in a fourteen-count indictment with three counts of providing or conspiring to provide material support to terrorists and eleven counts of making false statements to immigration authorities and visa fraud. Al-Hussayen consented to a detention order in his criminal case in the period leading up to trial because he was already subject to a detention hold by immigration authorities, who had requested his deportation for immigration fraud.

The ACLU is incorrect in claiming that the Department prosecuted Al-Hussayen "for engaging in First Amendment activities." The material-support-to-terrorism charges against Al-Hussayen were not based on an exercise of his right to free speech. On the contrary, the indictment charged that, among other things, Al-Hussayen had participated in illegal fundraising for HAMAS, a designated foreign-terrorist organization, as well as terrorist groups operating in Chechnya. Al-Hussayen did so by giving money and by using his computer skills to create and maintain websites, one of which included a fundraising appeal with a direct link to the official website for HAMAS. In addition, Al-Hussayen used his expertise in computer science to design web pages for the publication of several fatwas endorsing suicide attacks, and he himself published these fatwas on the Internet. One of these fatwas – published in May 2001 – actually suggested that an effective method for suicide attackers would be to fly an airplane into a building. Other evidence in the case included Al-Hussayen's own statements endorsing such violent jihad.

Prior to trial, Al-Hussayen moved to dismiss the material support charges on the grounds that his conduct was protected by the First Amendment. The trial judge denied that motion. Although Al-Hussayen was acquitted of the material support charges and some of the immigration charges, the jury was deadlocked on other immigration charges. Under these circumstances, the Government could have asked for a second trial on the remaining immigration charges. Instead, Al Hussayen was deported based on his immigration fraud, and the remaining charges were dropped.

- **ALLEGATION #5: "Patriot Act [was used] to deny, on account of his political beliefs, admission to the United States of a Swiss national, Tariq Ramadan, a prominent Muslim scholar who was to assume a teaching position at Notre Dame University."**

It is our understanding that the USA PATRIOT Act was not used to deny a visa to Tariq Ramadan. Indeed, a final determination regarding Ramadan's reapplication for a visa never occurred. The Ramadan case was handled by the Department of Homeland Security and the Department of State, and further questions regarding that case should be directed to those departments.

- **ALLEGATION #6: "Patriot Act [was used] to investigate and prosecute crimes that are not terrorism offenses, even though it cited terrorism prevention as the reason Congress should enact the law, and cites terrorism prevention as the reason why it cannot be changed."**

The ACLU highlights five matters that involved uses – not abuses – of the USA PATRIOT Act that did not involve terrorism investigations. Such uses were entirely proper and were not, as the ACLU contends, "misuses" of the Act. Many provisions in the Act simply updated the law to reflect recent technological developments and have been used, as Congress intended, not only in terrorism

cases, but also to combat other serious criminal conduct. Other provisions of the Act made general improvements to the law that apply to all types of criminal investigations. With respect to these provisions, the Department has used its authority appropriately to investigate and prosecute criminal offenses.

- **ALLEGATION A – "The FBI used the Patriot Act against Michael Galardi, the owner of two Las Vegas strip clubs, and several local officials that it believes accepted bribes from Galardi. Investigators reportedly delivered subpoenas under Section 314 of the Patriot Act – portrayed to Congress as necessary to undercut terrorist financing – to two Las Vegas stockbrokers ordering the release of detailed business records that prosecutors hope will reveal hidden proceeds that may be evidence of bribery."**

In the Las Vegas investigation, investigators requested financial information from various financial institutions pursuant to regulations promulgated under Section 314(a)[1] of the USA PATRIOT Act. Section 314 is entitled "Cooperative Efforts to Deter Money Laundering." Subpart (a) of Section 314 directs the Secretary of the Treasury to adopt regulations for the purpose of encouraging the sharing of information among financial institutions and federal law enforcement and regulatory agencies that pertain to individuals reasonably suspected of engaging in "terrorist acts or money laundering activities." (Emphasis added.) The plain text of the provision therefore makes it clear that the statute can and should be used in cases that do not involve terrorism.

The regulations promulgated pursuant to Section 314(a) were issued in September 2002, and are set forth in 31 C.F.R. §103.100. They establish a process by which federal law enforcement agencies may request account information from financial institutions through the Treasury Department's Financial Crimes Enforcement Network (FinCEN) if the requested information pertains to either terrorist activity or money laundering. In addition, by agreement between FinCEN and federal law enforcement agencies, this process may only be used to obtain information that is essential to a significant investigation.

It should be noted that a FinCEN request identifies only the existence of financial accounts. Account records are not available under Section 314(a) or the regulations promulgated under it. To obtain records, a law enforcement agency must comply with traditional legal process, such as a federal grand jury subpoena. Therefore, to the extent the ACLU suggests that the government used "subpoenas under 314 of the Patriot Act," it is incorrect.

---

[1]Section 314(a) originated in legislation to combat international money laundering, which was proposed by then Senate Banking Committee Chairman Sarbanes. *See* Section 104 of S. 1511, 1st Sess., 107th Cong.

In the Las Vegas case, the FBI followed the prescribed procedure to the letter. Michael Galardi ultimately pleaded guilty to a RICO violation in connection with his scheme to bribe local government officials.

- **ALLEGATION B – "The Justice Department used the Patriot Act against a lovesick 20-year-old woman from Orange County, CA, who planted threatening notes aboard a Hawaii-bound cruise ship on which she was traveling with her family. The woman, who said she made the threats to try to return home to her boyfriend, was sentenced to two years in federal prison because of a provision in the Patriot Act targeting threats of terrorism against mass transportation systems."**

The Department of Justice properly used Section 801 of the USA PATRIOT Act to prosecute Kelley Marie Ferguson, who pleaded guilty to one count of conveying false information about an attempt to cause death to the passengers and crew of a mass transportation system. Section 801, introduced by Senator Leahy, prohibits an individual from, among other things, conveying false information concerning attacks on mass transportation vehicles. In this case, Ms. Ferguson left two notes in cruise-ship restrooms stating that all American passengers and crew on the ship would be killed if the ship ported in the United States. Because of these notes, the ship was temporarily diverted off the shore of Honolulu with more than 1600 passengers and 700 crew members aboard. Approximately 120 federal, state, and local law enforcement officers of the Hawaii Joint Terrorism Task Force investigated the threat and searched the ship. After all of this took place, Ms. Ferguson left a third threatening note.

While it turned out that the terrorist threat in this case was a hoax, law enforcement authorities responded appropriately by taking seriously the threat to the lives of United States citizens. Ms. Ferguson was charged with and pleaded guilty to a violation of Section 801 – a violation that did involve a threat of terrorism in this case. Thus, this is not an example of a provision of the USA PATRIOT Act being used "outside the terrorism context," as the ACLU suggests.

In any event, even if Ms. Ferguson's threats had not been perceived to be and treated as threats of terrorism, it would have been entirely appropriate to prosecute her under Section 801. Nothing in the language or legislative history of that provision suggests that it is, or should be, confined to cases of terrorism. See 18 U.S.C. § 1993 (codifying Section 801). Indeed, when Senator Leahy described the provision on the floor of the Senate, he stated that the provision, as its title indicates, "targets acts of terrorism and other violence against mass transportation systems." Cong. Rec. S10997 (daily ed. Oct. 25, 2001) (emphasis added). Senator Leahy went on to provide an example of the "gap" in the law that Section 801 was intended to address; the example he provided – a deranged

passenger slitting the throat of a Greyhound bus driver, resulting in the death of six individuals – did not involve terrorism. Id.

- **ALLEGATION C – "In July 2002 Czech-born University of Connecticut graduate student, Tomas Foral, 26, became the first person to be charged under the USA Patriot Act for possession of a biological agent with no 'reasonably justified' purpose, a crime carrying a sentence of up to a decade in prison. His crime: discovering 35-year-old tissue samples from an anthrax-infected cow in a broken university cold-storage unit and moving them to a working freezer. Unfortunately for Foral, that freezer broke at the height of the anthrax scare and a tipster who found the samples phoned in Foral's name to the authorities. Foral finally agreed to community service and some restrictions on his activities."**

Section 817 of the USA PATRIOT Act prohibits individuals from possessing a biological agent, such as anthrax, "of a type or in a quantity that, under the circumstances, is not reasonably justified by a prophylactic, protective, bona fide research, or other peaceful purpose." 18 U.S.C. § 175. The use of this provision was entirely appropriate in the case of Tomas Foral. Foral was instructed by his professors to kill and then dispose of five anthrax samples. Instead, he knowingly kept two of the five samples of this extremely dangerous biological agent in his personal freezer in the school's laboratory even though he was not engaged in research involving anthrax.

Again, nothing in the language of Section 817 limits its use to cases of terrorism, and nothing in the legislative history suggests that Congress intended such a limitation. The provision was based on legislation that Senator Biden introduced in the 106th Congress – well before the events of September 11, 2001, and the anthrax attacks that followed shortly thereafter. Cong. Rec. S10997 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy); Cong. Rec. S11049 (daily ed. Oct. 25, 2001)(statement of Sen. Biden). The provision was intended simply to make it illegal to possess anthrax or other dangerous biological agents absent a bona fide research or other peaceful purpose – a prohibition that is needed and appropriate even in circumstances not known to involve terrorism.

- **ALLEGATION D – "On March 23, 2005, the Department of Justice charged David Banach of Parsippany, New Jersey under the Patriot Act for shining a laser beam on an airplane using a hand held device. Banach, age 38, faces a statutory maximum of 20 years in prison and a $250,000 fine for the offense, even though the FBI admitted that the incident had no connection to terrorism. Banach claimed that he was using the device to look at stars with his seven year-old daughter from the deck of his home."**

David Banach was charged with two counts of making false statements, in violation of 18 U.S.C. § 1001, and one count of interfering with pilots of an aircraft with reckless disregard for the safety of human life, in violation of 18 U.S.C. § 1993(a)(5), a provision that was added to the criminal code in Section 801 of the USA PATRIOT Act. Again, the use of Section 801, which, among other things, prohibits individuals from interfering with someone operating a mass transportation vehicle, was entirely appropriate in this case. According to the indictment, Banach admitted shining a hand-held laser into the cockpit of a small passenger jet, temporarily blinding the pilots as they were approaching a New Jersey airport for landing. He also admitted lying to FBI agents repeatedly about this incident.

As noted above, nothing in the language or legislative history of Section 801 suggests that the provision is or should be limited to cases of terrorism.

- **ALLEGATION E – "Section 213, the 'sneak and peek' warrant provision of the Patriot Act, appears to have been used almost exclusively outside of terrorism investigations. Indeed, when the Department of Justice selectively reported some of the instances in which it has used sneak and peek warrants, its list consisted primarily of investigation of non-terrorism offenses, even though it cites counter-terrorism rationales as the reasons why reasonable limits should not be put on these searches."**

Delayed-notice search warrants have been used by law enforcement officers for decades in traditional criminal investigations, such as those involving drugs and child pornography. Such warrants were not created by the USA PATRIOT Act; the Act simply codified a common-law practice recognized by courts across the country and created a uniform nationwide standard for the issuance of those warrants. The Department has continued using delayed-notice search warrants in criminal investigations appropriately but sparingly since the passage of the Act. The Department estimates, for example, that fewer than one in 500 search warrants obtained nationwide are delayed-notice warrants. For further details regarding the Department's use of Section 213, we are enclosing a copy of a letter from Assistant Attorney General William Moschella to Chairman Specter dated April 4, 2005.

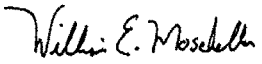
* * * *

As these facts show, the ACLU is simply incorrect in its claim that the "government has abused and misused the Patriot Act repeatedly." The Department of Justice takes seriously any accusation that the Department is "abusing or misusing" any provision of law – including the USA PATRIOT Act. It appears that in this case the accusations made by the ACLU are baseless. During the hearing, Attorney General Gonzales rightly stated:

"All of us have the same objective: ensuring the security of the American people while preserving our civil liberties. I therefore hope that we will consider reauthorization in a calm and thoughtful manner. Our dialogue should be based on facts, rather than exaggeration."

We appreciate this opportunity to present the facts and look forward to continuing to work with you to ensure the reauthorization of the USA PATRIOT Act. We sincerely believe that the tools it contains are essential to the government's ability to fight terrorism and serious criminal conduct.

Sincerely,



William E. Moschella
Assistant Attorney General

Enclosures

cc: Anthony Romero
Director, ACLU

The Honorable Arlen Specter
Chairman
Committee on the Judiciary

The Honorable Patrick J. Leahy
Ranking Minority Member
Committee on the Judiciary

The Use of Section 218 in Terrorism Investigations

Background: Before the passage of the USA PATRIOT Act, applications for orders authorizing electronic surveillance or physical searches under FISA had to include a certification from a high-ranking Executive Branch official that the purpose of the surveillance or search was to gather foreign intelligence information. As interpreted by the courts and later the Justice Department, this requirement meant that the "primary purpose" of the collection had to be to obtain foreign intelligence information rather than evidence of a crime. Over the years, the prevailing interpretation and implementation of the "primary purpose" standard had the effect of limiting coordination and information sharing between intelligence and law enforcement personnel. Because the courts evaluated the government's purpose for using FISA at least in part by examining the nature and extent of such coordination, the more coordination that occurred, the more likely courts would find that law enforcement, rather than foreign intelligence, had become the primary purpose of the surveillance or search.

During the 1980s, the Department operated under a set of largely unwritten rules that limited to some degree information sharing between intelligence and law enforcement officials. In 1995, however, the Department established formal procedures that more clearly separated law enforcement and intelligence investigations and limited the sharing of information between intelligence and law enforcement personnel more than the law required. The promulgation of these procedures was motivated in part by the concern that the use of FISA authorities would not be allowed to continue in particular investigations if criminal prosecution began to overcome intelligence gathering as an investigation's primary purpose. To be sure, the procedures were intended to permit a degree of interaction and information sharing between prosecutors and intelligence officers, while at the same time ensuring that the FBI would be able to obtain or continue FISA coverage and later use the fruits of that coverage in a criminal prosecution. Over time, however, coordination and information sharing between intelligence and law enforcement investigators became even more limited in practice than was allowed in theory under the Department's procedures. Due both to confusion about when sharing was permitted and to a perception that improper information sharing could end a career, a culture developed within the Department sharply limiting the exchange of information between intelligence and law enforcement officials.

In recent testimony before the Senate Judiciary Committee, Patrick Fitzgerald, U.S. Attorney for the Northern District of Illinois, recounted from personal experience how this "wall" between law enforcement and intelligence personnel operated in practice:

> I was on a prosecution team in New York that began a criminal investigation of Usama Bin Laden in early 1996. The team – prosecutors and FBI agents assigned to the criminal case – had access to a number of sources. We could talk to citizens. We could talk to local police officers. We could talk to other U.S. Government agencies. We could talk to foreign police officers. Even foreign intelligence personnel. And foreign citizens. And we did all those things as often as we could. We could even talk to al Qaeda members – and we did. We actually called several members and associates of al Qaeda to testify before a grand jury in

> New York. And we even debriefed al Qaeda members overseas who agreed to become cooperating witnesses.
>
> But there was one group of people we were not permitted to talk to. Who? The FBI agents across the street from us in lower Manhattan assigned to a parallel intelligence investigation of Usama Bin Laden and al Qaeda. We could not learn what information they had gathered. That was "the wall."

The USA PATRIOT Act brought down this "wall" separating intelligence officers from law enforcement agents. It not only erased the perceived statutory impediment to more robust information sharing between intelligence and law enforcement personnel, but it also provided the necessary impetus for the removal of the formal administrative restrictions as well as the informal cultural restrictions on information sharing.

Section 218 of the USA PATRIOT Act eliminated the "primary purpose" requirement. Under section 218, the government may conduct FISA surveillance or searches if foreign-intelligence gathering is a "significant" purpose of the surveillance or search, thus eliminating the need for courts to compare the relative weight of the "foreign intelligence" and "law enforcement" purposes of the surveillance or search, and thereby allowing for increased coordination and sharing of information between intelligence and law enforcement personnel. Section 504 buttressed section 218 by specifically amending FISA to allow intelligence officials conducting FISA surveillance or searches to "consult" with federal law enforcement officials to "coordinate" efforts to investigate or protect against international terrorism, espionage, and other foreign threats to national security, and to clarify that such coordination "shall not" preclude the certification of a "significant" foreign intelligence purpose or the issuance of an authorization order by the Foreign Intelligence Surveillance Court.

The Department has moved aggressively to implement sections 218 and 504 of the USA PATRIOT Act and bring down "the wall." Following passage of the Act, the Department adopted new procedures designed to increase information sharing between intelligence and law enforcement officers, which were affirmed by the Foreign Intelligence Surveillance Court of Review on November 18, 2002. The Attorney General also instructed every U.S. Attorney to review intelligence files to discover whether there was a basis for bringing criminal charges against the subjects of intelligence investigations; thousands of files have been reviewed as part of this process. The Attorney General likewise directed every U.S. Attorney to develop a plan to monitor terrorism and intelligence investigations and to ensure that information about terrorist threats is shared with other agencies and that criminal charges are considered in those investigations.

These efforts to increase coordination and information sharing between intelligence and law enforcement officers, which were made possible by the USA PATRIOT Act, have yielded extraordinary dividends by enabling the Department to open numerous criminal investigations, disrupt terrorist plots, bring numerous criminal charges, and convict numerous individuals in terrorism cases.

Examples:

1. **PORTLAND SEVEN:** The removal of the "wall" separating intelligence and law enforcement personnel played a crucial role in the Department's successful dismantling of a Portland, Oregon terror cell, popularly known as the "Portland Seven." Members of this terror cell had attempted to travel to Afghanistan in 2001 and 2002 to take up arms with the Taliban and al Qaeda against United States and coalition forces fighting there. Law enforcement agents investigating that case learned from one member of the terror cell, Jeffrey Battle, through an undercover informant, that before the plan to go to Afghanistan had been formulated, at least one member of the cell had contemplated attacking Jewish schools or synagogues and had even been casing such buildings to select a target for such an attack. By the time investigators received this information from the undercover informant, they had suspected that a number of other persons besides Battle had been involved in the Afghanistan conspiracy. But while several of these other individuals had returned to the United States from their unsuccessful attempts to reach Afghanistan, investigators did not yet have sufficient evidence to arrest them.

   Before the USA PATRIOT Act, prosecutors would have faced a dilemma in deciding whether to arrest Battle immediately. If prosecutors had failed to act, lives could have been lost through a domestic terrorist attack. But if prosecutors had arrested Battle in order to prevent a potential attack, the other suspects in the investigation would have undoubtedly scattered or attempted to cover up their crimes. Because of sections 218 and 504 of the USA PATRIOT Act, however, it was clear that the FBI agents could conduct FISA surveillance of Battle to detect whether he had received orders from an international terrorist group to reinstate the domestic attack plan on Jewish targets and keep prosecutors informed as to what they were learning. This gave prosecutors the confidence not to arrest Battle prematurely while they continued to gather evidence on the other members of the cell. Ultimately, prosecutors were able to collect sufficient evidence to charge seven defendants and then to secure convictions and prison sentences ranging from three to eighteen years for the six defendants taken into custody. Charges against the seventh defendant were dismissed after he was killed in Pakistan by Pakistani troops on October 3, 2003. Without sections 218 and 504 of the USA PATRIOT Act, however, this case likely would have been referred to as the "Portland One" rather than the "Portland Seven."

2. **SAMI AL-ARIAN:** The Department shared information pursuant to sections 218 and 504 before indicting Sami Al-Arian and several co-conspirators on charges related to their involvement with the Palestinian Islamic Jihad (PIJ). PIJ is alleged to be one of the world's most violent terrorist outfits. It is responsible for murdering over 100 innocent people, including Alisa Flatow, a young American killed in a bus bombing near the Israeli settlement of Kfar Darom. The indictment states that Al-Arian served as the secretary of the

Palestinian Islamic Jihad's governing council ("Shura Council"). He was also identified as the senior North American representative of the PIJ.

In this case, sections 218 and 504 of the USA PATRIOT Act enabled prosecutors to consider all evidence against Al- Arian and his co-conspirators, including evidence obtained pursuant to FISA that provided the necessary factual support for the criminal case. By considering the intelligence and law enforcement information together, prosecutors were able to create a complete history for the case and put each piece of evidence in its proper context. This comprehensive approach was essential in enabling prosecutors to build their case and pursue the proper charges. The trial in this case is scheduled to begin May 16, 2005.

3. **VIRGNIA JIHAD:** Prosecutors and investigators also used information shared pursuant to sections 218 and 504 of the USA PATRIOT Act in investigating the defendants in the socalled "Virginia Jihad" case. This prosecution involved members of the Dar al-Arqam Islamic Center, who trained for jihad in Northern Virginia by participating in paintball and paramilitary training, including nine individuals who traveled to terrorist training camps in Pakistan or Afghanistan between 1999 and 2001.These individuals are associates of a violent Islamic extremist group known as Lashkar-e-Taiba (LET), which primarily operates in Pakistan and Kashmir and has ties to the al Qaeda terrorist network. As the result of an investigation that included the use of information obtained through FISA, prosecutors on June 25, 2003, indicted eleven individuals in a 41-count indictment. Subsequently, four of these defendants, Yong Ki Kwon, Mohammed Aatique, Donald Thomas Surratt, and Khwaja Mahmood Hasan, pled guilty and agreed to cooperate. On September 25, 2003, a superseding indictment was filed charging the remaining seven defendants with the conspiracy, conspiracy to levy war against the United States, conspiracy to provide material support to al Qaeda, conspiracy to contribute services to the Taliban, conspiracy to contribute material support to Lashkar-e-Taiba, supplying services to the Taliban, commencing an expedition against a friendly nation, conspiracy to possess and use a firearm in connection with a crime of violence, receipt of firearm or ammunition with cause to believe a felony will be committed therewith, false official statements, and using a firearm in connection with a crime of violence. The first phase of the case has been completed with all of the defendants convicted.

4. **YEMENI SHEIKH:** The information sharing between intelligence and law enforcement personnel made possible by sections 218 and 504 of the USA PATRIOT Act was useful in the investigation of two Yemeni citizens, Mohammed Ali Hasan Al-Moayad and Mohshen Yahya Zayed, who were charged in 2003 with conspiring to provide material support to al Qaeda and HAMAS. The complaint against these two individuals alleges that an FBI undercover operation developed information that Al-Moayad had boasted that he had personally handed Usama Bin Laden $20 million from his terrorist

fund-raising network and that Al-Moayad and Zayed flew from Yemen to Frankfurt, Germany in 2003 with the intent to obtain $2 million from a terrorist sympathizer (portrayed by a confidential informant) who wanted to fund al Qaeda and HAMAS. During their meetings, Al-Moayad and Zayed specifically promised the donor that his money would be used to support HAMAS, al Qaeda, and any other mujahideen, and "swore to Allah" that they would keep their dealings secret. Al-Moayad and Zayed were extradited to the United States from Germany in November 2003 and were convicted on March 10, 2005. Al-Moayad and Zayed face up to 60 and 30 years in jail respectively.

5. **ARNAOUT CASE:** The Department used sections 218 and 504 to gain access to intelligence, which facilitated the indictment of Enaam Arnaout, the Executive Director of the Illinois-based Benevolence International Foundation (BIF). Arnaout conspired to obtain charitable donations fraudulently in order to provide financial assistance to Chechen rebels and organizations engaged in violence and terrorism. Arnaout had a long-standing relationship with Usama Bin Laden and used his charity organization both to obtain funds illicitly from unsuspecting Americans for terrorist organizations, such as al Qaeda, and to serve as a channel for people to contribute money knowingly to such groups. Arnaout ultimately pleaded guilty to a racketeering charge, admitting that he diverted thousands of dollars from BIF to support Islamic militant groups in Bosnia and Chechnya. He was sentenced to over 11 years in prison.

6. **DRUGS FOR STINGER MISSILES:** The broader information sharing and coordination made possible by sections 218 and 504 of the USA PATRIOT Act assisted the prosecution in San Diego of several persons involved in an al Qaeda drugs-for-weapons plot, which culminated in several guilty pleas. Two defendants admitted that they conspired to distribute approximately five metric tons of hashish and 600 kilograms of heroin originating in Pakistan to undercover United States law enforcement officers. Additionally, they admitted that they conspired to receive, as partial payment for the drugs, four "Stinger" anti-aircraft missiles that they then intended to sell to the Taliban, an organization they knew at the time to be affiliated with al Qaeda. The lead defendant in the case is currently awaiting trial.

7. **IRAQI SPY:** Sections 218 and 504 were critical in the successful prosecution of Khaled Abdel Latif Dumeisi, who was convicted by a jury in January 2004 of illegally acting as an agent of the former government of Iraq, as well as two counts of perjury. Before the Gulf War, Dumeisi passed information on Iraqi opposition members located in the United States to officers of the Iraqi Intelligence Service stationed in the Iraqi Mission to the United Nations. During this investigation, intelligence officers conducting surveillance of Dumeisi pursuant to FISA coordinated and shared information with law enforcement agents and prosecutors investigating Dumeisi for possible violations of criminal law. Because of this coordination, law enforcement agents and prosecutors learned from intelligence officers of an incriminating telephone conversation that took place in April 2003 between Dumeisi and a co-conspirator. This phone conversation corroborated other evidence that Dumeisi was acting as an agent of the Iraqi government and provided a compelling piece of evidence at Dumeisi's trial.

Chairman ROBERTS. That concludes the hearing, and we thank you for your time.

[Whereupon, at 11:28 a.m., the Committee adjourned.]

PROPOSED CHANGES TO THE UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM (USA PATRIOT) ACT OF 2001

DAY THREE

TUESDAY, MAY 24, 2005

UNITED STATES SENATE,
SELECT COMMITTEE ON INTELLIGENCE,
Washington, DC.

The Committee met, pursuant to notice, at 9:41 a.m., in room SD–106, Dirksen Senate Office Building, Hon. Pat Roberts (Chairman of the Committee) presiding.

Committee Members Present: Senators Roberts, Hatch, Bond, Lott, Snowe, Chambliss, Rockefeller, Levin, Feinstein, Wyden and Bayh.

OPENING STATEMENT OF HON. PAT ROBERTS

Chairman ROBERTS. The Committee will come to order. I apologize for the lateness of the arrival of the Chair. We are operating under a 2-hour rule, which I think everybody understands.

This morning, the Senate Select Committee on Intelligence continues its series of hearings on the USA PATRIOT Act. Over the past 4 weeks, the Committee has conducted three hearings—two open and one closed—concerning the use and reauthorization of the PATRIOT Act. Those hearings, our oversight activities, and the Committees comprehensive classified analysis of Executive branch activities under the Foreign Intelligence Surveillance Act form the basis of our legislative actions.

The purpose of our hearing this morning is to receive testimony on specific legislative proposals prior to the Committee's mark-up of PATRIOT Act legislation. This morning we will hear from two distinguished panels. First, the Committee will hear from Ms. Valerie Caproni, the General Counsel of the Federal Bureau of Investigation.

Our second panel will consist of Mr. David Kris, a former Associate Deputy Attorney General in the Department of Justice; Mr. Joe Onek, Senior Counsel and Director of the Liberty and Security Initiative at the Constitution Project; Mr. Daniel Collins, also a former Associate Deputy Attorney General and Chief Privacy Officer at the Department of Justice; and Mr. James Dempsey, Executive Director of the Center for Democracy and Technology.

I want to thank you all and the Committee thanks you all for being here today.

The Committee also has received the views of Professor Richard Seamon of the University of Idaho College of Law with regard to section 203 of the draft legislation. Without objection, Mr. Seamon's letter will be included in the record.

[The information referred to follows:]

Richard H. Seamon
Associate Professor of Law
phone: 208-885-7061
email: richard@uidaho.edu

University of Idaho
College of Law
P.O. Box 442321
Moscow, Idaho 83844-2321
208-885-4977

May 23, 2005

by email and regular mail
Chairman Pat Roberts
Vice Chairman John D. Rockefeller, IV
United States Senate
Select Committee on Intelligence
211 Hart Senate Office Building
Washington, D.C. 20510-6475

Re: **Draft Committee Bill to Reauthorize the USA PATRIOT Act**

Dear Chairman Roberts and Vice Chairman Rockefeller:

I write to support a provision in the draft Committee bill to reauthorize the Patriot Act. The provision, currently designated Section 203, would amend the definition of "foreign intelligence information" in the Foreign Intelligence Surveillance Act of 1978 ("FISA"). I support this amendment because it will correct the erroneous interpretation of FISA by the Foreign Intelligence Surveillance Court of Review in *In re Sealed Case*, 310 F.3d 717 (2002). The Court of Review interpreted FISA, as amended by the Patriot Act, to bar the government from using FISA surveillance to get evidence to arrest and prosecute foreign agents, even when such arrests and prosecutions are necessary to prevent acts of international terrorism and other foreign threats. That erroneous interpretation prevents the Patriot Act from achieving its purpose of bringing down the dysfunctional, statutory "wall" between foreign intelligence and criminal law enforcement activities. By correcting the Court of Review's error, Section 203 of the draft Committee bill will implement Congress's original intent in the FISA and the Patriot Act and, in the process, remove a potentially serious restriction on the government's power to fight international terrorism and other foreign threats.

To briefly describe my qualifications to address the issue, I served as an Assistant to the Solicitor General of the United States from 1990-1996. In that position, I became familiar with FISA and other statutory, as well as constitutional, provisions governing federal government surveillance of persons in the United States. Since 1996, I have been a law professor who has taught and done legal research and writing on issues of criminal procedure. Most relevantly, I have done extensive research on the history of FISA and the Patriot Act, focusing on those statutes' information sharing provisions. My research resulted in the publication of an article, co-written with William Dylan Gardner, entitled *The Patriot Act and the Wall Between Foreign Intelligence and Law Enforcement*, 28 Harvard Journal of Law & Public Policy 319 (2005), available at http://www.law.uidaho.edu/richard [hereafter cited as "Seamon & Gardner"].

To enrich education through diversity the University of Idaho is an equal opportunity/affirmative action employer.

In the paragraphs below, I briefly explain (1) how the Court of Review erred in interpreting FISA; (2) how that error harms the domestic fight against international terrorism; and (3) how the error would be appropriately corrected by Section 203 of the draft Committee bill.

1. The Court of Review misinterpreted FISA.

As amended by Section 218 of the Patriot Act, FISA authorizes the government to seek a FISA warrant and conduct FISA surveillance if "a significant purpose" of the proposed surveillance is "to obtain foreign intelligence information."[1] "Foreign intelligence information," in turn, is defined in relevant part to mean information that is "necessary to" the ability of the United States to protect against "international terrorism" and certain other foreign threats.[2] Under the plain language of the statute, the government should be able to seek a FISA warrant and conduct FISA surveillance for the purpose of getting the evidence needed to arrest and prosecute a foreign agent – for any type of crime – as long as the government reasonably considers the agent's arrest and prosecution necessary to prevent an act of international terrorism or one of the other foreign threats identified in FISA's definition of "foreign intelligence information."

The Foreign Intelligence Surveillance Court of Review accepted this analysis in *In re Sealed Case*, but only up to a point. The court found persuasive the government's argument that "arresting and prosecuting terrorist agents of, or spies for, a foreign power may well be the best technique to prevent them from successfully continuing their terrorist or espionage activity."[3] Nonetheless, the court concluded, contrary to the government's argument, that the government cannot use FISA surveillance to get evidence of "ordinary crimes" by a suspected terrorist, even if the government reasonably believes that the arrest and prosecution of the terrorist for those crimes is necessary to protect against a planned terrorist attack.[4]

The Court of Review's "ordinary crimes" restriction misinterprets FISA. FISA does not base the government's surveillance authority on the likelihood of crime, ordinary or otherwise. To the contrary, Congress deliberately decided against a purely criminal standard for FISA surveillance.[5] Congress decided, instead, to allow surveillance of U.S. persons based on conduct

---

[1] 50 U.S.C. 1804(a)(7)(b).

[2] *Id.* § 1801(e)(1).

[3] *In re Sealed Case*, 310 F.3d 717, 724 (Foreign Intell. Surv. Ct. Rev. 2002) (per curiam).

[4] *See id.* at 735-36.

[5] *See* Seamon & Gardner at 427-435.

that is not invariably a crime.[6] And, Congress required that the purpose of such surveillance be obtaining "foreign intelligence information," which does not invariably constitute evidence of crime.[7] Because of these decisions, the government does not need probable cause of crime to get a FISA warrant and it does not seek a FISA warrant merely to get more evidence of crime. Rather, the government's ultimate aim must be "to obtain foreign intelligence information," and "foreign intelligence information" is defined instrumentally – by reference to its necessity for achieving certain foreign intelligence purposes, including the protection of this country from specified foreign threats. Thus, evidence of crime – even "ordinary" crime – constitutes "foreign intelligence information" as long as it is needed for law enforcement measures that the government reasonably considers necessary to protect against the foreign threats specified in FISA's definition of "foreign intelligence information."

It bears emphasis that the interpretation of FISA that I am advancing is substantially the same that the Department of Justice advanced, and the court rejected, in *In re Sealed Case*.[8] As far as I know, the Department continues to believe, as I do, that the Court misinterpreted FISA by adopting the "ordinary crimes" restriction. Unlike me, the Department has not urged Congress (as far as I know) to correct the misinterpretation by amending FISA. The Department may have good (perhaps strategic) reasons for not seeking correction of what the Department itself (at least in 2002) believed was an error. That should not prevent Congress from considering an amendment of FISA to implement its original intent.[9]

---

[6]To get a FISA warrant, the government must, among other requirements, establish probable cause that the target of the proposed surveillance "is a foreign power or an agent of a foreign power." 50 U.S.C. 1804(a)(4)(A). FISA classifies a U.S. person as an "agent of a foreign power" based on the person's "knowing" involvement, "for or on behalf of a foreign power," in various activities that are often – but not always – a crime, including (1) "'clandestine intelligence gathering activities' [that] involve or may involve violations of Federal criminal law"; (2) "other clandestine intelligence activities," "pursuant to the direction of an intelligence service or network of a foreign power," "which * * * involve or are about to involve a violation of the criminal statutes of the United States"; (3) "sabotage or international terrorism [as defined elsewhere in the FISA, 50 U.S.C. 1801(c)] * * * or activities that are in preparation therefor"; (4) entering or remaining in the United States "under a false or fraudulent identity"; or (5) aiding or abetting, or conspiring to engage in, any of the first three categories of activities listed in this sentence. *Id.* § 1801(b)(2).

[7]*See In re Sealed Case*, 310 F.3d at 723 n.10.

[8]*See id.* at 735-36.

[9]In addition to imposing the "ordinary crimes" restriction discussed in the text, the Court of Review held that FISA, as amended by Section 218 of the Patriot Act, bars the government from using FISA surveillance for the sole purpose of prosecuting even "foreign intelligence crimes." *In re Sealed Case*, 310 F.3d at 735. The court based this "foreign intelligence crimes" restriction upon its view that Section 218 "imposed a requirement that the government have a measurable foreign intelligence purpose, *other than* just criminal prosecution of even foreign intelligence crimes." *Id.* at 735 (emphasis added). As discussed in the text, however, the plain language of FISA reflects that criminal prosecution of any type of crime can serve protective foreign intelligence purposes. Thus, the Court of Review's "foreign intelligence crimes" restriction, like its "ordinary crimes" restriction, misinterprets FISA. The Court of Review thought that its "foreign intelligence crimes" restriction would not "make much practical

2. The misinterpretation of Section 218 impairs the domestic fight against international terrorism.

The Department of Justice presumably believes that no great harm will come of *In re Sealed Case*'s erroneous restriction on FISA surveillance. The Department has been wrong about this sort of thing before (having participated in building the wall) . I urge the Committee to consider whether the Department is wrong now.

The Department has promised, since 9/11, that it will take the same approach to suspected terrorists that Robert Kennedy's Justice Department took toward suspected members of the mob: It has promised to arrest and prosecute suspected terrorists for any and all offenses, including ones as minor as "spitting on the sidewalk."[10] The problem is that the Department cannot use FISA surveillance to get evidence of such "ordinary crimes" under the erroneous interpretation discussed in Point 1.

Perhaps the Justice Department plans to fulfill its promise by relying on a different statute, Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[11] Title III will not always work, for two reasons. First, Title III authorizes surveillance for evidence of only certain crimes.[12] Thus, federal officials cannot use Title III to obtain evidence of minor state or federal offenses (such as overstaying a visa) even when, for example, the arrest of a suspected terrorist for such an offense would incapacitate the terrorist and thereby disrupt an ongoing terrorist plot. Second, officials conducting a FISA surveillance operation are not always able, in the midst of that operation, to determine when the purpose of the operation will be deemed – by a court in

---

difference," because, "when [the government] commences an electronic surveillance of a foreign agent, typically it will not have decided whether to prosecute the agent." *In re Sealed Case*, 310 F.3d at 735. The "foreign intelligence crimes" restriction, however, might be construed to operate not just at the commencement of electronic surveillance but throughout the surveillance. So construed, the restriction could require the government to cease surveillance under a FISA warrant if and when the sole objective of the surveillance becomes the gathering of evidence for a prosecution of a foreign intelligence crime. That result not only rests on a misreading of the Patriot Act; it also could significantly restrict the government's domestic fight against international terrorism, for essentially the same reasons as could the court's "ordinary crimes" restriction. *See infra* Point 2; *see also* Seamon & Gardner at 461-462.

[10]Attorney General John Ashcroft, Prepared Remarks for the US Mayors Conference (Oct. 25, 2001) ("Robert Kennedy's Justice Department, it is said, would arrest mobsters for 'spitting on the sidewalk' if it would help in the battle against organized crime. It has been and will be the policy of this Department of Justice to use the same aggressive arrest and detention tactics in the war on terror."), available at http://www.usdoj.gov/archive/ag/speeches/2001/agcrisisremarks10_25.htm (visited May 22, 2005); Viet Dinh, "Life After 9/11: Issues Affecting the Courts and the Nation," 51 U. Kan. L. Rev. 219, 224 (2003) (remarks to the same effect by then-Assistant Attorney General Viet Dinh at the 2002 Tenth Circuit Judicial Conference, Conference Proceedings).

[11]18 U.S.C. 2510-2522.

[12]*See* 18 U.S.C. 2516(1).

hindsight – to have become that of obtaining evidence of ordinary crime. Unless the officials guess correctly – and cease surveillance until they have secured a Title III warrant – the evidence collected under the FISA warrant could be considered illegally obtained under *In re Sealed Case.* The illegal nature of the evidence, in turn, could invalidate any arrest and prosecution, even if they are necessary to prevent a terrorist attack or other foreign threat from occurring.

The arrest and prosecution of dangerous persons for "ordinary crimes" is an important and well-established way to neutralize the danger that such persons pose.[13] The government understood this when it prosecuted Al Capone for not paying taxes and, later, when it undertook to arrest mob figures even for offenses as minor as "spitting on the sidewalk." The government must be able to use this same approach to suspected terrorists, especially when prosecuting them for "ordinary" crimes provides a way to avoid disclosing intelligence sources and methods.[14] The government's ability to use that approach, however, has been hampered by *In re Sealed Case*'s interpretation of FISA.

3. The Court of Review's misinterpretation of FISA would be appropriately corrected – and a potentially serious restriction on the government's power to international terrorism would be removed – by the amendment to the Definition of "Foreign Intelligence Information" proposed in Section 203 the draft Committee bill.

As discussed in Points 1 and 2, FISA authorizes the government to use FISA surveillance to take law enforcement measures in certain circumstances. Specifically, the government can use FISA surveillance to get evidence for arrest, prosecution, and other law-enforcement measures as long as the government reasonably considers those measures necessary to protect against international terrorism or one of the other foreign threats identified in FISA's definition of "foreign intelligence information." Although FISA now, and always has, permitted this use of FISA surveillance, courts have not recognized its permissibility. Section 203 of the draft Committee bill would clarify the matter, and thereby effectuate Congress's original intent. In the process, Section 203 would remove a potentially serious restriction on the government's power to fight international terrorism.

Section 203 would amend FISA's definition of "foreign intelligence information" in 50 U.S.C. 1801(e) to add the language that is underlined and in bold-face type below:

---

[13]*See, e.g.*, Harry Litman, "Pretextual Prosecution," 92 Geo. L.J. 1135, 1169-1170 (2004) (stating author's inclination "to defend in principle a policy of using the Al Capone approach to bring immigration charges (or other relatively trivial federal charges) when there is reason to believe that the defendants have material information about terrorism"); Daniel C. Richman & William J. Stuntz, "Al Capone's Revenge: An Essay on the Political Economy of Pretextual Prosecution," 105 Colum. L. Rev. 583, 623 (2005) ("there may be no realistic alternative" to the Justice Department's use of "the Al Capone approach to counterterrorism prosecutions").

[14]The 9/11 Commission's Report describes instances in which actual or suspected international terrorists committed crimes with no immediately obvious connection to their terrorist activities. *See* Seamon & Gardner at 461 & n.682 (citing relevant portions of Report).

"(e) 'Foreign intelligence information' means--,

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect **(including protection by use of law enforcement methods such as criminal prosecution)** against--,

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power * * *."

The amendment clarifies the definition by making it explicit that information can constitute "foreign intelligence information" – and therefore can be sought and collected under a FISA warrant – when it is intended to be used for law enforcement measures that will protect the United States from an act of international terrorism or one of the other foreign threats specified in the definition of "foreign intelligence information."[15]

It may be useful to describe a situation in which the amendment would clarify the government's power to use FISA surveillance.

- An alien innocently enters the United States on a student visa but, while here, joins a U.S. cell of al Qaeda. With the support of that organization and other members of the cell, he begins plotting to poison a large U.S. city's water supply. Based on his status as a foreign agent, the FBI obtains a FISA warrant for surveillance of his activities. While conducting surveillance under the FISA warrant, the FBI discovers not only evidence of the plot but also evidence that he has overstayed his student visa. The government determines that the best way to disrupt the plot, without revealing its knowledge of the plot, is to get evidence to arrest, prosecute, and deport the foreign agent for overstaying his visa. The government may use FISA surveillance to get the evidence needed for the agent's arrest, prosecution, and deportation.

This example shows that sometimes the best way to protect against a foreign threat is by law enforcement measures involving an "ordinary" offense. Other examples can be envisioned involving U.S. persons, rather than aliens, who are acting as foreign agents and who have

---

[15]My co-author and I have proposed a similar amendment to the definition of "foreign intelligence information." *See* Seamon & Gardner at 458-462.

committed other, seemingly "ordinary" offenses. Section 203 of the draft Committee bill clarifies that, when the arrest and prosecution of such agents protect against international terrorism or one of the foreign threats identified in FISA's definition of "foreign intelligence information," the evidence needed to take those law enforcement measures is "foreign intelligence information" that the government can use FISA surveillance to obtain.

When the government conducts surveillance in order to get information that is meant to be used to protect against foreign threats, that surveillance is foreign intelligence surveillance, rather than surveillance for ordinary criminal law enforcement purposes. In other words, foreign intelligence surveillance is identified by its objective of protecting the United States from foreign threats, rather than by the methods used to achieve that objective. Indeed, Congress recognized when enacting the original FISA that "use of foreign intelligence information as evidence in a criminal trial is one way the Government can lawfully protect against * * * international terrorism" and other foreign threats.[16] In this context, arrest, prosecution, and other law-enforcement measures function as counterintelligence activities, rather than as ends in themselves. Accordingly, FISA surveillance to obtain evidence for taking such law enforcement measures is governed by the constitutional requirements for foreign intelligence surveillance, rather than the constitutional requirements for criminal law enforcement surveillance.

The constitutional requirements for foreign intelligence surveillance differ from those for criminal law enforcement surveillance.[17] The different standards reflect, among other things, their different purposes. Criminal law enforcement surveillance has the programmatic purpose "to advance the general interest in crime control"[18] or one of the broader "social" purposes that invariably underlie "the general interest in crime control."[19] In contrast, foreign intelligence surveillance, as discussed above, serves the quite different, paramount purpose of preserving the nation. Congress carefully considered, and acted within, constitutional requirements for foreign intelligence surveillance both in 1978, when it enacted the original FISA, and in 2001, when it amended FISA in the Patriot Act. Because Section 203 of the draft Committee bill merely

---

[16]H.R. Rep. No. 95-1283, pt. 1, at 49 (1978).

[17]*See generally* United States v. United States District Court for the Eastern District of Michigan, 407 U.S. 297 (1972) (commonly known as "the *Keith* case").

[18]*Compare* City of Indianapolis v. Edmond, 531 U.S. 32, 44 & 46 (2000) (striking down on Fourth Amendment grounds a city's drug checkpoint program of stopping cars without a warrant and without individualized suspicion of drivers because the primary purpose of the program, judged at a "programmatic level," was "to advance the general interest in crime control").

[19]*Compare* Ferguson v. City of Charleston, 532 U.S. 67, 81 & 84 (2001) (striking down on Fourth Amendment grounds a city's program of drug testing pregnant women in situations indicating drug use because, judged at a "programmatic level," the "immediate" purpose of program was to gather evidence for prosecutions and the "ultimate" purposes of protecting unborn children and getting women off drugs did not distinguish the program from other law enforcement searches, since "law enforcement involvement always serves some broader social purpose or objective").

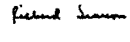
clarifies Congress's intent in those prior statutes, Section 203 itself satisfies constitutional requirements for foreign intelligence surveillance.

* * *

The USA PATRIOT Act was supposed to bring down the dysfunctional statutory "wall" between foreign intelligence and criminal law enforcement. The Act has not completely achieved that result, however, because of the Foreign Intelligence Surveillance Court of Review's decision in *In re Sealed Case*. Section 203 of the draft Committee bill corrects the Court of Review's error and, in the process, removes a potentially serious restriction on the government's power to fight international terrorism.

Thank you for considering my views. I would gladly answer any questions about my views that the Committee may have.

Respectfully submitted,



Richard H. Seamon
Associate Professor of Law

Chairman ROBERTS. Before recognizing the distinguished Vice Chairman for any comments he might have, I want to comment briefly on the draft bill we provided to our witnesses.

This draft bill does reflect, I think, a balanced approach, addressing both concerns about the use of existing authorities and identified gaps in investigative tools that are needed. The draft legislation accomplishes three simple goals.

First, it permanently authorizes nine intelligence-related provisions set to expire at the end of the year. I believe there is strong bipartisan support for these provisions.

Second, it extends to national security investigators tools already used in Federal criminal cases. It does not create new authority.

And, third, it addresses some of the concerns expressed by critics of the PATRIOT Act by establishing new reporting requirements and standards for use of certain tools under the Act.

Let me emphasize that the investigative tools that this bill extends to FBI national security investigators are the same tools that have been used by Federal criminal investigators for years to access information relevant to their investigations. For example, the mail cover provision is simply the statutory authorization of an authority which the FBI has had under Postal Service regulations for 30 years.

Additionally, the administrative subpoena provision is similar to 335 other legislatively enacted administrative subpoenas currently being used by the Executive branch. Such administrative subpoenas have been upheld against Constitutional challenges for over 50 years.

In fact, the Secretary of Labor can use administrative subpoenas to enforce the Fair Labor Standards Act. The Federal Maritime Commission can issue administrative subpoenas to support its investigations. And Federal criminal investigators can use administrative subpoenas in health care fraud, child pornography, and also any case dealing with drugs or narcotics.

Federal investigators, however, cannot use them to investigate spies and international terrorists. The Secret Service can issue an administrative subpoena to investigate threats against the President, but the President can not use an administrative subpoena to investigate threats against America posed by terrorists and spies.

I have yet to hear any reasonable reason to deprive national security investigators of well-established and long-used investigative tools. We expect the men and women of the FBI to protect us and yet some advocate constraints that would tie their hands, I think unnecessarily. I believe that national security investigators should be able to use every Constitutional tool at their disposal to protect the United States.

This is the Committee's fourth hearing on the USA PATRIOT Act this year. In prior hearings, the Committee has received testimony from panels of outside experts, law enforcement and intelligence officials who have used PATRIOT Act tools in the field, and the Attorney General, the Director of the FBI, and the Director of the CIA.

Moreover, with regard to the specific provisions that are being discussed and considered by this Committee, we have tried to go out of our way to ensure that every member has had the oppor-

tunity to be fully informed of the provisions included in the draft legislation. Our General Counsel has briefed the Members' designated staff and has been available to meet with any Member to discuss any concern about any provision of the bill.

Additionally, last week, the Committee held a briefing for all Members at which counsel from both sides of the aisle went through the legislation and were available for questions.

Finally, at my direction, the Committee staff has worked very diligently with those who have concerns about provisions in the bill in an effort to resolve those concerns. As a result, the staff has been able to reach a number of agreements that may be presented at markup as amendments are considered or as part of a managers' amendment.

More than 3½ years have passed since enactment of the PATRIOT Act. Members of Congress have had ample opportunity to inquire into the implementation of these authorities and to debate and consider the reauthorization of the expiring provisions. While fundamental differences will, no doubt, remain, I am committed to working with any Member of this Committee in an effort to address his or her concerns prior to markup.

At this time, I'd like to recognize the distinguished Vice Chairman, Senator Rockefeller, for any statement he would like to make.

Vice Chairman ROCKEFELLER. Thank you, Mr. Chairman, very much, and I welcome our witnesses, all of them. I want to make just a couple of comments to set my sense of the perspective of the hearing.

We meet, obviously, to hear testimony on a draft bill, which makes permanent certain PATRIOT Act authorities, and some of them are amended and others are added, like the investigative powers.

I support reauthorizing the PATRIOT Act and I am inclined to support adding investigative authorities, but only if it can be shown that these new authorities are necessary and would not infringe on the constitutional rights of Americans, which is a subjective subject.

I would like to identify several questions that the Committee, in my opinion, must address and that I hope the witnesses will before reporting the bill. The views of the witnesses, as I indicated, will be greatly appreciated.

The first question concerns the renewal of expiring authorities.

In its May 18 letter to the Committee last week, the Department of Justice quoted the President's statement of earlier this year, in which he said that "to protect the American people, the Congress must promptly renew all provisions of the PATRIOT Act this year."

Congress, most certainly, will—to use the President's word—"renew" all expiring provisions of the PATRIOT Act. In most cases, I believe that Congress will do that by making those provisions permanent. But should a new sunset date, such as in 4 years, be set for a few expiring provisions, much as we did on earlier ones, in order to ensure they are examined again before deciding whether they should be permanent? Does one go from zero to permanency or does one put in a time of review?

For example, the draft bill contains proposals to amend the FISA title on orders for business records and other tangible things. In

light of this, I think Congress extend rather than repeal the sunset of Section 215 of the PATRIOT Act on FISA Court orders for records and revisit this title in a few years to see how these amendments and others in the draft bill have worked out.

The second area I raise is the proposed changes to Section 215. The Attorney General has told this Committee and the Judiciary Committee that the Department of Justice is willing to support amendments that clarify Section 215 of the PATRIOT Act on several points. One of those matters is judicial review.

The draft bill that you have is silent on judicial review of Section 215 orders for business records and other tangible things. There are discussions within the Committee about an amendment to carry out the Attorney General's commitment.

I welcome the views of the witnesses about what is required to make the review meaningful. It will be essential to have rules that protect national security information. But should the statute also ensure that the applicant has access to the nonclassified parts of the Government's case and argument or to declassified summaries of classified information?

And what statutory language will be necessary to ensure that the applicant is able to raise, and the Court has the authority to decide, all appropriate questions of privilege and unreasonableness?

The third area deserving careful attention, in my judgment, is that of administrative subpoenas. The draft bill proposes to give to the Director of the FBI, or designees down to special agents in charge, the power to issue subpoenas for records in national security investigations. The Congress frequently grants subpoena authority to various agencies, boards, and officials who exercise economic or health and safety regulatory functions. This is not new. On several recent occasions it has given subpoena authority to the Attorney General in law enforcement circumstances. I am not aware of any time in which Congress has given, directly to the FBI, subpoena authority.

That doesn't make it right or wrong, but I think that needs to be thought about. I would like to know the views of the witnesses on a number of questions as we consider providing this expanded investigative authority:

What is the problem with the Department of Justice's and the FBI's current authority? The FBI is able to obtain records through National Security Letters, which are not subpoenas. If subpoenas or orders for records are needed, the FBI is able to obtain them—from the FISA Court or by way of grand jury subpoenas—through the Department of Justice. Has the Department of Justice demonstrated to the Committee that any investigations have faltered, even for one critical moment, because of the lack of administrative subpoena authority? I don't prejudge this; I raise this question for discussion.

If additional authority is needed, does the draft bill provide the right authority and the right protections?

As with judicial review of Section 215 orders, do the provisions on judicial review provide subpoenaed parties with a fair opportunity, and provide courts with sufficient authority, to challenge and prevent abuse?

Finally, the Committee would benefit from the views of the witnesses on two other notable changes contained in the proposed legislation.

The draft bill calls for an amendment to the definition of foreign intelligence information. The amendment has the potential to change the scope of FISA surveillance, search, and record production authorities. The draft bill also would provide for a new title in FISA on mail covers, an investigative power currently set forth in regulations but not statute.

I will be interested in the views of our witnesses, and I thank the Chairman.

Chairman ROBERTS. Our first witness is Ms. Valerie Caproni, the General Counsel of the Federal Bureau of Investigation. Ms. Caproni, please proceed.

[The prepared statement of Ms. Caproni follows:]

PREPARED STATEMENT OF VALERIE CAPRONI

Chairman Roberts, Vice Chaiiman Rockefeller, and Members of the Committee, it is my pleasure to appear before you this morning to discuss legislation that would reauthorize many important provisions of the USA PATRIOT Act and provide important new tools to national security investigators. Over the course of the last 7 weeks, the Department of Justice has made its case for why each one of the 16 USA PATRIOT Act provisions scheduled to sunset at the end of 2005 must be made permanent. In numerous hearings as well as classified and unclassified briefings for Members of Congress, we have explained how the Department has used those authorities contained in the USA PATRIOT Act to safeguard the safety and security of the American people. Thanks to the Act, we have been able to identify terrorist operatives, dismantle terrorist cells, disrupt terrorist plots, and capture terrorists before they have been able to strike. Moreover, the record demonstrates that we have done this while protecting the privacy rights and civil liberties of the American people.

Many of the most important provisions of the USA PATRIOT Act, however, are scheduled to sunset at the end of this year, and the Department therefore applauds this Committee for taking up legislation that would make permanent those provisions of the Act falling under this Committee's jurisdiction. We are also heartened that this Committee has come forward with novel and worthwhile ideas for strengthening the Department's counterterrorism capabilities. Prior to this Committee's April 27, 2005, oversight hearing on the USA PATRIOT Act, Attorney General Gonzales and Director Mueller submitted detailed written testimony on utility of the provisions of the Act that are scheduled to expire at the end of the year, and I will not repeat that testimony today.

Rather, I will simply reiterate the Department's strong support for making permanent those USA PATRIOT Act provisions covered by section 101 of this Committee's draft legislation: sections 203(b), 203(d), and 218, which toppled the wall separating intelligence investigators from law enforcement investigators and have allowed vital information sharing of immeasurable value in the war against terrorism; section 206, which provided national security investigators with the ability to obtain certain court-approved roving surveillance orders that had previously been available exclusively to criminal investigators; section 207, which has increased the efficiency of the Foreign Intelligence Surveillance Act (FISA) application process by lengthening the maximum duration of FISA electronic surveillance and physical search orders targeting certain non-United States persons; section 214, which allows national security investigators to utilize court-approved pen register or trap and trace devices to obtain information relevant to international terrorism or espionage investigations; Section 215, which allows national security investigators to obtain court orders requesting the production of records relevant to international terrorism or espionage investigations; and section 225, which provides those individuals and companies assisting in the implementations of FISA surveillance orders the same legal immunity granted to those assisting in the implementation of criminal investigative wiretaps.[1]

[1] As called for in section 101 of the Committee's draft legislation, the Department also supports making permanent section 204, which is essentially a technical amendment.

The Department also supports making permanent section 6001(a) of the Intelligence Reform and Terrorism Prevention Act of 2004. This provision, which has come to be known as the "Lone Wolf" provision, allows the government to gain court approval for FISA surveillance of a non-United States person when there is probable cause to believe that he or she is engaged in or preparing to engage in international terrorism, whether or not he or she is known to be affiliated with a larger terrorist group. While this provision is currently scheduled to sunset at the end of this year, unfortunately, the threat to the United States posed by known or apparent Lone Wolf terrorists will not similarly cease on December 31, 2005. Therefore, the Department strongly endorses the enactment of section 102 of the Committee's draft legislation, which would remove the sunset on the Lone Wolf provision.

Besides reauthorizing important counterterrorism authorities that are scheduled to expire at the end of this year, the Committee's draft legislation also contains other vital provisions that will enhance the Department's ability to safeguard the American people from our Nation's terrorist enemies. Section 216, for example, would extend the maximum duration for certain FISA surveillance, search, and pen register orders targeting non-United States persons, thus allowing the Department to take resources currently devoted to the mechanics of repeatedly renewing FISA applications in certain cases—which are considerable—and instead allow them to be focused on other investigative activities as well as conducting additional oversight of the use of intelligence collection authorities by the FBI. Indeed, as the Attorney General testified before the Committee, the Department estimates that, had these amendments been included in the USA PATRIOT Act, 25,000 attorney hours that were devoted by personnel in the Department's Office of Intelligence Policy and Review to processing FISA applications would already have been saved. That figure, moreover, does not include the time that would have been saved by agents and attorneys at the FBI. The bipartisan WMD Commission recently agreed that many of the changes contained in section 216 would allow the Department to focus its attention where it is most needed, and to ensure that adequate attention is given to cases implicating the civil liberties of Americans. The Department therefore commends the Committee for including this important provision in its draft legislation.

The Department also supports section 212 of the Committee's draft legislation, which relates the availability of mail covers in national security investigations. Mail covers are concerned with recording information appearing on the outside of mail and thus do not implicate the reasonable expectation of privacy that exists with respect to the contents of sealed mail. Notwithstanding the relatively non-intrusive nature of mail covers, however, the ability to obtain the type of information they provide promptly and effectively can be of great importance in the national security context. For example, if there is information indicating that a person may be involved in terrorist or terrorism-support activities, information showing that he has been in contact by mail with other persons who are known to be involved in international terrorism can be critical to advancing and determining the priority of the investigation.

As part of reforms made by Congress following the attacks of September 11, 2001, Congress has already acted to strengthen the legal procedures for obtaining comparable sender/receiver information in relation to electronic mail and telephone communications. Specifically, 18 U.S.C. § 2709 provides access to electronic communication transactional records and telephone toll billing records information, on certification by FBI officials at appropriately high supervisory levels that the information is relevant to an authorized investigation to protect against international terrorism or espionage. But there is no comparable statutory specification concerning national security mail covers. The current standards governing their availability are defined by United States Postal Service regulations, and the determination whether they will be conducted in particular cases ultimately depends on decisions by Postal Service personnel.

The FBI is, however, in the best position to assess whether investigative activity is needed in particular circumstances to protect against international terrorism or espionage, and whether the use of a mail cover is warranted in the context of such an investigation. As noted, Congress has recognized this point in relation to the corresponding information for electronic mail in existing statutory provisions. Section 212 would simply extend the same principle and similar procedures to information observable on the outside of physical mail and would thus enable the FBI to carry out more effectively its central mission of protecting Americans from terrorist attacks.

The Department also welcomes section 213 of the Committee's draft legislation, which responds to the President's call to provide for administrative subpoena authority in terrorism investigations. In combating terrorism, prevention is key: we cannot wait to disrupt terrorist acts or to prosecute terrorist crimes after they occur.

To stay a step ahead of the terrorists, investigators need tools allowing them to obtain relevant infollnation as quickly as possible.

An administrative subpoena is one such tool. An administrative subpoena is a request from a government official instructing the recipient to provide information relevant to the investigation. This type of subpoena authority would allow investigators to obtain relevant information quickly in terrorism investigations, where time is often of the essence.

Like any subpoena, administrative subpoenas are subject to judicial review. If a recipient refuses to comply with a request for the production of records, investigators may not simply seize those records; rather, they are required to ask a court to enforce it. Furthermore, recipients of administrative subpoenas need not wait for investigators to go to court. Instead, they may file their own challenges to the legality of the subpoena. But for those recipients who wish to assist investigators, administrative subpoenas provide a mechanism allowing them to quickly turn over relevant records while at the same time shielding themselves from civil liability.

The constitutionality of such subpoenas is well established, and executive branch agencies now have the authority to issue administrative subpoenas in more than 300 other areas. Such subpoenas, for example, may be issued by the Appalachian Regional Commission, Chemical Standard and Hazard Investigation Board, Commodity Futures Trading Commission, Consumer Product Safety Commission, and Corporation for National Community Service, just to name those departments and agencies whose names begin with a letter from A to C. These subpoenas are not, however, currently available in terrorism investigations, even though the consequences of a terrorist attack could be far more severe than those of the many other areas in which Congress has permitted the use of administrative subpoenas. Simply put, the Department believes that terrorism investigators should have at least the same investigative tools currently available to the Department in investigations ranging from health care fraud to child abuse. In 2001, for example, the Department issued 2,102 administrative subpoenas in Federal health care investigations and 1,783 in child abuse and exploitation investigations. Administrative subpoenas are a time-tested tool, and the Department looks forward to working with the Members of the Committee on this important proposal.

Before concluding my testimony, three other provisions in the Committee's draft legislation deserve mention. First, as the Attorney General recently disclosed, the Department has recently obtained Section 215 orders from the FISA Court to obtain subscriber information related to phone numbers captured through court-approved FISA pen register devices, just as such information is routinely obtained in criminal investigations through 18 U.S.C. § 2703(d) or a grand jury subpoena. Section 215 of the Committee's draft legislation, however, would allow the Department to instead obtain this information simply through a pen register order issued by the FISA Court. The Department believes that this proposal would reduce unnecessary paperwork and increase the efficiency of the FISA application process without impacting the privacy or civil liberties of the American people, and the Department is eager to work with the Committee on this initiative.

Second, the Department supports section 214 of the Committee's draft legislation, which would simplify reporting requirements under section 108 of FISA. And third, the Department backs the amendment to FISA's definition of the term "agent of a foreign power" contained in section 201 of the draft legislation.

In closing, the Department welcomes the Committee's effort to reauthorize critical intelligence tools contained in the USA PATRIOT Act and to provide terrorism investigators with additional tools necessary to protect the safety and security of the American people. We look forward to working with you closely as this bill makes its way through legislative process, and I would be happy to answer any questions you may have.

STATEMENT OF VALERIE CAPRONI, GENERAL COUNSEL, FEDERAL BUREAU OF INVESTIGATION

Ms. CAPRONI. Chairman Roberts, Vice Chairman Rockefeller, members of the Committee, it's my pleasure to appear before you this morning to discuss legislation that would reauthorize many important provisions of the USA PATRIOT Act and provide important new tools to national security investigators.

Over the course of the last 7 weeks the Department of Justice has made its case for why each one of the 16 USA PATRIOT Act provisions scheduled to sunset at the end of 2005 should be made

permanent. I know that time is short this morning, so I will keep my oral statement very brief, since written testimony has been submitted.

The Department applauds this Committee for taking up legislation that would make permanent those provisions of the PATRIOT Act that fall under this Committee's jurisdiction, as well as the Lone Wolf provision enacted in section 6001(a) of the Intelligence Reform and Terrorism Prevention Act of 2004.

We are also heartened that this Committee has taken the time during these hearings to gain a good understanding of how the authorities provided for in the PATRIOT Act work in real life. Additionally, you have advanced new ideas for strengthening the Department's counterterrorism capabilities, for which we are appreciative.

We look forward to working with you closely on this bill as it makes its way through the legislative process, and I would be happy to answer any questions that you may have this morning.

Chairman ROBERTS. Members will be recognized for 5 minutes in order of their appearance.

Ms. Caproni, in June 2004, before the Senate Judiciary Committee, Principal Deputy Attorney General Rachel Brand said this—and I'm quoting.

> "In combating terrorism, prevention is key. It is not good enough to prosecute terrorist crimes after they occur. For the law enforcement officers, responsibility for staying a step ahead of the terrorists in these investigations, time is very critical. Even a brief delay can be disastrous."

Obviously everybody on this committee understands that.

> "These officers need tools that allow them to obtain information and act as quickly as possible. Administrative subpoenas are the one tool that will enable investigators to avoid any costly delays."

Ms. Caproni, is there any real question in regard to the constitutionality of administrative subpoenas?

Ms. CAPRONI. As a general matter, Chairman, no, there's no question that administrative subpoenas as an instrument are constitutional. The key is that there needs to be the opportunity for meaningful judicial review. So long as there is an opportunity for meaningful judicial review, the courts have typically upheld the administrative subpoena power.

Chairman ROBERTS. We need some examples, if you will. Can you give us some examples of how the FBI might use an administrative subpoena in an international terrorist investigation?

Ms. CAPRONI. Sure. I'll give you two. One actually happened and the other would be a hypothetical, and I think the one that actually happened has been discussed previously in hearings.

But shortly after 9/11, investigators were attempting to run down all leads, and one of their leads took them to a hotel somewhere—I think it was in Virginia. They wanted and needed, in connection with the investigation, records of who was staying at the hotel on a particular night. The hotel was not being cooperative. I'm not criticizing the hotel, but they were not being cooperative in this regard.

At that point, they didn't have an AUSA available to issue a grand jury subpoena, and even if they had, there wasn't a grand jury sitting the next day that the records could be returned to.

That would be an example where an administrative subpoena would have been an excellent tool in order to get the hotel to provide the records that the investigators needed.

To use a hypothetical example, suppose that the investigators are aware of a particular individual and they have information that the person is about to do something bad—commit a terrorist act. And through the course of their investigation they know that this person has an EZ Pass device on their car, but they don't know where the person is right now.

One set of documents that we would want to investigate would be the records of the EZ Pass device, because that may well give us a very good lead as to where the car is and where the car is going. We could use an administrative subpoena to the EZ Pass organization in order to get those records and to get them very quickly for purposes of our investigation.

So those are just two examples. I could probably sit here and come up with lots of hypothetical examples of where the need to get a record quickly exists and where needing to go to an AUSA to get a grand jury subpoena may not be the best way to go, and where an NSL is not available. In neither the EZ Pass sample nor the hotel example is an NSL an available tool.

And then the other alternative would be to go for a 215 order, and that is not going to be done in a matter of hours.

Chairman ROBERTS. Now, when Mrs. Brand testified regarding terrorism, she said we know that terrorism may be the No. 1 threat facing the nation, but espionage certainly remains a serious concern of the FBI. My question is, would the ability to use a constitutionally valid administrative subpoena in espionage investigations also provide the same kind of timely access that you are asking for to this kind of very crucial information?

Ms. CAPRONI. Administrative subpoenas are always going to be able to provide us with quick access to information. It at least is a tool that we can use to serve on the party that holds the records. It may not get us the records because there could be resistance, but it is at least the tool to start the process for getting the records.

As this Committee knows probably beyond all other committees in Congress, certainly in the Senate, espionage cases are extremely important. Through our history we have seen incredible damage done to the national security through espionage, both by virtue of our assets overseas being compromised as well as secrets that we hold within the government being compromised to other countries.

And for those reasons espionage cases are extremely important. So anything that we can do in order to get records in connection with those investigations quickly is important to the FBI.

Chairman ROBERTS. I have one other observation, but in the interest of time and with my time running out, I recognize Senator Rockefeller.

Vice Chairman ROCKEFELLER. I'm going to continue a little bit on the same track but put it differently. Do you have any examples of where FBI investigations in fact faltered even for a moment because of the lack of administrative subpoena authority? Can you give an example?

Ms. CAPRONI. I think the example with the hotel was one where it faltered for a while. We ultimately were able to get the records, and in that case it did not result in harm to the national security.

But it could have. And that's the problem with a lot of these tools; is we need the records, we need them quickly. Can we show you that because we didn't get the record a bomb went off? We cannot.

Vice Chairman ROCKEFELLER. And was that a period of several hours?

Ms. CAPRONI. I think it was several hours; that's correct.

Vice Chairman ROCKEFELLER. That can make a difference.

Ms. CAPRONI. It certainly can make a difference. It doesn't always, but it certainly can make a difference.

Vice Chairman ROCKEFELLER. Again, how many statutes—and, if you can, name some of them—confer administrative subpoena authority on the FBI Director.

Ms. CAPRONI. There are a number of them. The ones that immediately come to mind and the ones that are probably used most often are the ones that provide administrative subpoena in narcotics cases and administrative subpoenas in health care fraud and child pornography cases. Those are the ones that are used the most.

Vice Chairman ROCKEFELLER. And that we've discussed in the committee. I thank you for that.

The draft bill provides for administrative subpoenas for records. It does not provide to administrative subpoenas for testimony. Does the administration agree that the administrative subpoena authority should be limited to records and should not include testimony?

Ms. CAPRONI. I think we're prepared to discuss that. I think as a realistic matter during the course of national security investigations and terrorism investigations the likelihood for needing testimony is low. Whether it's nonexistent, I'm not prepared to say that. But it is unlikely.

Again, the real need for speed typically resolves around the need for documents. If the FBI agents need to talk to someone, they will make efforts to talk to them. If they need to compel them to come forward, which an administrative subpoena for testimony would, that would be a different issue. And up to now I have not heard a lot of complaints that that's what the agents need in order to further the investigation and they don't have that authority.

Again, there's always the possibility and the available, though not immediately, to get a grand jury subpoena and to compel the person to appear before the grand jury to provide testimony.

Vice Chairman ROCKEFELLER. I'm right, aren't I, in suggesting that National Security Letters do not have anything attached to them that gets you a subpoena?

Ms. CAPRONI. That's correct. The National Security Letter is a request for documents.

Vice Chairman ROCKEFELLER. So it would have to be the administrative subpoena authority or else it wouldn't work.

Ms. CAPRONI. To get the documents through compulsion, the administrative subpoena compels the party who receives the subpoena to provide us with the documents. The National Security Letter requests the documents.

Vice Chairman ROCKEFELLER. My final question is, what current problems exist for the FBI and the Postal Service in the requesting, receiving and carrying out of mail cover authorities, and how would establishing these authorities in statute rectify those problems?

Ms. CAPRONI. I don't want to say that there are problems between us and the Postal Service. We have a long history with the Postal Service which is a warm and cooperative relationship. Postal Inspectors sit on the Joint Terrorism Task Forces and we work very well together with the postal authorities.

However, the current regime for mail covers, as you've noted, is a regulatory regime. And under the current regs the requirement is that a request for a national security mail cover has to come from a high FBI headquarters official, and there are a limited number of individuals within the Postal Inspection Service that are then authorized to actually execute the mail cover.

Further, as it is written, it gives to the Postal Service discretion to decide whether or not to actually execute the mail cover. As a philosophical or jurisprudential matter, it is odd, to say the least, that the FBI is the agency that is charged with protecting the country from terrorist attacks and from spies, and yet our ability to use this very basic tool of a mail cover is charged to the discretion of another agency.

Vice Chairman ROCKEFELLER. Thank you. In my remaining 14 seconds, in the last year how many National Security Letter requests have not been complied with, that you can think of?

Ms. CAPRONI. Well, one ended up in litigation, and that National Security Letter has not been complied with.

Vice Chairman ROCKEFELLER. So one?

Ms. CAPRONI. I know of one. I do not know the number of how many have not been complied with. I know that there are times when we have less than quick compliance from the party on whom have served the National Security Letter on.

Vice Chairman ROCKEFELLER. I thank you, and I thank the Chairman.

Chairman ROBERTS. So basically your answer is that it is more subjective in terms of the time required. I don't know as we could put a criteria on that in terms of a timeframe, but you might want to get back to the committee with a further statement on that, as opposed to a particular incident or the number from the timeframe. Of course you already spoke to that prior to that, but it might be a little difficult to say 6 or 7 of 27, for that matter, in regards to the time.

Ms. CAPRONI. We will try to get the Committee information in terms of the speed with which we get compliance with National Security Letters.

Chairman ROBERTS. I think that would be helpful to Senator Rockefeller's question.

Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman.

Mr. Chairman, first a little bit of business. I would hope, Mr. Chairman, that Thursday's markup would be held in an open session. It seems to me that there is so much that we have to do in closed session because of the implications for national security that that's appropriate, but I don't think that's the case here.

I think this is a matter of great public concern, and I just wanted to weigh in and say I hope that Thursday's session can be done in public.

Also, Mr. Chairman, we still have not heard from the FBI on the matter of the so-called discrete inquiries that are made of libraries. I've asked for this information more than a month ago, and it certainly causes me to wonder exactly how many of these so-called discrete inquiries are made. And I've been told that we can't even get a timetable when the department will get us that information. I just want to say I remain concerned on it.

Chairman ROBERTS. Well, as the Senator knows, we are backing him up on his questions for the record, and I will take his suggestion for an open meeting under advisement.

We have had now three open meetings, but I intend to ask questions, event-oriented, that deal with classified information from the intelligence community on how the PATRIOT Act actually works. So we're going to have to go through that and make a determination. My off-the-cuff commentary is that that might be very difficult to do.

But I thank the Senator for his suggestion and he is recognized for 5 minutes.

Senator WYDEN. I thank the Chair for his thoughtfulness, and I do appreciate your consideration.

It seems to me, Ms. Caproni, the heart of your case is that you feel that it is now time to intertwine the criminal justice system and the intelligence system. In effect, what's used for criminal investigations should be used for foreign intelligence operations. And you are certainly blurring the lines here in a way that concerns me.

Foreign intelligence investigations have to be much more secretive. They don't require evidence that a crime has been committed. They are broader. Tell me what the argument is for making this dramatic shift now in public policy and sort of intertwining these two areas the way you do and essentially giving us the argument that what you use in a criminal investigation now should be used in a foreign intelligence investigation.

Ms. CAPRONI. Senator, I think I have a couple of different answers to that. First off, I don't think there's ever been a bright line nor should there have ever been a bright line between criminal on the one side and foreign intelligence/national security investigations on the other side. That to some extent, as the FISA Court of Review said, is a false dichotomy.

The reality is that many of the things that we investigate as foreign intelligence matters are also criminal conduct. Furthermore, individuals who are agents of a foreign power commit crimes. So there is inevitably a cross-over between the two notions of a foreign intelligence investigation and a criminal investigation.

The second relates to the use of tools. I don't think we're suggesting that there should be a cross-over of the tools. I think what we're suggesting is that administrative subpoena power has been available in criminal investigations for a long time, and it's available in lots of different sorts of criminal investigation. It is a great tool for investigators. It has not supplanted other tools. The reality is that grand jury subpoenas are still used in narcotics cases, in

health care fraud cases, and in child pornography cases, though administrative subpoenas are also used in the same investigations.

Criminal investigators have the opportunity to decide what is the best tool in this particular incident to get the materials that I need for this investigation. It's anomalous and odd that in national security investigations, where we're trying to protect the national security of the country, that same tool and that same ability for the investigators to look at the situation and say what's the best tool for me to use here—is the best tool for me to use to walk down the street to my friendly AUSA and say, "Hey, let's open a grand jury investigation on this," or is the best tool to use is to come to headquarters and say we need a 215 order, or is another tool a better tool.

We believe—and we have been saying this now for several years—that an administrative subpoena is a tool that we need in national security investigations.

Senator WYDEN. As I read the administrative subpoena proposal that you've made, essentially without going to a judge, an FBI field office head can basically go and ask anybody for anything, just asserting that it's constitutional and relevant to an investigation. Tell me how you would differ in terms of your assessment of it?

I mean, I can see somebody in a regional office showing up at a hospital, saying I want all the records of the patients. The hospital administrator could hand them over unless later on he wanted to challenge it in court. Tell me where the checks are in this kind of process.

Ms. CAPRONI. The checks, Senator, are the same checks that exist in other processes.

Senator WYDEN. After the fact.

Ms. CAPRONI. Well, with an administrative subpoena the check is both after the fact from a judicial standpoint but there is a before-the-fact check as well, which is agents are bound by the Attorney General guidelines in conducting their investigations. There is an attorney in every field office in this country who is responsible for making sure that agents don't go off on wild tears.

To legislate, respectfully, from the position of some agent somewhere may screw up is not how we would like to see you legislate. We put checks in place. There are judicial checks in place. This committee exercises oversight and gets to see how the FBI uses the tools that we have been provided.

We believe that from an internal perspective it would be—I can assure you that the Director would have some harsh words for the SAC who authorized an agent to serve an administrative subpoena for all records of a hospital in connection with a national security investigation. I'm not saying it's not possible that that would be the correct way to go, but I can assure you that we would have wanted to hear about it at headquarters and talked through those issues.

So I think that from the standpoint of the FBI as an organization that is steeped in the need to comply with the Constitution, we need to respect the privacy rights of individuals, I don't think an administrative subpoena from this standpoint for those investigations is any more subject to abuse than the administrative subpoenas in the other fields where we have the ability to serve administrative subpoenas.

Senator WYDEN. Thank you, Mr. Chairman.

Chairman ROBERTS. Senator Bond.

Senator BOND. Thank you, Mr. Chairman.

Ms. Caproni, I agree with you that certainly while narcotics violations, health care fraud and child pornography are critically important issues, national security should at least be treated with the same degree of power for the FBI agents.

You have said that the agents are bound by the Attorney General's guidelines and if somebody screws up there will be harsh words. Now I'm not sure harsh words will satisfy people. What other remedies are offending agents, who get off the reservation, likely to face and what is the sanction against some agent who may go on an unwarrantedly broad fishing expedition?

Ms. CAPRONI. Well, again I think in the first instance we try to prevent those unwarranted fishing expeditions.

Senator BOND. Right.

Ms. CAPRONI. Along those lines, though, to the extent we gathered up a bunch of information on individuals that had nothing to do with the national security investigation, that information would be clamped down. It wouldn't be generally available to the agents to simply go pawing through.

An agent who intentionally engages in misconduct is subject to discipline. They are subject to being investigated. They are subject to being suspended and being fired if they intentionally engage in misconduct during the course of an investigation.

Senator BOND. That's the point I wanted to raise.

With respect to administrative procedures, you've touched on it. Can you go through for us the other safeguards that are in place to protect affected U.S. citizens and legal aliens in the issuance? What are the panoply of protections to safeguard their constitutional rights?

Ms. CAPRONI. We'll start with the way the bill works right now. An administrative subpoena would have to be authorized by the special agent in charge of the individual office. That means, as a practical matter, it has to come up the chain of the FBI within the field office, which means that an attorney would look at it, and they would review it to determine whether or not it is in compliance with the Attorney General guidelines for national security investigations. That would be the first check.

The second check would be on the individual who receives the subpoena. A hospital who receives a subpoena for all of their health records is likely to move to quash it.

Senator BOND. So there is a judicial remedy before they comply? They do have access to the courts to challenge the subpoena if the recipient of the subpoena views it as unduly broad?

Ms. CAPRONI. Correct. Under the bill that this Committee is considering, the recipient could move to quash or move to modify.

Senator BOND. How frequently does that happen in other settings? In what percentage of the cases are those administrative subpoenas which the FBI is now empowered to issue challenged in court and what is the success rate of the challenge?

Ms. CAPRONI. Senator, I don't have those statistics, but it is a rare motion to quash. But that's not surprising. Motions to quash grand jury subpoenas are also rare. The reality is, these tools are

typically served on third party custodians. They will move to quash if you are going to shut them down in order for them to comply with the subpoena.

But as a general matter, investigators narrowly tailor their requests. Investigators don't like to have to paw through lots of irrelevant documents. So with a narrowly tailored request to a third party document custodian, the percentage of custodians who move to quash is very low.

Senator BOND. Do they succeed very often?

Ms. CAPRONI. Generally not.

Senator BOND. All right. You have mentioned the hotel example. Are there other examples that you can tell us in an open hearing or are there examples that you can describe to us in a closed hearing where the enhanced authorities, the broader enhanced authorities, would have been useful in the post-9/11 terrorist investigation? Any other things that come to mind or are there things that you can share with us with a different setting?

Ms. CAPRONI. I don't think there are any others that I can share in this setting. Certainly any time the materials that we need were stuff that was not available through a National Security Letter, so that we had to resort to other tools, any of those examples would be good examples of where an administrative subpoena would have been helpful.

Senator BOND. And we may have the opportunity to learn more about that in another setting.

Just very quickly, the modification in Title II, section 211, the addition of the explicit relevance requirement, how could that enhance your authorities?

Ms. CAPRONI. Senator, I don't think it enhances our authority, but it certainly clarifies the law in a way that some have objected to. So we would support the notion of clarifying that the standard to be used in a 215 order is that the materials are relevant to a national security investigation.

Senator BOND. Thank you, Mr. Chairman.

Chairman ROBERTS. Senator Feinstein.

Senator FEINSTEIN. Thanks very much, Mr. Chairman.

I'd ask that my full statement be incorporated in the record.

Chairman ROBERTS. Without objection, it is so order.

Senator FEINSTEIN. Thank you, Mr. Chairman.

[The prepared statement of Senator Feinstein follows:]

PREPARED STATEMENT OF HON. DIANNE FEINSTEIN

I thank you for holding this open hearing to discuss the Committee's draft legislation to reauthorize and amend the PATRIOT Act and to provide the executive branch with new authorities to use in the war on terror. It would be my preference to hold our mark-up on this legislation in an open forum as well and urge you to consider that course of action.

The PATRIOT Act was enacted just 45 days after the September 11, 2001 attacks after less than 1 month of Congressional debate. Congress moved quickly to provide new tools for prosecuting the war on terror, fearing that more attacks might come at any moment. As a safeguard, we built in a mechanism to force review and reconsideration of several sunset provisions.

After careful review on this Committee and on the Judiciary Committee, I am now prepared to support the reauthorization of the intelligence-related PATRIOT Act provisions. In reaching this position, I have reviewed both the implementation of the authorities by the Department of Justice and the FBI and the allegations of misuse. I have found that the implementation has been reasonable in scope and tailored to

the needs of our intelligence and law enforcement communities. Some have stated that it is only because of the sunsets placed in the PATRIOT Act that the FBI has tread lightly for now, and that abuses are more likely to occur in the future. For this reason, continued Congressional oversight will remain critically important.

I also support several provisions included in Title II of today's legislation, such as the ones extending the duration of surveillance orders and reporting requirements to Congress in order to reduce bureaucratic hurdles at the Department of Justice. It is my hope that this will allow Justice and FBI employees to spend more time conducting intelligence investigations than passing papers through the bureaucracy. Perhaps that can be a first step in much larger changes that are needed to turn the FBI into a true intelligence agency, and not a place recently described by the Inspector General as one where professional analysts are treated like clerical staff.

Finally, I support the legislation's language to add protections to Section 215 of the PATRIOT Act (the Business Records section). This section adds an explicit "relevance" standard to the law; provides useful relief from the nondisclosure provision without risking intelligence operations; requires minimization procedures to protect US Persons; and recognizes the sensitivity of library and bookseller records, gun purchases, health information, and tax forms.

I thank you, Mr. Chairman, for including these changes to the Business Records section. They respond to the concerns this committee has heard that the language was too broad, but they won't get in the way of conducting effective counterterrorism investigations. I believe this is the model that the Congress should follow: reviewing the implementation of existing law, addressing legitimate concerns, and reviewing requests for additional authorities.

In this light, I am concerned with two sections of this legislation and hope they will be removed or modified at mark-up.

Section 203 adds criminal prosecution to the definition of foreign intelligence. Supporters of this section say this language is necessary to remove forever the so-called "wall" between intelligence and law enforcement. In fact, this provision goes much further than that. This language would, in effect, eliminate the much-needed distinction between intelligence conducted under FISA and traditional law enforcement, by making law enforcement a subset of foreign intelligence.

We have heard time and time again that information sought for either intelligence or law enforcement purposes have to be shared quickly and fully to the other. Removing the wall between the two, both when requesting investigative authorities under FISA and in sharing information so gathered, was the most important achievement of the PATRIOT Act, particularly under Section 203.

The Act, however, recognized that FISA needs to remain rooted in the intelligence world and should not be used exclusively as a law enforcement tool. Intelligence is a prospective effort where any information possibly available is collected and analyzed to enhance our understanding of possible future actions. Criminal prosecution is, by definition, a backwards-looking action, where law enforcement seeks information in connection with one or more specific events. In hindsight, it is possible to say what is and what is not relevant to an investigation. Despite arguments to the contrary, there is no abiding reason why law enforcement and intelligence investigations should proceed under the same governing authorities. There is no need to lump "criminal prosecution" into the definition of foreign intelligence as this legislation would do.

In 2001, Congress struggled with the right formulation to specifically allow intelligence and law enforcement personnel to be involved in the same investigation. To that end, I worked with Attorney General Ashcroft to write the "significant standard" language, incorporated in the PATRIOT Act as Section 218. This language replaced the "primary standard" that the Justice Department had used in practice for so long. The new standard allows the FBI to use FISA authorities for law enforcement, including prosecution, so long as there is a "significant" intelligence purpose of the investigation. The FISA Court of Review commented on this specific point and found that this language is the only thing stopping the FBI from pursuing FISA warrants solely for law enforcement matters involving international terrorism. I believe this is a good thing, and thus oppose section 203 of today's legislation, which would remove this boundary between intelligence and law enforcement.

Since enactment of the "significant purpose" test I have heard not a single argument from either our law enforcement or intelligence elements that this fix did not solve the problem. In fact, Attorney General Gonzales, in his April 5, 2005 remarks on the Patriot Act had this to say about the current law: "Section 218 of the Act, in particular, helped to tear down the "wall" by eliminating the "primary purpose" requirement under FISA and replacing it with a "significant purpose" test. Under section 218, the Department may now conduct FISA surveillance or searches if for-

eign-intelligence gathering is a "significant purpose" of the surveillance or search. As a result, courts no longer need to compare the relative weight of the "foreign intelligence" and "law enforcement" purposes of a proposed surveillance or search and determine which is the primary purpose; they simply need to determine whether a significant purpose of the surveillance is to obtain foreign intelligence. The consequence is that intelligence and law enforcement personnel may share information much more freely without fear that such coordination will undermine the Department's ability to continue to gain authorization for surveillance under FISA."

I note that in its recent statement on the pending legislation, the Department of Justice supported several provisions, but provided no support for this section.

Second, I am troubled by the addition of administrative subpoenas in this legislation. I want to make clear that I am not opposed to providing the FBI and the rest of the Intelligence Community with new tools. But we should do so only where there is a clear and compelling need and suitable checks on investigative authority.

To be sure, the Bush Administration has requested administrative subpoena authority for counterterrorism many times. But that request has been for subpoena authority for the law enforcement side of the FBI, not under FISA. In fact, Director Mueller has repeatedly told me, and the Judiciary Committee, that his highest priority legislation was a Title 18 administrative subpoena for terrorism cases. I have heard no similar requests, and certainly neither the Director of Central Intelligence or his successor, the Director of National Intelligence, for this remarkable expansion of the intelligence powers granted to the FBI.

It is one thing to have administrative subpoena in the criminal or regulatory context—in fact, supporters of the criminal administrative subpoena have often argued that there are more than 300 other such subpoena now authorized by law. It is entirely different to add a sweeping new power to the intelligence arsenal.

Let me be clear—if this provision is passed into law, all of our discussion about Section 215 will be rendered superfluous, as the administrative subpoena—with no judicial supervision of its issuance—would replace the FISA business records. When the Attorney General recently told this Committee that he supported adding the "relevance" language to Section 215, I cannot imagine that he took this position with the knowledge or expectation that we would soon pass a separate law making Section 215 obsolete.

Section 213 of this bill would allow FBI officials at the field office level the authority to subpoena any "records or other materials that are relevant to an authorized investigation. . . ." This authority could be delegated to a Special Agent in Charge, with no prior approvals from any subordinate to the Attorney General, from any court, or even by a prosecutor as is done under a grand jury subpoena arrangement.

The only case where such a sweeping authority could be justified is where a field agent needs intelligence information so quickly that a FISA Court order, National Security Letter, or grand jury subpoena were impossible to obtain. Yet this legislation does not limit the use of administrative subpoenas to such exigent circumstances. Indeed, as I have said, this authority would have the effect of making FISA business records requests obsolete.

The idea of replacing the most controversial authority in the PATRIOT Act with one that doesn't even contain prior approval and can be used in basically any national security investigation is not responsible lawmaking. I urge that this committee use the mark-up to address some of these concerns.

Senator FEINSTEIN. Thank you, Mr. Chairman. The reason is because I express my concern with two sections. One of them is what is happening today on the administrative subpoena. And I'd like to speak as a member of the Judiciary Committee.

We had a hearing last year in my subcommittee, Technology and Terrorism, on Senator Kyl's bill. At that time Mr. Mueller asked for an administrative subpoena under Title 18, a criminal administrative subpoena, not under Title 50. As I understand it, the FBI has always maintained that the Title 18 criminal subpoena, not a FISA administrative subpoena, was its top legislative priority in this area. Am I correct?

Ms. CAPRONI. Senator, I believe the FBI's priority is for an administrative subpoena. The issue of whether it's under Title 50 or Title 18 I have not personally discussed with Director Mueller, but I believe we would like administrative subpoena authority.

Senator FEINSTEIN. Well, let me just say that's my recollection as a member of the Judiciary Committee, that it has always been Title 18. And I'm very concerned about this, so I just want to say I'm drafting an amendment which would replace section 213 of Senator Roberts' bill with a provision to give the FBI the criminal administrative subpoena authority it requested, with two limitations. The first is a requirement that the FBI only use this new power in circumstances for which it is needed, where there are emergency circumstances which prevent the use of existing mechanisms, such as the one you just described, and the existing mechanism, of course, would be a grand jury subpoena.

And second, a requirement that a Department of Justice Assistant U.S. Attorney sign off on this subpoena, perhaps only via telephone, but at least there is some check and balance on the use of that subpoena.

I'd like you to take that back to the FBI. I'd like to get an opinion of it. But I'm very concerned. This is the first time I have ever heard the request for a Title 50 administrative subpoena, and if there is such a request anywhere in writing by the FBI, I'd like to have it, if I might.

Ms. CAPRONI. Senator, again the FBI has been very consistent that we would like administrative subpoena authority. The issue of whether it's in Title 18 or Title 50 I don't express any opinion on.

I am prepared to address the issue of whether there should be an emergency requirement or the requirement of an AUSA signoff on it.

Senator FEINSTEIN. If you would, that would be great.

Ms. CAPRONI. As you know, those requirements do not exist in any other administrative subpoena that we currently have. And the reality is that—again to go back to my answer I believe to Senator Wyden—it's anomalous to have different standards that are applied when the FBI is conducting national security investigations, the most important investigations that we conduct, that are not present in routine criminal investigations.

In terms of an AUSA signoff, I love AUSAs—some of my best friends are AUSAs, I'm a former AUSA. So I'm not denigrating AUSAs. They are great people. However, it seems to me that asking for an AUSA to sign off takes us back to the world where the answer to terrorism was criminal prosecution. That's how you need to think. You need to think about criminal prosecution. I think it subtly sends the message to the agents who are conducting these investigations that a criminal prosecution is necessarily part of the answer here.

Again, AUSAs are great people, but it's sort of like going to a surgeon for a tummy ache. They're going to take out your appendix. They cut. AUSAs prosecute.

Senator FEINSTEIN. My time is almost up. Let me just indicate, Mr. Chairman, what my concern is.

This is a very broad power. When used directly, the individual would know about it. In this case, they would have no recourse to court. If it's used in a secondary way, not affecting the individual, such as you go to somewhere to collect data that the individual would not know, there really is no check on the power.

So you're really giving this subpoena carte blanche to go out on any kind of fishing expedition, with no necessary stricture that determines exactly how it can be used. And that's why I think some form of signoff, just as judges are duty judges and they sign off on certain things, it seems to me that the U.S. Attorney should provide that kind of a signoff, just as a guarantee. Because this is a new area.

Chairman ROBERTS. I thank the Senator for her views. We are under a rather strict time limit.

Senator Hagel.

Senator HAGEL. Mr. Chairman, thank you.

Ms. Caproni, as you have noted generally this morning, administrative subpoenas have been used and are being used. And I'd like to ask a question regarding how the administrative subpoena function in the PATRIOT Act differs, if it does, from what the FBI has used in the past regarding using the administrative subpoenas for drug enforcement.

Ms. CAPRONI. I'm sorry, you mean the administrative subpoena proposal that's in this bill?

Senator HAGEL. Yes, is there a difference? Would there be a difference?

Ms. CAPRONI. I think it would work essentially the same way, depending on how it gets delegated down into the field.

Senator HAGEL. How far down into the field—special agent in charge? Do you think that's appropriate, to push it down that far?

Ms. CAPRONI. Yes, I think it is appropriate to push it down that far, and in fact, if it wasn't pushed down to the special agents in charge of the field offices, its benefit to the Bureau will be limited. The advantage of having it pushed to the field office level is that you have, one, a high-level FBI agent, the special agent in charge, who has to sign off on it. So you have accountability and you have someone who's charged with running an office and is a member of the senior executive service. They have come a long way within the Bureau and they are charged with making sure that we conduct our investigations appropriately.

If it's not delegated down to the special agent in charge and everybody has to come back to headquarters, that again will slow things down and it will make the tool not nearly as effective to the agent in the field as it is in the other sorts of investigations—again, narcotics, health care and child pornography.

Senator HAGEL. In order to issue these subpoenas, the desired information must be relevant to the investigation. Can you explain why the relevance standard is particularly appropriate in regard to the subpoenas that we're talking about today and how that works? What are the limitations and difficulties you've had in the past, in drug enforcement, for example?

Ms. CAPRONI. Well, in drug enforcement that would be the same standard. Are the materials that you're seeking relevant to the investigation you are conducting? Relevance is a standard that agents understand. They are taught from the time they come into Quantico that they need evidence that is relevant, that it tends to prove something that's important to the investigation. So it's a concept that's familiar to them.

In certain prior provisions that were modified as part of the PATRIOT Act there was a higher standard that had to be met for certain tools. National Security Letters, for example. It used to be that you had to show specific and articulable facts that the records were relevant to an agent of a foreign power. That essentially meant that you needed to know where you were going before you got the basic tools to determine whether or not the person was an agent of a foreign power.

The PATRIOT Act reduced that to a relevance standard across all the tools, which we think is appropriate. Again, it's a standard that everyone understands. It means that you cannot simply go on a wild fishing expedition for matters that have nothing to do with the investigation that you're conducting.

Senator HAGEL. If I could go back to a general question on administrative subpoenas, you have provided this Committee here in the last few minutes with some specific examples of uses.

Focus on the potential use of this administrative subpoena for dealing with terrorists. Give the Committee a couple of examples of how you could see this would be particularly important in dealing with terrorists.

Ms. CAPRONI. The example I started with would be, we know the terrorist or we believe the terrorist is about to do something bad. We don't know exactly where he is. We want his Easy Pass records. That would be a record that is not obtainable by an NSL and to get it through a 215 order would require coming to Washington, writing up fairly detailed papers in order to get it.

Senator HAGEL. So timeliness would be one dynamic of this.

Ms. CAPRONI. Timeliness is a huge dynamic. I think the other dynamic is that as investigators work there is something to be said about being able to stand in front of the person, ask for the records. When the person says no, either I can't give them to you or I won't give them to you, to be able to come back promptly and say here's the instrument that requires you to give them to me, if you still don't want to give them to me, you have to go to court.

But that dynamic of being able to keep the investigation moving forward and get the documents and the materials that the investigator needs to continue the investigation are important. Those are important aspects of an administrative subpoena.

Senator HAGEL. Mr. Chairman, thank you.

Chairman ROBERTS. Senator Hatch.

Senator HATCH. Well, thank you, Mr. Chairman. Welcome to the Committee. We're happy to have you here again, and we appreciate the testimony you give because of your experience and background, just to mention a few things.

Now, as I understand it, as one who worked very strongly on the PATRIOT Act, it's been used very efficiently and well by the FBI, the Justice Department and other law enforcement personnel in protecting us ever since 9/11. Isn't it true that before the PATRIOT Act we were not up to speed with regard to the laws regarding international terrorism?

Ms. CAPRONI. Senator, it's certainly the case that there were many of our tools that were used in national security investigations that had not been updated to recognize the reality of a world where Internet communication was a very common way that individuals

communicate, that tradecraft required agents of foreign powers to move and change telephones very quickly. Those sorts of tools were definitely in need of update, and the PATRIOT Act did that.

Senator HATCH. How many layers of FBI hierarchy look at the use of administrative subpoenas before agents in the field use them?

Ms. CAPRONI. If this bill passes, as it's laid out, it would certainly go from a line agent to a supervisor, probably to an assistant special agent in charge, through the chief division counsel, who is a lawyer, to the special agent in charge.

Senator HATCH. So there are lots of checks.

Ms. CAPRONI. There are lots of checks.

Senator HATCH. A lot more checks then you have in general anticrime laws where the administrative subpoena is in use, right?

Ms. CAPRONI. That's correct. It is quite easy for an agent to issue an administrative subpoena. Again, this bill requires it to go up to the special agent in charge. And I would note that that is more review certainly in some offices than a grand jury subpoena gets.

When I was a brand new AUSA, I could issue a grand jury subpoena by reaching in my drawer and typing it up, and I was still wet behind the ears.

Senator HATCH. In section 211 and 213 of the proposed bill there are significant provisions for congressional oversight, including specific reporting for libraries, book sellers and others. Are there examples of terrorists using libraries for these activities?

Ms. CAPRONI. There are certainly examples of where spies have used computers that are located within libraries in order to engage in communication activities. I think we've probably provided another example of where an individual, who I guess could be considered a terrorist, posted a bomb threat on an FBI web site. That individual did that from a library computer.

So libraries are certainly used in the course of terrorist conduct.

Senator HATCH. And, of course, that illustration of the Unibomber is one that's often used as well.

Ms. CAPRONI. That's correct. The Unibomber, the book that he received through his local library was certainly a valuable piece of evidence tending to point to him as being the Unibomber during the period of time when they were trying to put together a search warrant.

Senator HATCH. So looking in libraries is not a relatively new thing.

Ms. CAPRONI. It's definitely not relatively new, but I would also say that the FBI going to libraries to get records is an extremely rare thing. It is not something we do every day. It is not common. We've tried, in response to questions from this committee as well as from other committees, to try to figure out how often and what were the circumstances that we received materials from libraries. I know Senator Wyden has an outstanding question for the record concerning the FBI's appearance in libraries to get materials.

We don't track records that way. We don't track conduct that way, although if this bill was passed and we issue subpoenas to libraries it will certainly be something that we would have to keep track of. But it's not something that we do every day—very dif-

ferent from a phone company or an ISP, where we regularly receive records from them.

Senator HATCH. In fact, you've hardly used that power so far.

Ms. CAPRONI. The 215 power?

Senator HATCH. Right.

Ms. CAPRONI. That's correct. The AG declassified the numbers, and it was less than 40.

Senator HATCH. OK. I want the FBI to get the information they need. I also want people to feel secure in conducting legal business in the country. Now, how do you assure us that administrative subpoena powers will stay in check?

Ms. CAPRONI. Again, as this bill has set out, there are several things that would keep this power in check. One is that we are still bound by the Attorney General guidelines. The subpoenas can only be issued if they are relevant to an investigation. The party receiving the subpoena, just like the recipient of any other administrative subpoena that the government has the power to issue, has the power to go to court to move to quash it. That is, the ultimate power lies in the hand of the recipient. So there's the possibility of judicial review.

This bill asks for extensive reporting of the use of it. So this committee and the other intelligence committee, if this bill passes, would have the ability to provide oversight.

Senator HATCH. Thank you. Thank you, Mr. Chairman.

Chairman ROBERTS. Senator Levin.

Senator LEVIN. Thank you, Mr. Chairman.

You indicated in response to Senator Rockefeller that there was only one case known to you where a National Security Letter was challenged in court. Can you tell us approximately how many of those NSLs have been issued? Is it in the hundreds a year?

Ms. CAPRONI. That number is classified; I'm sorry. It's a classified number. It's provided to this Committee as part of our regular reporting.

Senator LEVIN. I see. But it's not classified that you only know of one that's been challenged? That's not classified?

Ms. CAPRONI. That case is a public case. It's a public case. It's DOE versus Department of Justice or Ashcroft. I don't remember.

Senator LEVIN. Are you able to tell us in an unclassified setting whether the number of NSLs is in the hundreds or thousands a year? Can you give us a range in a public setting?

Ms. CAPRONI. I can't, but it is a very rare action to have an NSL challenged.

Senator LEVIN. No. How many are issued is the question.

Ms. CAPRONI. I can't give you that number in open session.

Senator LEVIN. Not even a range or an estimate? So we don't know if it's a hundred, a thousand, ten thousand a year?

Ms. CAPRONI. I'm sorry. I'll provide you the exact number in a classified setting.

Senator LEVIN. No problem.

On the administrative subpoena issue, currently, as I understand your testimony, there are three places where administrative subpoenas can be issued. Is that correct? There's three areas—drug enforcement——

Ms. CAPRONI. I think there are like more than 300 different types of administrative subpoenas. The ones that intersect most commonly with the FBI are in narcotics, health care fraud and child pornography cases. There are many other administrative subpoenas.

Senator LEVIN. And in those cases, in those three types of cases, where there is common intersect, right now nobody below the agent in charge, special agent in charge, inside the FBI can authorize it, but there are people in the Justice Department that can authorize it. Is that accurate, in those areas?

Ms. CAPRONI. I don't think that's accurate.

Senator LEVIN. Can anyone below a special agent in the FBI authorize it?

Ms. CAPRONI. I believe they can in narcotics cases and also in child pornography cases. I'm not positive, but I believe they can.

Senator LEVIN. In the bill that you support, nobody below the special agent in charge in the FBI could authorize it, or somebody in the Justice Department; is that correct?

Ms. CAPRONI. That's how this bill is written.

Senator LEVIN. Is that what you support?

Ms. CAPRONI. We support the notion of administrative subpoenas.

Senator LEVIN. I got that, but do you support authorizing people below the special agent in charge in the FBI to authorize an administrative subpoena?

Ms. CAPRONI. I think that under the current circumstances, where this would be a new power in a national security investigation, and where there is significant concern that the power could be misused, it is not unreasonable at this time to have the delegation go to the special agent in charge of the office.

Senator LEVIN. And nobody below?

Ms. CAPRONI. That's correct.

Senator LEVIN. Thank you.

Under FISA, is there the ability to challenge in court an order for access to records?

Ms. CAPRONI. Under Section 215 of the PATRIOT Act? It doesn't clearly state that. I think the AG has made it clear that he would support an amendment that clearly provides that a recipient of a 215 order could move to set aside or to modify the order.

Senator LEVIN. And that would be under FISA or the PATRIOT Act. You would support that?

Ms. CAPRONI. Correct.

Senator LEVIN. There's a provision—if I can find it—under section 214 of the Act—and this is the application for a trap and trace or pen register under FISA—it says there that the reason for requesting that authority cannot be solely based on First Amendment protected activity. Are we together so far, under section 214?

Ms. CAPRONI. Is it 214 of the PATRIOT Act? Yes.

Senator LEVIN. OK. Let's assume that one of the purposes violates the First Amendment rights of somebody. Would that be allowed? You've got two purposes. One is legitimate and one would violate the First Amendment rights of a citizen. Do you think we ought to tolerate that, if one of the purposes of seeking an order is to trap and trace phone calls?

Ms. CAPRONI. No agent should have, as a purpose, to violate someone's First Amendment rights. I don't think that's what that provision is driving at. The provision provides that we can't investigate a U.S. person—we can't investigate them—based solely on their First Amendment activities.

On the other hand——

Senator LEVIN. The word "solely" is what troubles me, because, given your answer of 10 seconds ago, even partly, if that's the partial motive, it would be deeply troubling.

Ms. CAPRONI. What I'm concerned about is the suggestion that the agent would be, part of his goal would be to violate the First Amendment rights of a person. That's not what this is getting at. I think what this is getting at is, if all you know about the person is First Amendment protected activity, you cannot investigate them for those reasons. You have to have something else. You have to have some other reason to believe they are engaged in this conduct.

Senator LEVIN. But if one of the reasons for investigating that person is to violate his First Amendment rights or would impinge on his First Amendment rights illegally, under the wording "solely" that would seem to be permitted. I don't think it should be, and I don't think you think it should be. And you don't think that's the purpose of the language.

Ms. CAPRONI. That's correct. I think the notion is you could have someone who is engaging in oral conduct, who, sitting by itself—if that's all you know about the person—everyone would say that's First Amendment conduct.

But if you put in other stuff that you know, then it ceases to be protected First Amendment conduct but is part of criminal conduct. Just because you are speaking doesn't mean that it's not criminal. If that's all you know, it could be First Amendment conduct that we would not use solely to conduct an investigation.

But if we know other things about them, that may color what their oral conduct is, which might otherwise be viewed as First Amendment activity. I think that's the reason that the statute is written that way—that if all you know about the person is their protected activity, you can't open an investigation on them.

Senator LEVIN. Thank you.

Chairman ROBERTS. The Senator's time has expired.

Chairman ROBERTS. Senator Bayh.

Senator BAYH. Ms. Caproni, thank you for your time and for your service to our country.

Several of my colleagues have asked questions along the lines that I'd like to pursue, so if some of this is redundant, I apologize in advance. I think we're all trying to get our hands around just how significant an impediment this has been to your ability to conduct national security investigations.

So my first question is, how many investigations have been adversely impacted by not having the advisory subpoena authority?

Ms. CAPRONI. Senator, I can't give you those numbers. It's not a number that we would collect.

Senator BAYH. How are we supposed to decide this issue if we don't have any idea whether this has been material to your ability to carry out your responsibilities? Is this all hypothetical or are there actual cases? I understand we can't discuss the specific cases,

but has this hampered you 1 percent of the time, 50 percent of the time, or has it never hampered you?

Ms. CAPRONI. It definitely does hamper us. The inability to promptly get information that we need. As I think I indicated in response to Senator Roberts, I'm not sure that we can show—and I know we can't—that because our investigation was delayed for a day or 2 days or a month or 2 months——

Senator BAYH. Well, then I guess the nature of my question would be what percentage of the investigations that you've conducted have been delayed because you don't have this authority?

Ms. CAPRONI. I can't give you percentage. I can tell you there are circumstances where, because we don't have administrative subpoena authorities and have to resort to other methods to get materials, that those investigations have been delayed.

Senator BAYH. So we have no way of knowing whether these delays are extraordinarily unlikely or whether they happen all the time. I'm just trying to get my hands around how material this is. Is this something that has just occurred once where it's been an inconvenience or a delay, or is this something that repeatedly comes up that is really hampering you in your ability to conduct these investigations frequently.

Ms. CAPRONI. The think about national security investigations and terrorism investigations is that even if it only happens once, if that once is in the wrong case, then it would have a catastrophic effect.

Senator BAYH. Well, then that's something I'd like to pursue in closed session, if in fact that's happened.

Ms. CAPRONI. Again, I'm not saying it has happened, but I'm saying that these tools are available in other circumstances where the possibility of the detrimental effect of delay are less than in a terrorism case. Again, can we show you a precise example of where, because of delay, a bomb went off? We cannot. But could it happen tomorrow? It could.

This is a tool that is readily available in other contexts. It again is an anomaly that it's not available in a national security investigation, where I think the American public would like the FBI to have the broadest range of tools available, recognizing that they need to use them responsibly.

Senator BAYH. The best I can tell here today, this is something that you are prospectively concerned about, that there may be cases crop up where this might materially hamper you. You can't really say it's happened yet, but it might, and therefore we ought to err on the side of doing more rather than less.

Ms. CAPRONI. There are examples where, because we didn't have the administrative subpoena authority, we had to go in other ways to get the material and it took longer.

Senator BAYH. How often is the administrative subpoena authority used in the criminal context, these 300-some areas where you're allowed to use it now? Is this the kind of thing that happens all the time or is it kind of a rare occurrence?

Ms. CAPRONI. It depends. I thought I saw the statistic last night, like on a year-in/year-out basis maybe 3,000 are issued a year. I'm not sure if those numbers are right, but we'll get back to you on the numbers of administrative subpoenas that are issued.

Senator BAYH. I'm just trying to get my hands around how material this is, how often this crops up and therefore how big an issue it is for you.

Ms. CAPRONI. Within a national security investigation, anytime we need a record and we don't have a willing custodian—sometimes we have willing custodians, but if we don't have a willing custodian, we need some mechanism to get the documents.

Senator BAYH. I've only got a few seconds left, so in rapid fire I'd like to follow up on something my colleagues, Senator Wyden, asked you about, where he spoke about the criminal context and now we're getting into the security/intelligence realm. And you pointed out that very often potential terrorism suspects are committing criminal acts, that kind of thing.

But then there's going to be a subset where in fact they've not committed a crime or are suspected of committing a crime. Can you give us any idea about those percentages in terms of how many are actually suspected of criminal activity and how many would be investigated for intelligence reasons that are not suspected of criminal activity?

Ms. CAPRONI. I think we may be able to get you some at least approximate numbers on that, but it would be classified.

Senator BAYH. Well, let me ask you about the mail covers. As I understand it, this is currently in the hands of the Postal Service; is that correct?

Ms. CAPRONI. That's correct.

Senator BAYH. And there's a somewhat different threshold for approving this than would be embodied in the legislation we're considering here; is that correct?

Ms. CAPRONI. I think that's right, and I think this legislation would make it mandatory, if we request it, as opposed to the current regulatory scheme, which puts it in the discretion of the Postal Inspector.

Senator BAYH. And do you have any sense about the checks that the Postal Inspector has in place to ensure that the use of this kind of authority is not misused versus the kind of checks that you would have in place to make sure that it's not misused?

Ms. CAPRONI. Well, the checks that are in place by the Postal Inspector is that they review our requests, and this to some extent varies between postal inspector and postal inspector.

Senator BAYH. Do they kind of grant your request routinely, or is it the kind of thing they really scrutinize and sort of agonize over and say, "Gee, should we really do this or not?"

Ms. CAPRONI. I have to say it varies and it also depends to some extent on postal inspector to postal inspector. They are not a rubber stamp. They believe that they have the discretion to decide, yes or no, whether they're going to proceed with the mail cover.

Senator BAYH. My time is up. I believe the courts have already ruled, have they not, that you have the ability to, for example, if someone puts their trash out on the curb, the courts have ruled you've got no privacy expectation on that; is that correct?

Ms. CAPRONI. That's correct.

Senator BAYH. Other things that you put out in the public domain are already kind of out there for private investigators and others to kind of access.

Ms. CAPRONI. You run the risk that someone's going to steal your garbage and go through it.

Senator BAYH. And that may not be the kind of thing I think is right, but that's the way it is.

Ms. CAPRONI. That's what the courts have held, that once you abandon the property to the garbage man, you've abandoned your expectation of privacy in it.

Senator BAYH. So one of the things here is whether mail should be treated as other things that are put out and once it leaves your zone of privacy.

Ms. CAPRONI. Again, there are court cases on this.

Senator BAYH. Whether you should have access to that kind of information, just as anybody else can have access to it, in some ways.

Ms. CAPRONI. Again, the courts have considered the constitutionality of mail covers, and the rationale is that mail covers are constitutional. You don't need a search warrant for them. And it's for the same general idea, that this information, which is only what's on the exterior of the envelope——

Senator BAYH. You're not going inside the mail.

Ms. CAPRONI. We're not opening the mail, no. We would need court approval to open the mail.

Senator BAYH. Thank you, ma'am.

Chairman ROBERTS. I had one other observation before we have the next panel come up, and Senator Snowe was next but she has indicated she will pass.

If administrative subpoenas are constitutional investigative tools that provide timely access to crucial information necessary to protect national security, with the significant checks and balances of the judicial review, minimization procedures and congressional oversight, I see no reason why investigations of terrorists and spies should not have the same tool provided to the investigators that they now have in regard to health care fraud, child pornography and narcotics trafficking.

Using the logic in regard to some of the questions that have been raised, you could call for more hoops—well, hoops is probably a bad word—more safeguards in those cases as well in terms of the time involved that it takes to investigate health care fraud, a child pornography case or narcotics trafficking or 335 other instances where the Federal Government does use this tool.

So, with that, we thank you for your testimony and we now ask the second panel to please come forward.

We would like to welcome the second panel: Mr. David Kris, Mr. Joe Onek, Mr. Daniel Collins, Mr. James Dempsey.

Mr. Kris, would you please proceed?

[The prepared statement of Mr. Kris follows:]

PREPARED STATEMENT OF DAVID S. KRIS

Chairman Roberts, Vice Chairman Rockefeller, and Members of the Committee: Thank you for the opportunity to testify about the Foreign Intelligence Surveillance Act (FISA) and related provisions in the Committee's draft bill. I join the Department of Justice (DOJ) in applauding the bill for addressing several difficult and important issues. Having first seen it less than a week ago, however, I have not yet mastered all of its policy implications or technical aspects. This is a very complicated area of law. Accordingly, while I pledge my continuing availability, this morning I can offer only tentative views based on a few days' consideration. Subject

to that caveat, set forth below are a few general comments, and several specific comments, on the bill. In appearing before you today, I speak only for myself, and not for any former or current employer, including DOJ and Time Warner.

In general, the Committee's draft bill authorizes and regulates several vitally important investigative tools, and I am therefore not surprised that DOJ has expressed its support. For example, Sections 101 and 203 will prevent any resurgence of the FISA "wall" separating intelligence and law enforcement. As I testified in the House last month,[1] the wall is extremely dangerous; this bill will help keep it down. Section 101 of the bill will also help ensure the government's continuing authority to conduct "roving" FISA surveillance, a tool that appears to be very valuable, and that already contains strong protections for civil liberties. Section 102 makes permanent the lone-wolf provision of FISA, which I understand DOJ strongly supports. Two other provisions of the bill, Sections 201 and 216, will likely ease administrative burdens on the FBI and DOJ by extending the duration of FISA authorization orders involving non-U.S. persons (Sections 214 and 215 may have similarly helpful effects). In an era of increasing FISA activity, this helps focus resources on cases involving U.S. persons, where civil liberties concerns are preeminent.

This bill should also enjoy substantial support from civil libertarians. For example, Section 213 would authorize administrative subpoenas that are similar to existing national security letters, but with an express provision for motions to quash. Another part of the bill, Section 211, would expand the disclosure rights of persons who receive a FISA tangible things order, and permit them to consult with counsel. Section 211 would also require special minimization procedures governing the retention and dissemination of information obtained from a tangible things order. And it would expand the government's reporting obligations.

I do have questions about certain provisions in the bill. In Sections 202 and 212, for example, I wonder whether it offers legislative solutions to problems that the executive branch ought to be able to resolve internally. I believe that Congress should change FISA only to address specific shortcomings not amenable to other remedies. However, I also think that law and policy should reflect operational experience. My own operational experience in this area, once extensive, is now 2 years out of date. I may not recognize or understand all of the problems facing government today. The Department of Justice, and you and your staff, are the real experts in this area, and I hasten to defer to your expertise. In any event, I do not think that Sections 202 and 212 threaten civil liberties.

Finally, in evaluating this bill, particularly Section 213, I urge you to consider not only whether "the government"—meaning the executive branch as a whole—should have certain investigative power, but also *which parts* of government should have power. Although I have no doubts about the constitutionality or importance of Section 213, I believe strongly that government is more effective, and civil liberties are better protected, when FBI agents and DOJ lawyers work as closely and cooperatively in national security investigations as they do in traditional criminal investigations. Until late 2002, of course, the FISA wall effectively prohibited this. As we emerge from the shadow of the wall, broad structural changes, such as the creation of a DOJ National Security Division, may be necessary to foster the cooperative model. But substantive bills like the Committee's draft should also do so where they can.

Thank you again for the opportunity to be here. The balance of this submission presents a section-by-section review of the Committee's draft bill. Again, in light of the complexity of the legal issues and the speed with which I have prepared this testimony, I emphasize the tentative nature of my comments.

SECTIONS 101, 102 AND 203

Sections 101 and 102 of the Committee's draft bill are designed to eliminate the upcoming sunset for several provisions of the USA Patriot Act,[2] and for the lone-wolf provision of last year's Intelligence Reform and Terrorism Prevention Act.[3] You and your counterparts in the House of Representatives have already heard from many witnesses on both sides of the sunset debate. By and large, I support renewal of the Patriot Act, but I would like to focus today on two important provisions: Section 218 of the Patriot Act, the "significant purpose" amendment to FISA (in connection with which I also discuss Section 203 of the Committee's bill); and Section 206 of the Patriot Act, the "roving surveillance" amendment to FISA.

1. Patriot Act Section 218: Significant Purpose

On April 28, 2005, I testified about Section 218 before the Subcommittee on Crime, Terrorism, and Homeland Security of the House Judiciary Committee.[4] My position then (as now) was that Congress should renew Section 218. I also urged the Subcommittee explicitly to endorse the reasoning and decision of the Foreign In-

telligence Surveillance Court of Review (FISCR or Court of Review) interpreting Section 218 and other provisions of FISA.[5] I testified:

> Whether or not you agree with its outcome, the Court of Review's opinion is a very sophisticated and technically sound interpretation of a complex statute. If Congress were to adopt its reasoning, it would provide guidance that is equally sophisticated and sound. That, above all, is what the country needs in this area.[6]

I maintain that view today, and I therefore renew my recommendation that Congress adopt the Court of Review's reasoning, either through explicit legislative history or a specific provision of public law.[7]

Repealing the sunset for Patriot Act Section 218 intersects with another provision of the Committee's bill, Section 203. Section 203 would amend the definition of "foreign intelligence information" to make explicit that information is "foreign intelligence information" even if it is sought for use in law enforcement efforts (such as criminal prosecution) to protect against terrorism and other foreign intelligence threats.[8] As a technical matter, I believe that Section 203 will accomplish what it is evidently meant to accomplish—that is, it will make clear Congress's intent to allow FISA searches or surveillance for the primary purpose, or even the exclusive purpose, of obtaining evidence for the prosecution of a foreign spy or terrorist.[9]

As a policy matter, however, you know from my House testimony that I do not support such an amendment for two reasons.[10] First, Section 203 of the Committee's bill would further expand governmental power at a time when the Department of Justice itself has not asked for broader authority. Second, a related point, I fear that any operational benefit from the amendment would not justify the resulting cost in uncertainty about the state of the law. As I stated at the outset, I believe that FISA should not be amended except where the amendment is genuinely necessary.[11]

If you disagree, and decide to enact Section 203 of your bill, you should consider how it will interact with Patriot Act Section 218. That is because, when read together, the two provisions could produce strange results. As explained above, Section 203 would allow the government to use FISA exclusively, not just primarily, to gather evidence for the prosecution of a foreign spy or terrorist—because Section 203 defines "foreign intelligence information" to include evidence sought for such a prosecution. Under Patriot Act Section 218, however, acquisition of "foreign intelligence information" need only be a "significant purpose" of a FISA search or surveillance. Thus, with both provisions on the books, the government might have authority to use FISA for a significant purpose of prosecuting a spy or terrorist, but with the primary purpose of something else—ranging from ordinary law enforcement, to civil debt collection, to (maybe) sheer voyeurism.[12] I myself support the status quo through renewal of Patriot Act Section 218 and adoption of the Court of Review's decision. A reasonable person might disagree and prefer Section 203 of your bill. If you both renew Section 218 and enact Section 203, I recommend that you include strong legislative history to guard against any misreading.

2. Patriot Act Section 206: Roving Surveillance

I believe the current debate over roving FISA surveillance has gone awry. Some have claimed that under Patriot Act Section 206, "[t]he government can now issue 'John Doe' roving wiretaps that fail to specify a target or a telephone, and can use wiretaps without checking that the conversations they are intercepting actually involve a target of the investigation."[13] I disagree. As I try to demonstrate below by analyzing the two statutes, FISA's rules on roving surveillance compare favorably with those in Title III,[14] its counterpart in conventional criminal law.

a. Title III

The conduct that fundamentally justifies and underlies all Title III electronic surveillance is the commission of a specified criminal offense.[15] To obtain a normal (non-roving) surveillance order under Title III, the government must identify the offense.[16] However, it need not identify or describe the person suspected of committing the offense,[17] and it need not establish a nexus between any person and the location, telephone, or other facility to be monitored. Instead, under Title III, the government establishes a nexus between the offense and the location, telephone or other facility to be monitored.[18]

By contrast, when the government obtains a roving surveillance order under Title III, these requirements are effectively reversed. For obvious reasons, in such cases, the government must identify the person committing the specified offense and whose communications are to be intercepted.[19] However, the government need not identify the facilities from which or the place where the communications are to be intercepted, and it need not establish a nexus between those facilities or places and

the specified offense.[20] Unlike ordinary Title III surveillance, roving Title III surveillance focuses on the target, not the facility being used in connection with a crime.[21]

To use Title III's roving surveillance provisions, the government must also make certain additional showings. To obtain a roving surveillance order with respect to what Title III defines as "oral communications,"[22] the government must persuade the court that it is not "practical" to establish a nexus between the underlying conduct and the location to be monitored,[23] and may not begin the monitoring until "the place where the communication is to be intercepted is ascertained."[24] With respect to what Title III defines as "wire communications"[25] or "electronic communications"[26] the government must establish probable cause that the actions of the person committing the underlying conduct "could have the effect of thwarting interception from a specified facility,"[27] and the roving surveillance order must be "limited to interception only for such time as it is reasonable to presume that the person * * * is or was reasonably proximate to the instrument through which such communication will be or was transmitted."[28]

b. FISA

FISA establishes a different regime. In a normal (non-roving) FISA case, the government must identify or describe the target of the surveillance,[29] and must also show that the target is engaged in the underlying conduct that justifies the surveillance.[30] Under FISA, of course, that underlying conduct is whatever makes the target a foreign power or an agent of a foreign power, which may (but need not always be) criminal conduct—e.g., for a U.S. person, knowing engagement in international terrorism, or for a non-U.S. person, serving as a foreign country's diplomat in the United States.[31] The government must also establish a nexus between the target and the facility to be monitored, by showing that the target is using, or about to use, the facility.[32] However, the government need not establish a nexus between the target's underlying conduct and the facility—e.g., it need not show that the facility is being used in connection with international terrorism.[33]

All of the foregoing requirements apply equally to roving FISA surveillance. The only difference between ordinary and roving FISA surveillance is that in a roving case, where the FISC "finds that the actions of the target * * * may have the effect of thwarting the identification of a specified person" who can assist the government in accomplishing the electronic surveillance, the FISC may order such assistance from "other persons" as well as the specified persons normally included in a secondary order.[34] Thus, for example, rather than issuing a secondary order directing assistance from a particular telecommunications company, the FISC can issue a generic order directing *any* telecommunications company to assist the government. The government can use this order to follow the target wherever he goes.

Or can it? As discussed above, in normal surveillance cases, both Title III and FISA require some showing of a nexus between the telephone or other facility that will be wiretapped, and either the target (under FISA)[35] or the specified criminal offense (under Title III[36] Title III eliminates that nexus requirement in roving cases—On the theory that in such cases the government cannot make the showing because it "may not know, until shortly before the communication, which telephone line will be used by the person under surveillance."[37] FISA seems to recognize this same theory, because (as amended in 2002) it requires the FISC's authorization order to specify the nature and location of each facility to be surveilled only "if known."[38] Nonetheless, FISA does not eliminate the nexus requirement: In roving cases as well as ordinary cases, it demands probable cause that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power."[39] How can the government make that showing in a roving case, where—by definition—it cannot even identify the facilities or places at the time the FISC enters its order?

In my view, the best answer lies in FISA's minimization provisions. As you know, those provisions require the Attorney General to propose, and the FISC to approve (as proposed or as modified), specific procedures "that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition * * * of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain * * * foreign intelligence information."[40] If the minimization procedures require a nexus before the government commences roving surveillance on a new facility—e.g., through observation of the target using the facility, or some other method—they ought to satisfy the requirement that each facility "is" being used or about to be used by the target before the surveillance begins.[41]

In practical effect, instead of finding probable cause with respect to particular facilities not yet known, the FISC finds that there necessarily *will be* probable cause under the minimization procedures it imposes as part of its authorization order. This is roughly equivalent to Title III's provisions eschewing a formal nexus requirement to any particular facility but requiring that roving surveillance of wire or electronic communications be "limited to interception only for such time as it is reasonable to presume that the [target] * * * is or was reasonably proximate to the instrument through which such communication will be or was transmitted."[42] It is broader than Title III in that it could be satisfied by something other than proximity to a communications instrument (e.g., where the target uses one facility to communicate through another, remote facility), but it is narrower in that mere proximity is not necessarily sufficient (e.g., where the target walks past a pay phone but does not use it).

c. Conclusion

In light of the foregoing, if I am reading the statute correctly, it is ironic that civil libertarians have raised concerns about "John Doe" roving FISA orders. Every provision in FISA that applies to ordinary surveillance applies to roving surveillance; there are no exceptions. One of those FISA provisions requires probable cause that the target is using, or is about to use, "each" facility subjected to surveillance. As a question of roving surveillance compared to ordinary surveillance, you literally could not ask for more (other than, perhaps, what I describe in the next paragraph).[43]

There is one amendment to FISA that might address some of the concerns raised by civil libertarians without unduly inhibiting the government. In essence, FISA roving surveillance resembles a highly circumscribed form of emergency surveillance. In a typical emergency surveillance case, the government determines unilaterally whether it can satisfy *all* of the provisions of FISA (subject to later ratification by the FISC).[44] In a roving case, the government determines unilaterally only whether it can satisfy the nexus requirement (the FISC determines in advance all other issues, such as whether the target is an agent of a foreign power). As in emergency cases, therefore, it may be worth considering whether the government should be required to submit to the FISC, within some reasonable time after commencing roving surveillance on a new facility, a description of the information upon which it relied to do so. Such a provision would read something like this:

Sec. XXX. Report in Roving Surveillance Cases

Subsection 105(c)(2) of the Foreign Intelligence Surveillance Act (50 U.S.C. § 1805(c)(2)) is amended by adding the following new subsection (E):

> that, in any case in which the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person as described in subsection (c)(2)(B) of this section, and in which the electronic surveillance is directed against any facility or place the nature and location of which is not specified in the Court's order under subsection (c)(1)(B) of this section, the applicant or another Federal officer promptly report to the Court the information relied upon determine that the target of the surveillance was using, or was about to use, such facility or place.

This amendment should assuage fears about FISA roving surveillance by requiring judicial review, albeit shortly after the fact. Obviously, if the FISC found the government's submission unsatisfactory, it could terminate surveillance on the new facility (on the theory that the government had not complied with the minimization procedures).

I do not know what the Department of Justice will say in response to this amendment, but it seems reasonable to me in concept. If the word "promptly" is unsatisfactory for any reason—I borrowed it from 50 U.S.C. § 1824(c)(2)(E), the provision requiring the government to file a return following execution of a physical search—a fixed period (3 days, 7 days, 10 days), or a "reasonable period to be determined by the Court," could be used instead.

SECTIONS 201 & 216

Section 201 of the Committee's bill would amend FISA's definition of "agent of a foreign power" in 50 U.S.C. § 1801(b)(1)(A). As you know, 50 U.S.C. § 1801(b)(1)(A) currently applies to any non-U.S. person who "acts in the United States as * * * a member of" a group engaged in international terrorism or activities in preparation therefor.[45] Another provision, 50 U.S.C. § 1801(b)(2)(E), currently applies to any person (including a U.S. person) who "knowingly aids or abets any person in the con-

duct of," or "knowingly conspires with any person to engage in," sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power.[46] Section 201 of the bill would add to 50 U.S.C. § 1801(b)(1)(A) the aiding-and-abetting and conspiracy language from 50 U.S.C. § 1801(b)(2)(E).

This proposal would not change FISA's definitions in any substantive way. It would neither expand nor contract the reach of FISA, because anyone who would fall under Section 201 of the bill is already covered by 50 U.S.C. § 1801(b)(2)(E). The principal effect of Section 201 would be to extend the duration of FISA search or surveillance orders applicable to such persons (if they are not U.S. persons), from 90 days, to an initial order of 120 days and renewal orders of 1 year each.[47] A subsidiary effect would be to eliminate FISA's civil damages remedy for such persons.[48]

As a policy matter, Section 201 seems reasonable. If longer periods of surveillance and search authority are appropriate for non-U.S. persons who are "members" of groups engaged in international terrorism or activities in preparation therefor,[49] then they seem tolerable for non-U.S. persons who knowingly aid and abet or conspire to engage in sabotage, international terrorism, or activities in preparation therefor. In keeping with my basic view that FISA should be amended only when necessary, however, I would defer to the Department of Justice on whether Section 201 of the bill would in fact ease a burden—by reducing the number of applications that must be filed—or otherwise solve a real problem in the administration of the statute.

Section 216 is a related provision that specifically amends the duration provisions of FISA. Under Section 216, FISA electronic surveillance and physical searches targeting non-U.S. persons who are agents of foreign powers could be conducted for an initial period of 120 days and for renewal periods of 1 year. This would change current law, under which those longer authorization periods apply only to officers or employees of foreign powers, and to members of international terrorist groups.[50] If Section 216 is enacted, Section 201 becomes superfluous (except for its effect on FISA's civil damages remedy as discussed above). (Of course, there is nothing wrong with including both provisions in the bill at this stage of the legislative process.) Section 216 would also extend from 90 days to 1 year the initial and renewal authorization periods for FISA pen-trap surveillance where the applicant certifies that the "information likely to be obtained is foreign intelligence information not concerning a United States person."

SECTION 202

Section 202 of the bill would amend FISA's definition of "contents"[51] essentially to conform to the definition of the same term in Title III.[52] I think I understand the motivation for this amendment, but I question the need for it.

Since its enactment in 1978, FISA has allowed the government to seek, and the FISC to issue, orders authorizing pen-trap surveillance. For the first 20 years of the statute's existence, however, the government could do so under FISA only by satisfying the requirements for a full-content "electronic surveillance" order.[53] In 1998, Congress amended FISA to allow the government to obtain pen-trap orders under a different, and less demanding, set of standards.[54]

FISA's 1998 provisions define the terms "pen register" and "trap and trace device" by reference to the pen-trap provisions applicable in criminal investigations.[55] Under the criminal provisions, a pen register is a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.[56]

Reduced to its essentials, this definition means that a pen register is supposed to detect the destination of outbound communications from a monitored telephone or other facility, without detecting the contents of the communication being sent.[57] A pen register on your telephone can identify whose number you call, but not what you say if someone answers.

A trap and trace device is the reciprocal of a pen register: It is supposed to detect the source of inbound communications to a monitored facility. Thus, a trap and trace on your telephone can identify whose telephone number called you, but not what you say. As a technical matter, a trap and trace device defined to be a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling informa-

tion reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.[58] Since 2001, a pen register and a trap and trace device may either be a "device" or a "process," which includes software as well as hardware methods of gathering information.[59]

Typically, pen register orders are used to obtain the numbers being dialed from a targeted telephone number, and trap and trace orders obtain the numbers of telephones making calls to a targeted number.[60] Under amendments enacted in the Patriot Act, however, neither FISA nor the criminal pen-trap statute is limited to telephone numbers. Those statutes may now be used to obtain any "dialing, routing, addressing, or signaling information" that identifies the destination or source of an electronic communication, including email and Internet communications.[61] But a pen-trap order may not be used to obtain the "contents of any communication."[62]

Although FISA itself defines the term "contents," that definition does not govern FISA pen-trap surveillance.[63] Indeed, if it did apply, the statute would effectively forbid what it authorizes, because FISA defines "contents" to include "any information concerning the identity of the parties to [a] communication or the existence * * * of that communication"[64]—a standard that clearly includes the routing and addressing information acquired by a pen-trap.

This, I believe, is the concern that underlies Section 202 of the Committee's bill: A concern that FISA's broad definition of "contents" somehow calls into question the validity of FISA pen-trap surveillance.[65] I believe the concern is misplaced for two reasons.[66]

First, FISA's pen-trap provisions clearly take their definition of "contents" from Title III[67] which (as noted above) defines the term more narrowly than FISA to mean "any information concerning the substance, purport, or meaning of [a] communication,"[68] but does not include information concerning the identity of the parties or the existence of the communication. Thus, a FISA pen-trap order allows acquisition of routing and addressing information that is not "contents" as defined by Title III, even if such information is "contents" as defined by FISA. Put another way, having narrowed Title III's definition of "contents" in 1986,[69] and cross-referenced the narrower definition in FISA's pen-trap provisions, you need not amend FISA's definition of "contents" today.

Second, FISA's pen-trap provisions, and their incorporation of Title III's narrow definition of "contents," do not conflict with FISA's electronic surveillance provisions and their broad definition of "contents." On the contrary, FISA authorizes pen-trap surveillance "[n]otwithstanding any other provision of law" and "in addition to the authority" granted to conduct electronic surveillance.[70] Thus, FISA pen-trap surveillance remains lawful, and there is no need for any change to FISA's definition of "contents."

In sum, FISA seems clearly to authorize pen-trap surveillance without a full-blown "electronic surveillance" order issued under 50 U.S.C. § 1805. The government has in fact been conducting FISA pen-trap surveillance for many years. If agents or others in the executive branch remain concerned, perhaps it highlights the need for more training and outreach efforts. But I am not aware of any statutory problem in need of repair.

SECTION 211

Section 211 amends FISA's "tangible things" provisions in four ways. First, it makes two changes to the language of 50 U.S.C. § 1861(a)(1). As amended by Section 211, 50 U.S.C. § 1861(a)(1) would provide (with deleted text in *strikeout* and added text in redline):

> The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) *for* relevant to an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, *provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution*.

I have no objection to the first change—replacing "for" with "relevant to."[71] And in view of the First Amendment provision that remains in 50 U.S.C. § 1861(2)(B),[72] I have no objection to the Committee's deletion of what amounts to a redundant First Amendment provision from Section 1861(a)(1).

Second, Section 211 would change the non-disclosure provision in the tangible things statute. Today, that provision states simply that "[n]o person shall disclose

to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section."[73] Section 211 would add several exceptions to this general prohibition, including disclosure to "an attorney to obtain legal advice with respect to the production of things in response to the order," and "other persons as permitted by" the FBI Director or his designee. Recipients of disclosure are subject to the same general non-disclosure obligations and must be so advised by the person making the disclosure to them.

These changes seem to be motivated by (and reasonable in light of) *Doe* v. *Ashcroft*,[74] which struck down on First Amendment grounds a similar non-disclosure provision in one of the national security letter statutes.[75] The court in *Doe* recognized that "the Government's interest in protecting the integrity and efficacy of international terrorism and counterintelligence investigations is a compelling one," and that non-disclosure rules further that interest.[76] But the court found that the "categorical, perpetual, and automatic ban on disclosure is not a narrowly tailored means to advance those legitimate public interests."[77]

I don't know whether *Doe* was correctly decided—I believe the government has appealed—but it seems reasonable in any event to consider additional exceptions to the non-disclosure rules in FISA's tangible things provisions. Of course, any exception creates some risk—disclosure to a lawyer could be dangerous, as illustrated by the recent prosecution of Lynne Stewart—but there is no way to keep the orders absolutely secret. More importantly, I am very sympathetic to persons who receive these strange-looking papers from the FISA Court by way of the FBI. I know the FISA statute pretty well, but if I someone handed me a tangible things order, I'd want to consult with a lawyer before responding.[78]

An additional disclosure exception, not presently in Section 211 of the Committee's bill, may be worth considering. One of the concerns in *Doe* was the unlimited duration of the ban on disclosure. That may seem a marginal concern, but under the First Amendment, concerns at the margin of a statute's application can have far-reaching consequences.[79] I think the problem is solved, however, if the ban on disclosure endures only so long as the underlying application and order remain properly classified under the ordinary rules governing classification.[80] There should be no First Amendment problem with requiring recipients of properly classified information generally to keep it secret.[81]

Third, Section 211 would direct the Attorney General to adopt "minimization procedures governing the [FBI's] retention and dissemination" of tangible things. As a policy matter, this requirement is unobjectionable—indeed, I support the use of minimization procedures as important safeguards for civil liberties. I do, however, have a few, minor technical concerns. First of all, as far as I can tell, the "minimization procedures" mentioned here would not be reviewed and approved by the FISC. Thus, they are not "minimization procedures" as that term is used elsewhere in FISA.[82] If that is correct, the provision may not be necessary, at least as far as U.S. persons are concerned. Under Executive Order 12333, "[a]gencies within the Intelligence Community are authorized to collect, retain or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency involved and approved by the Attorney General."[83] If the provision is to remain in the statute, and these "minimization procedures" are not meant to be reviewed by the FISC, a different term should be used to avoid confusion.

Fourth and finally, Section 211 would expand the government's reporting obligations to include the total number of tangible things orders granted, and the total number of them directed at libraries and certain other specified establishments. This seems reasonable enough, and I defer to the Department of Justice, which has recently revealed similar statistics in public testimony.[84]

SECTION 212

Section 212 amends FISA to direct the United States Postal Service to comply with a request for a mail cover from a designated official of the FBI. As far as I can tell, Section 212 codifies many of the provisions now set out at 39 CFR § 233.3, and changes certain of them.[85] Normally, I would say that Section 212 presents a legislative solution to a sub-legislative problem, and that concerns about the mail cover regulations should be taken up by the FBI with the Postal Service. However, if—as I understand may be the case—sub-legislative remedies have been exhausted,[86] a statutory fix becomes more plausible. From a civil liberties perspective, Section 212 also has the advantage of requiring Congressional oversight of the use of national security mail covers.

Under the current postal regulations, the FBI can get a mail cover by asking the Postal Service. A mail cover is available to "[p]rotect national security," a term that

is defined to include most of the threats specified in the first half of FISA's definition of "foreign intelligence information."[87] To obtain a mail cover, a "law enforcement agency," which is defined to include "any authority of the Federal Government * * * one of whose functions is to * * * protect the national security,"[88] submits a written request (or when time is of the essence, an oral request[89]) to the Chief Postal Inspector or his designee with "reasonable grounds to demonstrate the mail cover is necessary to * * * Protect the national security."[90] In national security cases, a mail cover can remain in effect for 120 days, and longer with the approval of certain Postal Service officials.[91] A national security mail cover must be approved personally by the head of the agency requesting it, or by a single designee at the requesting agency's headquarters.[92]

I can understand why the FBI might chafe at certain of these requirements—particularly the one concerning high-level approval of any national security request, and the fact that compliance with a request is not mandatory. In my view, this sort of inter-agency dispute is usually best resolved within the Executive Branch.[93] Were it not for the fact that the Attorney General had personally raised this issue with the Postmaster General more than 6 months ago, I would be very skeptical of Section 212. As it is, I can understand DOJ's desire to seek the Committee's aid. I note with interest the Department's views letter of May 18, 2005, in which it expresses support for Section 212, and I assume (in accord with OMB Circular A–19) that the Administration does not object to that expression of support. Perhaps the possibility of a legislative amendment will concentrate the Postal Service's mind and cause it to reconsider.

SECTION 213

Section 213 of the Committee's bill would allow certain designated FBI officials to issue administrative subpoenas in the context of national security investigations authorized under Executive Order 12333[94] and not premised solely on First Amendment activities. It allows enforcement of such a subpoena by the Attorney General through the FISC, and also provides for motions to quash filed in the FISC or in the recipient's local United States District Court. Proceedings in courts other than the FISC are to be closed and subject to nondisclosure rules, and the government may submit materials to such courts *ex parte* and *in camera*. The Director of the FBI is directed to establish regulations for the implementation of the subpoena provisions, and the Attorney General is directed to establish minimization procedures governing retention and dissemination of information obtained by subpoena. There is a provision for congressional oversight through the Intelligence Committees.

The government needs the power to compel production of documents and other materials in national security investigations, and administrative subpoenas are one important way to grant such power. From a civil liberties standpoint, Section 213 is, if anything, an improvement over current law. Unlike the current version of FISA's tangible things provisions,[95] Section 213 provides expressly for disclosure to an attorney. Moreover, unlike even the version of the tangible things provisions proposed by Section 211 of the Committee's bill, Section 213 provides for judicial review of a subpoena upon a motion to quash filed by the recipient. It allows private litigants access to the FISC, which may be viewed by civil libertarians as a good thing regardless of what is litigated. There are now several administrative subpoena provisions on the books for use in investigations pertaining to such things as health care fraud, child sexual abuse, and threats against protected persons,[96] as well as drug cases.[97] Thousands of administrative subpoenas have been issued in these kinds of cases.[98] Administrative subpoenas in national security cases, with the same or similar protections—including authorization for motions to quash—seem unobjectionable by comparison.

I have two other observations about Section 213. First, I am concerned about the invitation to private litigants to file motions in the FISC. This is not so much a philosophical concern as a pragmatic one. If thousands of subpoenas are issued, several motions to quash may be filed.[99] As far as I know, the FISC is simply not equipped to handle that kind of litigation. Indeed, the FISC is not really equipped to handle any litigation involving private parties—it has no publicly accessible space, and a relatively small staff. To be sure, these logistical obstacles could be overcome, but only by changing the FISC's nature and focus. With the dramatic increases in FISA activity over the past few years, I think the FISC should remain centered on its core function of reviewing applications. If the recent statistics revealing substantial numbers of denials and modifications of FISA applications are any guide, the FISC has been doing a careful job. I would not lightly open the FISC to adversary proceedings, particularly over something like an administrative subpoena. But I have no similar objection to motions to quash filed in ordinary district courts, as long as

the government is prepared to assume the risk of a leak. And ultimately, I largely defer to the Department of Justice with respect to what is workable here, at least in the first instance.

My second concern arises because Section 213 grants administrative subpoena power to the Director of the FBI, and orders the Director to establish regulations for the use of such subpoenas. I think the authority should be granted to the Attorney General, who may delegate (and in some other cases has delegated[100]) the authority to the Director. This may seem a trivial point—and in many respects it is—but I believe it relates to a broader and vitally important concern. I think it may be helpful to the Committee if I lay out that broader concern, using Section 213 as an illustration.

As the Committee is aware, the executive branch is now considering whether and how to restructure the government to deal with domestic counterintelligence matters. Spurred by the 9-11 Commission Report, and the more recent WMD Commission Report, some have suggested splitting the FBI to create an American version of MI-5—that is, a domestic counterintelligence agency separate from Federal law enforcement. The FBI obviously opposes that idea. I also oppose creating an American MI-5, primarily because I think such a major change would take years to bear fruit, and would create chaos in the interim. Unfortunately, our adversaries will not let us call a time-out while we restructure.

In my view, the more promising approach is to mandate significantly increased coordination between the FBI and DOJ prosecutors and other lawyers. Such coordination should, in my view, be required in individual cases and investigations, in national-level programs, and also in policymaking (both intra- and inter-agency). As I explained last month in my testimony before the House,[101] bringing agents and lawyers together would make the Department and the FBI more efficient and effective, and would also enhance protection of civil liberties. It would do this by taking advantage of the DOJ/FBI culture and training that have been in effect for many years in all investigative areas except national security. Agents and lawyers working together produce better results than either group working alone.

In keeping with this view, I support legislative measures that tend to unite agents and lawyers in national security investigations. Section 213 will not do that because, like the current national security letter statutes, it allows the FBI to take investigative action unilaterally. It thus stands in contrast to grand jury subpoenas, which cannot be issued without the involvement of prosecutors. I believe Section 213 should encourage cooperation between agents and lawyers by requiring lawyers' involvement, or at least by giving the Attorney General the option to do so. The Attorney General controls both DOJ proper and the FBI, and he may therefore decide to delegate administrative subpoena power directly to the FBI. On the other hand, particularly if DOJ creates a National Security Division, he might delegate the power to the head of that division, and/or to specially designated Assistant U.S. Attorneys in the field. I recommend that Section 213 be changed to grant administrative subpoena authority to the Attorney General.

SECTION 214

Section 214 would eliminate the current requirement that the Department of Justice report to Congress on the number of cases in which FISA information has been authorized for use in criminal cases.[102] The obligation to report authorizations for use of FISA information at trial would remain.[103] If, as I hope, this provision reflects a vastly expanded administrative burden arising from vastly expanded sharing of intelligence information with law enforcement officials, then I take it as a very promising sign that dots are being connected.

SECTION 215

Section 215 would allow the government to obtain subscriber information, of the sort normally acquired by a FISA tangible things order, as part of FISA pen-trap surveillance. Thus, for example, instead of obtaining only the telephone numbers called by a monitored telephone, the government could get the telephone numbers and the names, addresses, length of service, and other information about the subscribers to those telephone numbers. This appears to be patterned after 18 U.S.C. § 2703(c)(2). This seems like a reasonable effort to spare the government the need to file two applications instead of one, but again I would defer in the first instance to the Department of Justice on the question whether Section 215 would in fact remove a real burden. If Section 215 is desirable, I would also consider whether DOJ wants similar authority for FISA "electronic surveillance" orders issued under 50 U.S.C. § 1805.

ENDNOTES

1. Written Testimony of David S. Kris before the House Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security (April 28, 2005) (hereinafter Kris House Testimony). I have, of course, made that testimony available to your staff. As of this writing, it is also available at *http://judiciary.house.gov/media/pdfs/kris042805.pdf.*

2. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act or Patriot Act), Pub. L. No. 107–56, 115 Stat. 272 (Oct. 26, 2001). Section 224 of the Patriot Act provides:

> (a) IN GENERAL.—Except as provided in subsection (b), this title and the amendments made by this title (other than sections 203(a), 203(c), 205, 208, 210, 211, 213, 216, 219, 221, and 222, and the amendments made by those sections) shall cease to have effect on December 31, 2005.
>
> (b) EXCEPTION.—With respect to any particular foreign intelligence investigation that began before the date on which the provisions referred to in subsection (a) cease to have effect, or with respect to any particular offense or potential offense that began or occurred before the date on which such provisions cease to have effect, such provisions shall continue in effect.

115 Stat. 295.

3. Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. No. 108–458, 118 Stat. 3638 (Dec. 17, 2004). Section 6001 of the IRTPA provides:

> (a) IN GENERAL.—Section 101(b)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801(b)(1)) is amended by adding at the end the following new subparagraph:
>
> "(C) engages in international terrorism or activities in preparation therefore; or".
>
> (b) SUNSET.—The amendment made by subsection (a) shall be subject to the sunset provision in section 224 of Public Law 107–56 (115 Stat. 295), including the exception provided in subsection (b) of such section 224.

118 Stat. 3742.

4. See Kris House Testimony.

5. *In re Sealed Case*, 310 F.3d 717 (FISCR 2002).

6. Kris House Testimony at 13.

7. Your legislative staff and the Department of Justice's Offices of Legislative Affairs and Legal Counsel would be better equipped than I am to determine the best way for Congress to express its endorsement of the Court of Review's decision. With some Justices and judges increasingly wary of legislative history, however, an enacted provision of public law may be more authoritative than even the clearest committee report or floor statement. See, *e.g., Shannon* v. *United States*, 512 U.S. 573, 583 (1994) (citing cases and noting that "Members of this Court have expressed differing views regarding the role that legislative history should play in statutory interpretation").

8. Under 50 U.S.C. § 1801(e), as amended by Section 203 of the Committee's bill, the term "foreign intelligence information" would be defined as follows (with Section 203's proposed language in redline):

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect (including protection by use of law enforcement methods such, as criminal prosecution) against—
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) 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 defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.

9. In my House testimony last month, I stated:

> If you decide that you *want* to expand DOD's authority along these lines, and remove any statutory doubt, you should amend the definition of "foreign intelligence information" by adding the phrase "including protection against the foregoing using law enforcement methods, such as criminal prosecution," immediately after 50 U.S.C. § 1801(e)(1)(C).

Kris House Testimony at note 91 (emphasis in original). Section 203 of the bill uses almost 18 identical language in a slightly different place in the definition. Pro-

fessor Richard Seamon, a thoughtful academic commentator in this area, has recommended a similar approach. See Richard Seamon and William Gardner, *The Patriot Act and the Wall Between Intelligence and Law Enforcement*, 28 Harv. Journal on Law and Pub. Policy 319, 458–459 (Spring 2005) (recommending an amendment to 50 U.S.C. § 1801(e)(1) to provide that foreign intelligence information means "information that relates to, and if concerning a United States person is necessary to, the ability of the United States, by law-enforcement or other lawful means, to protect against" specified threats).

For a detailed explanation of why and how this sort of amendment would function, see Kris House Testimony at 1–4, 9–12.

10. See Kris House Testimony at 12–14 & n.90.

11. I know at least one very intelligent person who disagrees. See Letter from Professor Richard Seamon to Chairman Howard Coble, House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security (May 4, 2005).

12. A full explanation for why this is the case appears on pages 9–12 of my House testimony last month. Here is an abbreviated explanation: The Court of Review interpreted Section 218 as codifying the "false dichotomy" between law enforcement methods and all other methods of protecting national security. It explained: "The government heroically tries to give [Section 218] a wholly benign interpretation. It concedes that 'the *significant purpose* amendment recognizes the *existence* of the dichotomy between foreign intelligence and law enforcement,' but it contends that 'it cannot be said to recognize (or approve) its *legitimacy*.' Supp. Br. of U.S. at 25 (emphasis in original). We are not persuaded." *In re Sealed Case*, 310 F.3d at 734–735. On that basis, the Court of Review read Section 218 to permit FISA searches and surveillance primarily for law enforcement methods of protecting national security (id. at 734):

> as a matter of straightforward logic, if a FISA application can be granted even if 'foreign intelligence' is only a significant—not a primary—purpose, another purpose can be primary. One other legitimate purpose that could exist is to prosecute a target for a foreign intelligence crime.

Section 203 of the Committee's bill would eliminate the false dichotomy, and so also the premise of the Court of Review's interpretation of Section 218. To paraphrase from the block quote above, if the "foreign intelligence" purpose now *includes* the purpose to prosecute a target for a foreign intelligence crime (because of Section 203), then the "other purpose" that can be primary under Patriot Act Section 218 would have to be something different than prosecuting a target for a foreign intelligence crime—and indeed, different than anything that protects national security. Allowing FISA to be used primarily for something other than a "foreign intelligence" purpose (once "foreign intelligence" has been defined to include prosecution) seems unnecessary and unwise.

13. Testimony of Gregory T. Nojeim, Associate Director and Chief Legislative Counsel Washington Legislative Office, American Civil Liberties Union, before the Subcommittee on Crime, Terrorism and Homeland Security of the House Judiciary Committee (April 28, 2005) (available at *http://judiciary.house.gov/media/pdfs/nojeim042805.pdf)*

14. 18 U.S.C. §§ 2510–2522.

15. A Title III application must contain "details as to the particular offense that has been, is being, or is about to be committed." 18 U.S.C. § 2518(1)(b)(i). To grant the application, the court must find "probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter." 18 U.S.C. § 2518(3)(a). These provisions apply to all Title III cases, roving and non-roving.

16. See note 15, *supra*.

17. A Title III application must include "the identity of the person, *if known*, committing the [specified] offense and whose communications are to be intercepted." 18 U.S.C. § 2518(1)(b)(iv) (emphasis added). To grant the application, the court must find probable cause that "*an individual* is committing, has committed, or is about to commit a particular [specified] offense." 18 U.S.C. § 2518(3)(a) (emphasis added). In keeping with these provisions, the Supreme Court has held that "when there is probable cause to believe that a particular telephone is being used to commit an offense but no particular person is identifiable, a [non-roving] wire interception order may, nevertheless, properly issue under the statute." *United States* v. *Kahn*, 415 U.S. 143, 157 (1974).

18. A Title III application in a non-roving case must include "a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted." 18 U.S.C. § 2518(1)(b)(ii). To grant the application, the court must find probable cause either (1) that "the facilities from which,

or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of [the specified] offense," or (2) that those facilities or places are "leased to, listed in the name of, or commonly used by [the] person" committing the specified offense. 18 U.S.C. § 2518(3)(d). However, the Department of Justice has publicly revealed that "[for prudential reasons," it is "often cautious about using the 'listed, leased, or commonly used' provision of Title III absent evidence that the facility is in fact being used in connection with the predicate offense." Supplemental Brief for the United States in *In re Sealed Case*, 310 F.3d 717 (FISCR 2002), at 18 n.6.

19. To obtain Title III roving surveillance authority for oral communications, the government must "identif[y] the person committing the offense and whose communications are to be intercepted." 18 U.S.C. § 2518(11)(a)(ii). To obtain Title III roving surveillance authority for wire and electronic communications, the government must "identif[y] the person believed to be committing the offense and whose communications are to be intercepted." 18 U.S.C. § 2518(11)(b)(ii).

20. Under 18 U.S.C. § 2518(11), the requirements of 18 U.S.C. §§ 2518(1)(b)(ii) and (3)(d), discussed in note 18, *supra*, "do not apply" if the government meets the other requirements for Title III roving surveillance of oral, wire, or electronic communications.

21. Here is the description of roving Title III surveillance authority from the United States Attorneys' Manual (§ 9–7.111):

> Pursuant to 18 U.S.C. § 2518(11)(a) and (b), the government may obtain authorization to intercept wire, oral, and electronic communications of specifically named subjects without specifying with particularity the premises within, or the facilities over which, the communications will be intercepted. (Such authorization is commonly referred to as "roving" authorization.) As to the interception of oral communications, the government may seek authorization without specifying the location(s) of the interception when it can be shown that it is not practical to do so. See *United States* v. *Bianco*, 998 F.2d 1112 (2d Cir. 1993), cert. denied, 114 S. Ct. 1644 (1994); *United States* v. *Orena*, 883 F. Supp. 849 (E.D.N.Y. 1995). An application for the interception of wire and electronic communications of specifically named subjects may be made without specifying the facility or facilities over which the communications will be intercepted when it can be shown that the subject or subjects of the interception have demonstrated a purpose to thwart interception by changing facilities. See *United States* v. *Gaytan*, 74 F.3d 545 (5th Cir. 1996); *United States* v. *Petti*, 973 F.2d 1441 (9th Cir. 1992), cert. denied, 113 S. Ct. 1859 (1993); *United States* v. *Villegas*, 1993 WL 535013 (S.D.N.Y. December 22, 1993).

22. Under Title III, the term "oral communication" means "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication." 18 U.S.C. § 2510(4). Oral communications would be intercepted by, e. g. , a concealed microphone.

23. 18 U.S.C. § 2518(11)(a). Section 2518(11)(a) provides:

The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if—

(a) in the case of an application with respect to the interception of an oral communication—

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(ii) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

(iii) the judge finds that such specification is not practical.

24. 18 U.S.C. § 2518(12). The legislative history of this provision explains with respect to this "ascertainment" language:

> Proposed subsection 2518(12) of title 18 provides * * * that where the Federal Government has been successful in obtaining a relaxed specificity order, it cannot begin the interception until the facilities or place from which the communication is to be intercepted is ascertained by the person implementing the interception order. In other words, the actual interception could not begin until the suspect begins or evidences an intention to begin a conversation. * * * This provision puts the burden on the investigation agency to ascertain when the interception is to take place.

S. Rep. No. 99–541, 99th Cong., 2d Sess. 32 (Oct. 17, 1986) (hereinafter ECPA Senate Report).

25. Under Title III, the term "wire communication" means "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce." 18 U.S.C. § 2510(1). Under Title III, a telephone call is a wire communication.

26. Under Title III, the term "electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—(A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds." 18 U.S.C. § 2510(12). Under Title III, an electronic mail message is an electronic communication.

22 27. 18 U.S.C. § 2518(11)(b)(ii)–(iii). Section 2518(11) provides:

The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if—

* * * *

(b) in the case of an application with respect to a wire or electronic communication—

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General; the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility;

(iii) the judge finds that such showing has been adequately made; and

(iv) the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted.

28. 18 U.S.C. § 2518(11)(b)(iv). Under 18 U.S.C. § 2518(12), "[a] provider of wire or electronic communications service that has received [a roving surveillance order] may move the court to modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion."

29. A FISA application for electronic surveillance must include "the identity, if known, or a description of the target of the electronic surveillance." 50 U.S.C. § 1804(a)(3).

30. A FISA application for electronic surveillance must include "a statement of the facts and circumstances relied upon by the applicant to justify his belief that—(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power." 50 U.S.C. § 1804(a)(4)(A). To grant the FISA application, the Foreign Intelligence Surveillance Court (FISC) must find, "on the basis of the facts submitted by the applicant," that "there is probable cause to believe that—(A) the target of the surveillance is a foreign power or an agent of a foreign power." 50 U.S.C. § 1804(a)(4)(A).

31. See 50 U.S.C. § 1801(a)-(b) (defining "foreign power" and "agent of a foreign power").

32. A FISA application for electronic surveillance must include "a statement of the facts and circumstances relied upon by the applicant to justify his belief that * * * (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1804(a)(4)(B). To grant the FISA application, the FISC must find, "on the basis of the facts submitted by the applicant," that "there is probable cause to believe that * * * (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1805(a)(3)(B). See note 32, *supra*.

33. The certification that is part of every FISA application must designate the type of foreign intelligence information being sought by the electronic surveillance, and explain the basis for the designation. 50 U.S.C. § 1804(a)(7)(D) and (E)(i).

34. 50 U.S.C. § 1805(c)(2)(B).

35. See note 32, *supra*.

36. As discussed in notes 18 and 32, *supra*, the government normally satisfies Title III by establishing probable cause that "the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of [the underlying] offense," 18 U.S.C. § 2518(3)(d), and FISA requires probable cause that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1805(a)(3)(B).

37. ECPA Senate Report at 31.

38. 50 U.S.C. § 1805(c)(1)(B).

39. 50 U.S.C. § 1805(a)(3)(B)

40. 50 U.S.C. § 1801(h)(1).

41. The nexus requirement applies only to each facility at which surveillance "is" directed, but the use of the present tense plainly would not support an argument that roving surveillance—which occurs in the future—is exempt from the requirement. On the contrary, even in an ordinary (non-roving) FISA case, the surveillance commences in the future—i.e., *after* the FISC has issued its order.

42. 18 U.S.C. § 2518(11)(b)(iv).

43. Roving FISA surveillance is in fact being done. The Department of Justice revealed that there had been 49 roving FISA surveillance orders issued as of March 30, 2005. Testimony of James A. Baker, Counsel for Intelligence Policy, before the Subcommittee on Crime, Terrorism, and Homeland Security, Committee on the Judiciary, U.S. House of Representatives, April 28, 2005 (available at *http://judiciary.house.gov/media/pdfs/baker042805.pdf*) (hereinafter Baker House Testimony).

The Department supports roving FISA surveillance with arguments similar to, but not identical to, the ones I advance here. As James Baker, the Counsel for Intelligence Policy, testified on April 28, 2005:

> Let me respond to this criticism [concerning "John Doe" warrants] in the following way. First, even when the government is unsure of the name of a target of such a wiretap, FISA requires the government to provide "the identity, if known, or a description of the target of the electronic surveillance" to the FISA Court prior to obtaining the surveillance order. 50 U.S.C. §§ 1804(a)(3) and 1805(c)(1)(A). As a result, each roving wiretap order is tied to a particular target whom the FISA Court must find probable cause to believe is a foreign power or an agent of a foreign power. In addition, the FISA Court must find "that the actions of *the target* of the application may have the effect of thwarting" the surveillance, thereby requiring an analysis of the activities of a foreign power or an agent of a foreign power that can be identified or described. 50 U.S.C. § 1805(c)(2)(B). Finally, it is important to remember that FISA has always required that the government conduct every surveillance pursuant to appropriate minimization procedures that limit the government's acquisition, retention, and dissemination of irrelevant communications of innocent Americans. Both the Attorney General and the FISA Court must approve those minimization procedures. Taken together, we believe that these provisions adequately protect against unwarranted governmental intrusions into the privacy of Americans.

Baker House Testimony at 2 (emphasis in original).

44. See 50 U.S.C. § 1805(f).

45. Under 50 U.S.C. § 1801(b)(1)(A), an "agent of a foreign power" is defined to include:

(1) any person other than a United States person, who—

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section.

Under 50 U.S.C. § 1801(a)(4), a "foreign power" is defined to include "a group engaged in international terrorism or activities in preparation therefor."

Under 50 U.S.C. § 1801(c), "international terrorism" is defined to mean activities that:

(1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;

(2) appear to be intended—

(A) to intimidate or coerce a civilian population;

(B) to influence the policy of a government by intimidation or coercion; or

(C) to affect the conduct of a government by assassination or kidnapping; and

(3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

46. Under 50 U.S.C. § 1801(b)(2), an "agent of a foreign power" is defined to include: any person who—

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;

(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or

(E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

47. See 50 U.S.C. §§ 1805(e)(1)(B), (e)(2)(B) (electronic surveillance), 1824(d)(1)(B), (d)(2)(B) (physical searches).

48. See 50 U.S.C. §§ 1810 ("An aggrieved person, other than a foreign power or an agent of a foreign power, as defined in section 1801(a) or (b)(1)(A) of this title, respectively, who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 of this title shall have a cause of action against any person who committed such violation and shall be entitled to recover" money damages); 1828 ("An aggrieved person, other than a foreign power or an agent of a foreign power, as defined in section 1801(a) or (b)(1)(A), respectively, of this title, whose premises, property, information, or material has been subjected to a physical search within the United States or about whom information obtained by such a physical search has been disclosed or used in violation of section 1827 of this title shall have a cause of action against any person who committed such violation and shall be entitled to recover" money damages).

49. See 50 U.S.C. §§ 1801(b)(1)(A), 1805(e)(1)(B). FISA's legislative history explains that the "term 'member' means an active, knowing member of the group or organization which is a foreign power. It does not include mere sympathizers, fellow-travelers, or persons who may have merely attended meetings of the group or organization." H.R. Rep. No. 1283, Part I, 95th Cong., 2d Sess. 34 (1978) (hereinafter House Report) This is, of course, a fact-intensive inquiry.

50. 50 U.S.C. §§ 1805(e)(1)(B), (2)(B), 1824(d)(1)(B), (d)(2)(B); see 50 U.S.C. §§ 1801(b)(1)(A).

51. 50 U.S.C. §§ 1801(n) ("Contents', 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").

52. 18 U.S.C. § 2510(8) ("contents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication").

53. See House Report at 51 (stating that pen registers were intended to be included in the definition of "electronic surveillance" in 50 U.S.C. § 1801(f)(2)), 67 ("devices such as pen registers are included"); see also S. Rep. No. 185, 105th Cong., 2d Sess. 27 (1998) (noting that pen registers were considered electronic surveillance under the original version of FISA) (hereinafter Senate Intelligence Pen-Trap Report).

54. Pub. L. No. 105–272, § 601, 112 Stat. 2396 (Oct. 20, 1998), codified at 50 U.S.C. §§ 1841–1846. Pen-trap orders may be obtained on a lesser showing than would be necessary for electronic surveillance or a physical search because the Supreme Court has held that limited information concerning the source or destination of a communication is not protected by the Fourth Amendment. See *Smith* v. *Maryland*, 442 U.S. 735 (1979). The Court in *Smith* reasoned that a person does not have a reasonable expectation of privacy in the numbers dialed from a telephone and therefore that a pen register does not constitute a "search" within the meaning of the Fourth Amendment. *Id.* at 742–46. Absent the statutory requirements to obtain a court order, therefore, the government could employ pen-trap devices without any judicial authorization.

55. See 50 U.S.C. § 1841(2) (defining pen register and trap and trace by reference to 18 U.S.C. § 3127).
56. 18 U.S.C. § 3127(3).
57. See note 62, *infra*.
58. 18 U.S.C. § 3127(4).
59. See *www.usdoj.gov/criminal/cybercrime/PatriotAct.htm*. A trap and trace device is still defined in the statute as a trap and trace "device" even if it is in fact a process, rather than a device.
60. See *United States* v. *New York Tel. Co.*, 434 U.S. 159, 161 n.1 (1977) ("A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electronic impulses caused when the dial on the phone is released. It does not overhear oral communications and does not indicate whether calls are actually completed.").
61. See U.S. Internet Service Provider Association, *Electronic Evidence Compliance—A Guide for Internet Service Providers*, 18 Berkeley Tech. L. J. 945, 956 (2003) ("Law enforcement may also use pen register and trap and trace orders to trace communications on the Internet and other computer networks."). Prior to the Patriot Act, pen registers had been used to obtain computer routing and addressing information, but it was not well settled that this was the correct interpretation of the statute. See *www.usdoj.gov/criminal/cybercrime/PatriotAct.htm.*
62. 18 U.S.C. § 3127(3) & (4). FISA does not incorporate a provision of the criminal code that requires the government to use "technology reasonably available to it that restricts" pen-trap interceptions "so as not to include the contents of any wire or electronic communications." 18 U.S.C. § 3121(c). However, Section 2.4 of Executive Order 12333 imposes similar restrictions, requiring Intelligence Community agencies, which include the intelligence elements of the FBI, to "use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad."
63. It applies only to the subchapter of FISA regulating electronic surveillance. Under the first sentence of 50 U.S.C. § 1801, the definitions in that section apply only to "this title," or Title I of FISA. The pen-trap provisions are in Title IV of FISA. Although Congress chose to incorporate by reference into the FISA pen-trap provisions many of the definitions applicable to electronic surveillance, it did not incorporate FISA's definition of "contents." See 50 U.S.C. § 1841.
64. 50 U.S.C. § 1801(n).
65. There may, of course, be another reason for Section 202, but if so I am unaware of it.
66. One other concern might arise from 18 U.S.C. § 2511(2)(f), which provides in relevant part that "procedures in [Title III] or [the Stored Communications Act, 18 U.S.C. §§ 2701–2712] and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as described in [50 U.S.C. § 1801], and the interception of domestic wire, oral, and electronic communications may be conducted." FISA's broad definition of "contents" means that its definition of "electronic surveillance" is correspondingly broad, see 50 U.S.C. § 1801(f)(1)–(3), and includes pen-trap surveillance. This might give rise to the concern that Section 2511(2)(f) forbids criminal pen-trap surveillance because it provides that FISA and Title III are the "exclusive means" for conducting such surveillance. In other contexts, however, the courts of appeals have rejected arguments that Section 2511(2)(f) forbids domestic law enforcement investigative conduct that is "electronic surveillance" under FISA but not under Title III. See, *e.g., United States* v. *Koyomejian*, 970 F.2d 536. 540–541 (9th Cir. 1992) (en banc) (silent video surveillance, which is "electronic surveillance" as defined by FISA but is not regulated by Title III, may be conducted against domestic, criminal targets without following either FISA or Title III). This is a very complex area, in which I may not know all the relevant facts, but in any event, my sense is that if an amendment is needed, the provision to be amended should be 18 U.S.C. § 2511(2)(f), not FISA.
67. See 50 U.S.C. § 1841(2) (FISA pen-trap devices defined by cross-reference to criminal pen-trap statute), 18 U.S.C. § 3127(3)–(4) (criminal pen-trap surveillance may not intercept "contents"), 18 U.S.C. § 3127(1) (defining "contents" for criminal pen-trap statute by cross-reference to Title III), 18 U.S.C. § 2510(8) (defining "contents" in Title III as "any information concerning the substance, purport, or meaning of [a] communication").
68. 18 U.S.C. § 2510(8).
69. See Electronic Communications Privacy Act (ECPA), Pub. L. 99–508, § 101(a)(5), 100 Stat. 1848, amending 18 U.S.C. § 2510(8); see also ECPA Senate Report at 13–14.
70. 50 U.S.C. §§ 1842(a)(1), (a)(2).

71. As a technical drafting matter, the bill should specify that the change pertains to the second use of the word "for" in the provision.

72. There are similar First Amendment provisions in other parts of FISA. See 50 U.S.C. §§ 1805(a)(3)(A), 1824(a)(3)(A) ("no United States person may be considered * * * an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States"). (The electronic surveillance version of this standard applies to foreign powers and agents of foreign powers; the physical search version applies only to agents of foreign powers. I doubt the omission was intentional.) See also 50 U.S.C. § 1842(a)(1), (c)(2), 1843(a), (b)(1) (similar provisions for pen-trap surveillance).

73. 50 U.S.C. § 1861(d).

74. 334 F. Supp.2d 471 (S.D.N.Y. 2004).

75. 18 U.S.C. § 2709. Section 2709 provides that "[a] wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation." 18 U.S.C. § 2709(a). It also provides that "[n]o wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section." 18 U.S.C. § 2709(c).

76. 334 F. Supp.2d at 514.

77. *Id.*

78. The Department of Justice is apparently of the same view. See Baker House Testimony at 3–4 ("some criticisms of section 215 have apparently been based on possible ambiguity in the law. The Department has already stated in litigation that the recipient of a section 215 order may consult with his attorney and may challenge that order in court. The Department has also stated that the government may seek, and a court may require, only the production of records that are relevant to a national security investigation, a standard similar to the relevance standard that applies to grand jury subpoenas in criminal cases. The text of section 215, however, is not as clear as it could be in these respects. The Department, therefore, is willing to support amendments to Section 215 to clarify these points.").

79. See, *e.g., Los Angeles Police Dep't* v. *United Reporting Publishing Co.*, 528 U.S. 32, 37–39 (1999) (explaining First Amendment overbreadth doctrine); cf. *United States* v. *Salerno*, 481 U.S. 739, 745 (1987) ("The fact that [a statute] might operate unconstitutionally under some conceivable set of circumstances is insufficient to render it wholly invalid, since we have not recognized an 'overbreadth' doctrine outside the limited context of the First Amendment").

80. See, *e.g.,* Executive Order 12958 (as amended).

81. See, *e.g., Snepp* v. *United States*, 444 U.S. 507, 510 n.3 (1980).

82. 50 U.S.C. §§ 1801(h), 1805(a), 1805(c)(2)(A), 1821(4), 1824(a), 1824(c)(2)(A).

83. Executive Order 12333 § 2.3; see also *id.* § 1.14. The intelligence elements of the FBI are in the intelligence community. *Id.* § 3.4(f)(6).

84. Baker House Testimony at 3 ("The Attorney General also recently declassified the fact that the FISA Court has issued 35 orders under section 215 from the effective date of the Act through March 30th of this year. The Attorney General also declassified the types of business records sought by these orders. They include driver's license records, public accommodation records, apartment leasing records, credit card records, and subscriber information, such as names and addresses, for telephone numbers captured through court-authorized pen register devices. None of those orders were issued to libraries and/or booksellers, or were for medical or gun records.").

85. I have not reviewed Section 212 word-by-word against the current postal regulations.

86. I was recently made aware of a November 19, 2004 letter from Attorney General Ashcroft to the Postmaster General, in which the Attorney General asked the Postmaster General to amend the mail regulations. The requested changes were not made.

87. Compare 39 C.F.R. § 233.3(c)(1)(i) and (9)(i)-(iii), with 50 U.S.C. § 1801(e)(1).

88. 39 C.F.R. § 233.3(c)(3)(8).

89. 39 C.F.R. § 233.3(e)(3).

90. 39 C.F.R. § 233.3(e)(2)(i).

91. 39 C.F.R. § 233.3(g)(5)-(6).

92. 39 C.F.R. § 233.3(g)(8).

93. Under 39 U.S.C. § 201, the Postal Service is "an independent establishment of the executive branch." For a discussion of the status and corporate governance structure of the Postal Service, see *United States Postal Service* v. *Flamingo Industries (USA) Ltd.*, 540 U.S. 736, 740 (2004).

94. The current guidelines for national security investigations issued under Executive Order 12333 are classified in part. See *www.usdoj.gov/olp/nsiguidelines.pdf* and *www.usdoj.gov/olp/nsifactsheet.pdf.* An earlier version of these guidelines, issued in May 1995, is also classified in part. See *www.usdoj.gov/ag/readingroom/terrorismintel2.pdf.*

95. 50 U.S.C. §§ 1861–1862.

96. 18 U.S.C. § 3486.

97. 21 U.S.C. § 876 ("In any investigation relating to his functions under this subchapter with respect to controlled substances, listed chemicals, tableting machines, or encapsulating machines, the Attorney General may subpoena witnesses, compel the attendance and testimony of witnesses, and require the production of any records (including books, papers, documents, and other tangible things which constitute or contain evidence) which the Attorney General finds relevant or material to the investigation."). For what appears to be a truly comprehensive list of administrative subpoena authorities held by Executive Branch entities, see United States Department of Justice, Office of Legal Policy, *Appendices A, B & C Accompanying Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities Pursuant to Public Law 106–544,* available at *www.usdoj.gov/olp/appendixal.pdf, www.usdoj.gov/olp/appendixa2.pdf, www.usdoj.gov/olp/appendixb.pdf,* and *www.usdoj.gov/olp/appendixc.pdf.*

98. See United States Department of Justice, Office of Legal Policy, *Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities Pursuant to Public Law 106–544*, Table I at 40–41, available at *http://www.usdoj.gov/olp/intro.pdf* (hereinafter DOJ Administrative Subpoena Report).

99. Between October 26, 2001, and January 21, 2003, the FBI issued what appears to be several hundred national security letters, although the precise number is apparently classified. See *www.aclu.org/patriot foia/FOIA/NSLLists.pdf.*

100. DOJ Administrative Subpoena Report at 41 (noting delegation from Attorney General to FBI Director of authority to issue subpoenas under 18 U.S.C. § 3486 in investigations of child sex abuse).

101. See Kris House Testimony at 16–18.

102. See 50 U.S.C. § 1808(a)(2)(A) (semi-annual report shall describe "each criminal case in which information acquired under this Act has been passed for law enforcement purposes during the period covered by such report"). See also 50 U.S.C. § 1806(b) ("No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.").

103. Under 50 U.S.C. § 1808(a)(2)(B), the semi-annual report must include a description of "each criminal case in which information acquired under this chapter has been authorized for use at trial during such reporting period."

STATEMENT OF DAVID S. KRIS, FORMER ASSOCIATE DEPUTY ATTORNEY GENERAL, DEPARTMENT OF JUSTICE

Mr. KRIS. Yes. Chairman Roberts, Vice Chairman Rockefeller, thank you very much for the opportunity to testify about your draft bill. I am speaking this morning as a private citizen and for myself only. But as a former government lawyer I would like to begin by joining the Department of Justice in applauding the bill. I think several provisions of it will help to keep us safe.

For example, the renewal of several provisions from the Patriot Act is, in my view, a good idea about which I know you've heard a lot.

My written testimony singles out two PATRIOT Act provisions, the ones pertaining to the FISA wall, Section 218, and the one pertaining to FISA roving surveillance, where I think I've made some observations that may not be obvious and may be helpful to you.

I also applaud the bill as a private citizen and one who cares about and values privacy and civil liberties. There are a couple of provisions in the bill worthy of mention in that regard—section 211 which expands the disclosure rights and the reporting obligations

for FISA tangible things orders; and section 213, which, in authorizing administrative subpoenas, also specifically provides for motions to quash such subpoenas filed by the recipients either in their local U.S District Courts or even in the Foreign Intelligence Surveillance Court. Actually, I have to say that that, in my view, is a questionable provision although it is protective of civil liberties, I think.

At some sort of basic level it seems to me pretty clear that the Department and the FBI need to have the authority to compel the production of documents and other things in national security investigations, whether it be by National Security Letters or tangible things orders or administrative subpoenas, just as they have corresponding authority by administrative subpoena or grand jury subpoena in criminal cases.

The question, it seems to me, is under what circumstances and what conditions will that authority be exercised? And just in sitting here listening to the dialog I sort of sketched out what I think are five or six factors that might or might not be applied to the exercise of administrative subpoena power.

There is first the requirement for high level executive branch approval before such a subpoena could be issued; a requirement for a submission or a certification by an applicant in front of a judicial officer; advance judicial review, either substantive—looking at the certification and questioning it or procedural—making sure that the certification has all the required elements. There would be consultation rights and nondisclosure rules governing recipients. And then finally there would be the possibility of after-the-fact judicial review, either in a motion to quash by the recipient or maybe in some kind of ratification by a court of the administrative subpoena in the same way that FISA emergency orders are ratified after the fact.

So those it seems to me are the factors. And this bill it seems to me is aiming for a balanced approach to the question of granting authority but also conditioning it in appropriate ways. At a minimum, it strikes me as a good place to begin the dialog.

One other thing that I think is worth thinking about in considering the administrative subpoena provisions and the other provisions in this bill: it is not just a question of whether the government as a whole should have this power or should not have this power under certain conditions. I think it's also a question of which parts of the government have the power, because in a bureaucracy as big as the executive branch, every time you grant power to one part you change the way it relates to the others.

And in my view, it is important to grant the authority here to the Attorney General, for two reasons—first to reaffirm once again that the Attorney General is, in fact, in charge both of DOJ proper and of the FBI, and also because I think it is important as we go forward, sort of emerging from the shadow of the FISA wall, to encourage wherever possible the interaction of agents and lawyers, whether they be prosecutors or other lawyers, within the Department of Justice.

And so I think the Attorney General ought to have the authority to delegate this power of administrative subpoenas, if it's granted,

to whomever he or she believes is the appropriate recipient, maybe with some floor set by statute.

For example, right now there is a discussion I believe, according to the *New York Times*, about whether to create a national security division within the Department of Justice. And if such a division were created the Attorney General might well choose to delegate this power to the assistant attorney general for that division rather than to the Director. So I think the statute should give the Attorney General that authority.

And now I would obviously be happy to answer any of your questions.

Chairman ROBERTS. We thank you for your testimony, Mr. Kris.

Mr. Onek.

[The prepared statement of Mr. Onek follows:]

PREPARED STATEMENT OF JOSEPH ONEK

Mr. Chairman, Senator Rockefeller, Members of the Committee. I greatly appreciate this opportunity to testify on the pending proposals to extend and amend provisions of the Patriot Act and the Foreign Intelligence Surveillance Act. The Patriot Act and FISA are important tools in the fight against terrorism, but both raise significant civil liberties issues. We therefore need to subject them to careful and continuing scrutiny.

ADMINISTRATIVE SUBPOENAS

The draft legislation proposes to amend FISA by providing for administrative subpoenas in national security investigations. Administrative subpoenas are now used in many types of investigations, and the government asks why they shouldn't also be used by the FBI in the fight against terrorism. But the government ignores some very crucial facts.

First, administrative subpoenas are typically used for discrete purposes and to obtain limited types of records. But here the subpoenas would be seeking records relating to foreign intelligence and terrorism. The range of activities that relate foreign intelligence and terrorism is enormous and, therefore, there is virtually no limit to the type of records the FBI will be able to subpoena. The FBI will seek financial records, employment records, transportation records, medical records and yes, sometimes, library records. The collection of this massive array of records creates special problems. Inevitably, FBI investigations will sweep up sensitive information about innocent, law-abiding people. How do we assure this information is not abused? The FBI will also sweep up information about people who have nothing whatsoever to do with terrorism but who may have committed other infractions, both minor and major. What will the FBI do with this information? Should it use the information in criminal prosecutions or other proceedings unrelated to terrorism? Does it make any difference that a highly disproportionate amount of this information will be collected about people who (quite naturally and innocently) happen to write, visit and send money to places such as Pakistan and Iraq?

I am not suggesting that the Committee now address these complex privacy and profiling issues. But I do believe the Committee should keep these issues in mind as it considers whether to give the FBI essentially unlimited subpoena authority.

There is a second crucial difference between the ordinary use of administrative subpoenas and proposal before the Committee. As set forth in the draft, the FBI's subpoenas must be kept completely secret whenever the FBI says that national security requires non-disclosure. This means that a record holder who receives a subpoena that is overbroad or impinges on first amendment rights will not be able to complain to the press, the Congress or the public.

This is not an insignificant disadvantage. Just last year, a Federal prosecutor in Iowa served grand jury subpoenas on Drake University and members of the university community in connection with a peaceful antiwar forum. The university community protested loudly, the press took up the controversy, and the subpoenas were promptly withdrawn. This cannot happen when the subpoenas are secret.

If subpoenas covering a vast array of records are going to be served in secret, there must be additional safeguards. The most obvious safeguard is prior judicial approval, such as is provided, however inadequately, in Section 215 of the Patriot

Act. We should not permit, for the first time in our history, the massive use of secret subpoenas that have not been approved by a judge.

I recognize that the proposed draft provides record holders with the opportunity to challenge any subpoena in Federal court. But this opportunity is no substitute for prior judicial approval. Third party record holders will generally have no incentive to undertake the burdens of a Federal court challenge, and the secrecy provisions further reduce the likelihood of a challenge. If, for example, a hospital receives a subpoena for a massive number of medical records and the subpoena is made public, the medical staff and patient groups might pressure the hospital to file a challenge. There will be no such pressure with a secret subpoena. Thus, there will be little judicial supervision of the FBI's use of secret subpoenas.

The FBI should be required to obtain a court order when it seeks access to business records. I believe the current standards for issuing such orders, as set forth in Section 215 of the Patriot Act, should be tightened along the lines suggested by the SAFE Act. Subpoena power should be limited to records involving or pertaining to an "agent of a foreign power" as defined in FISA. But in any event there must be a requirement for judicial approval. Such a requirement imposes a salutary discipline on the government. It forces the government to think through and describe, in the words of Deputy Attorney General Comey, the "meaningful, logical connection between the record sought and the subject of the investigation." If the government believes that obtaining a court order is too slow in certain circumstances, it should propose procedures for the prompter handling of urgent requests.

In sum, I believe the Committee should not go forward with the proposal for new subpoena authority for the FBI. But if the Committee does go forward, it should clarify and improve certain provisions.

Section 808(a)(3)(b), providing for judicial review, states that upon the government's request the court "shall" receive government submissions ex parte and in camera. Of course, there may be a need for the government to submit classified information to the court ex parte and in camera. But under the section as written the government could make a submission to the court without even notifying the opposing party of that fact and without disclosing those portions of its submission, such as discussions of legal precedents, that do not require special protection. This section should be modified to grant the court discretion to assure that, as in the Classified Information Procedures Act, both the government's interest in protecting national security and the private party's interest in a fair hearing are appropriately accommodated.

Section 808(d), Standard of Review, is ambiguously worded. The standard for court modification of a subpoena is whether compliance would be "unreasonable or oppressive", while the standard for setting aside a subpoena is "abuse of discretion." What is the relationship between the two standards? Can there be an unreasonable or oppressive subpoena that does not constitute an abuse of discretion? Can there be an abuse of discretion based on other factors?

MAIL COVERS

In addition to granting the FBI new subpoena power, the draft legislation proposes to amend FISA to authorize the FBI to request mail covers from the Postal Service. As with the subpoena power, it is not clear why this new authority is necessary. The FBI already has the ability to request mail covers under Postal Service regulations.

Perhaps, however, this is an opportunity to make the laws regulating FBI investigations more coherent. Mail covers are conceptually similar to the pen registers and trap and trace devices that are presently regulated by Title IV of FISA. Why shouldn't they be treated in a similar fashion under FISA? This would require the FBI to obtain a court order for mail covers. As you know from previous Committee hearings, there is some dispute about the standards for the issuance of pen register and trap and trace orders. I will not go into that here. The crucial point is that there should be some judicial supervision and some coherence in the law.

LONE WOLF

The Committee draft repeals the sunset of the "Lone Wolf" provision that was enacted just a few months ago. I believe the "Lone Wolf" provision may well be unconstitutional and that, in light of criminal surveillance authorities, it is unnecessary. The Committee has not yet received the government's first report on the provision and cannot have an adequate record as to how the provision has been used and whether alternative surveillance authorities were available. I suggest, therefore, that the current sunset requirement be extended until December 31, 2007. This will

give the Committee and the Congress a better opportunity to assess the need for the provision.

OTHER FISA ISSUES

Section 203 of the Committee's draft amends FISA by stating that "foreign intelligence information" includes information relating to national security criminal prosecutions. Once again, I am not sure why this amendment is necessary, since there is widespread agreement that the "wall" no longer exists. But the amendment does underscore the very significant fact that today an increasing number of criminal cases involve the use of FISA evidence. This requires a re-examination of whether current procedures for the use of FISA evidence in criminal cases are fair.

As Jim Dempsey testified before this Committee in April, criminal defendants in most cases can obtain access to the affidavit that served as the basis for the wiretap order or search warrant and thus can challenge the basis for the wiretap or search in an adversarial proceeding. By contrast, defendants in FISA cases have never been granted such access and have never had a meaningful opportunity to challenge the basis for the search. Congress should assure that normal criminal adversary procedures apply when FISA evidence is used against individuals, with appropriate use of the Classified Information Procedures Act to protect government interests.

There is another problem with FISA that has not been adequately addressed. Under FISA, the government can obtain an order to conduct secret searches of any home or office. Unlike the "sneak and peek" searches authorized in Section 213 of the Patriot Act, these searches remain secret forever unless the government chooses to disclose them or there is a criminal trial involving evidence seized during the search. This means that innocent Americans have had, and will have, their most intimate records and belongings searched by the government without ever being informed of the search. Similarly, although Title III wiretaps are ultimately disclosed, FISA wiretaps are not.

I believe that FISA should be amended to assure that individuals are informed they have been subject to a secret FISA search or wiretap unless there are valid national security grounds to continue the secrecy. In cases where there has been a secret search or wiretap but no disclosure of that fact in a criminal trial the government should be required to periodically file a motion with the FISA court requesting and justifying continued non-disclosure.

CONCLUSION

In concluding, I would like to commend the Committee for its attention to congressional oversight, including the reporting requirements contained in the draft legislation. Congressional oversight is crucial and must be pursued vigorously. But executive branch accountability requires more than congressional oversight; it requires judicial oversight and as much openness as is consistent with national security. When, as in terrorism investigations, a high degree of secrecy is warranted, a meaningful role for the judiciary becomes all the more important. The Committee should not eviscerate that role by granting broad subpoena power to the FBI.

STATEMENT OF JOSEPH ONEK, SENIOR POLICY ANALYST, OPEN SOCIETY INSTITUTE, AND SENIOR COUNSEL, CONSTITUTION PROJECT

Mr. ONEK. Thank you, Chairman Roberts, Vice Chairman Rockefeller, members of the committee.

I'd like to begin, if I may, by talking about the Lone Wolf provision because I think it may get lost in the shuffle. This provision was not passed 3½ years ago; it was passed just a few months ago. Yet the draft legislation would repeal the sunset for it. And I think this may be a good example of what Senator Rockefeller had described earlier of a provision where the sunset should clearly be extended.

I happen to believe that the Lone Wolf provision may be unconstitutional and that, in light of other criminal surveillance authorities, it's unnecessary.

But the crucial point is that this Committee has not yet received the government's first report, because the 6-month period isn't up

yet, on this provision. The Committee can't have an adequate record as to how often or when the provision has been used and whether alternative surveillance authorities are available.

So I think this is the perfect occasion, certainly, to take up Senator Rockefeller's suggestion about these provisions. And in this case I think it's clear the sunset provision should be extended for 3 or 4 years. This would give the Committee and the Congress a better opportunity to assess the need for the Lone Wolf provision.

I'd like to turn to administrative subpoenas. There's been a discussion of how often they've been used in other contexts. There's also already been a discussion about the fact that here we're dealing with a much, much broader array of records. Indeed, because we're investigating foreign intelligence and terrorism, there's essentially no limit on the kinds of records that can be subpoenaed. And I think this raises all sorts of privacy and profiling issues, which I'd be glad to discuss in the questioning.

But there's another difference between these subpoenas and the other uses of administrative subpoenas. These are going to be largely secret. That means that the recipient can't complain to the press, can't complain to the public, can't complain to the Congress.

And this isn't insignificant. Just last year in Iowa, a Federal prosecutor requested records from Drake University and members of the community in connection with a peaceful antiwar forum. The university community got up in arms and protested. The press took up the controversy. And the subpoenas were withdrawn 3 days later. Now, that just can't happen when the subpoenas are secret.

So if you're going to have secret subpoenas, I think there have to be additional safeguards. And the obvious and best safeguard is prior judicial approval, as is provided, for example, in Section 215. Now there can be an exception for emergency cases, as Senator Feinstein suggested, and FISA already has exceptions in Title I and Title III for emergencies.

But never in our history, I don't believe, has there ever been a situation where there's been massive use of secret subpoenas without prior judicial approval. This is a totally new thing. All the other subpoenas they're talking about are not secret, and the people who get them have a chance to complain about them.

This is a very different situation. You'd be creating, for the first time in our history, a regime of mass secret subpoenas, because I'm sure this is going to be used a great deal. Most of the time they will be secret. And under those circumstances I think prior judicial approval is required.

Post-judicial approval won't work. Ms. Caproni was very candid with this Committee when she pointed out that very few third-party record-holders ever move to quash a subpoena. She was very clear on that. So I don't think that post-hoc judicial review is going to take place. It just ain't going to happen.

And by the way, it's going to happen even less because of the secrecy. For example, if you subpoena hospital records and was public, maybe the patient groups and the medical staff would pressure the hospital into challenging the subpoena. But if it's a secret subpoena and, as in this legislation, the hospital has immunity from giving the records over, its just going to give them over.

So after-the-fact judicial review is not going to happen. This is a classic case where we should have judicial approval. If you're going to have vast numbers of secret subpoenas, the real safeguard you must have is prior judicial approval as in Section 215. I happen to believe that the standard in Section 215 should be tightened. We can, of course, discuss that in the question-and-answer period.

Thank you.

Chairman ROBERTS. We thank you for your testimony, sir.

Mr. Collins.

[The prepared statement of Mr. Collins follows:]

PREPARED STATEMENT OF DANIEL P. COLLINS

Chairman Roberts, Vice-Chairnian Rockefeller, and Members of the Committee, I am grateful for the opportunity to testify before you today. Three and one-half years ago, the USA PATRIOT Act was signed into law by President Bush with overwhelming support in both Houses of Congress. *See* Pub. L. No. 107–56, 115 Stat. 272 (Oct. 26, 2001). That strong bipartisan consensus reflected the gravity and importance of the chief objective of that legislation, which was set forth right in the title: "providing appropriate tools required to intercept and obstruct terrorism." As the horrific events of September 11 demonstrated, there are few priorities more pressing than detecting and preventing terrorist attacks. It is critical that the men and women whose job it is to protect us have the tools they need to get that job done, and to get it done in a manner that both enhances security and respects liberty.

However, as the Committee is well aware, several provisions of Title II of the PATRIOT Act are scheduled to expire on December 31, 2005, absent action by Congress. *Id.*, § 224(a), 115 Stat. at 295. Under Section 101 of the draft legislation that is the subject of this hearing, nine of the PATRIOT Act provisions that are currently subject to sunset would be made peiivanent. *See* Section 101 (repealing the sunset of sections 203(b), 203(d), 204, 206, 207, 214, 215, 218, and 225 of the PATRIOT Act). I agree that these nine provisions should be made permanent. Today, as in 2001, they are "appropriate tools" in the war on terror.

My perspective on these matters is informed by my service over the years in various capacities in the Justice Department. Most recently, I served from June 2001 until September 2003 as an Associate Deputy Attorney General ("ADAG") in the office of Deputy Attorney General Larry Thompson. During the same period, I also served as the Department's Chief Privacy Officer, and in that capacity, I had the responsibility for coordinating the Department's policies on privacy issues. I also served, from 1992 to 1996, as an Assistant United States Attorney in the Criminal Division of the U.S. Attorney's Office for the Central District of California in Los Angeles. And prior to that, I had served from 1989 to 1991 as an Attorney-Advisor in the Office of Legal Counsel in Washington, D.C. I am now back in private practice in Los Angeles, and I emphasize that the views I offer today are solely my own.

Before turning to the nine relevant PATRIOT Act provisions that are up for "sunset" review by this Committee, I think it is useful to outline some of the basic principles that should guide an analysis of these provisions. The overarching question whether a particular surveillance authority is an "*appropriate* tool" ultimately turns on whether that tool assists in detecting and preventing terrorism, and whether it does so in a manner that preserves and enhances privacy. In making that judgment, it is important not to fall into the fallacy of "zero-sum" thinking, whereby *every* expansion of government surveillance authority is somehow deemed *inherently* to represent a loss of privacy. This sort of thinking does not make much sense either from a national security perspective or from a civil liberties perspective. The question instead is whether the *conditions* placed on the availability and use of a particular tool are sufficient to permit it to be deployed effectively when warranted, but only in a manner that is respectful of privacy and basic civil liberties.

Beyond that very general statement, there is, I think, general agreement on a number of more specific principles that help to inform any judgment about the propriety and adequacy of the conditions place upon the use of a particular tool:

• *Unwavering fidelity to the Constitution.* Privacy is a cherished American right. Among the various ways in which the Constitution protects that right, the Fourth Amendment specifically reaffirms the right of the people to be free from unreasonable searches of their "houses, papers, and effects." Our laws must scrupulously re-

spect the limits established by the Constitution. As many have said, we have to think outside the box, but not outside the Constitution. But while the Constitution sets the minimum, our laws have long properly reflected the judgment that, from a policy perspective, there should be additional statutory protections for privacy. I do not question that judgment.

• *Not all privacy interests are the same.* Not all privacy interests are of the same magnitude, and it makes no policy sense to act as if they were. For example, some categories of information are more important and more sensitive than others. The fact that the supermarket club could maintain a computerized stockpile of information about my personal buying habits may raise a privacy concern, but it is not on the same level as someone eavesdropping on my phone conversations or reading my medical records. The nature and severity of the privacy intrusion at issue are certainly important factors to consider.

• *Privacy is not always the most important value.* It is essential to keep in mind that, while privacy is an important right, it is by no means the only important value. Human society, by its very nature, involves some loss of personal privacy. Competing concerns raised by new technology may also justify particular intrusions on privacy: no one can deny that airport inspections are essential to public safety, regardless of the cost to privacy.

• *If it's good enough for fighting the mob, it's good enough for fighting terrorism.* Any tool that is already available to fight any other type of crime—be it racketeering, drug trafficking, child pornography, or health care fraud—should be available for fighting terrorism, and should have an appropriate analog in the foreign intelligence context. If the judgment has already been made that the tool is appropriate for fighting these other crimes, and that any privacy interests at stake must yield to that effort, then surely the tool should also be available to fight terrorism.

• *The law of inertia must not be a principle of privacy policy.* It does not make much sense to perpetuate outmoded ways of doing things simply because it has always been done that way. As times and technologies change, the judgments that are reflected in existing statutory rules may need to be re-evaluated.

• *The importance of technological neutrality.* In applying privacy principles to new and emerging technologies, an important benchmark is the concept of "technological neutrality." The idea is that, just because a transaction is conducted using a new technology, there should not have to be a loss of privacy when compared to similar transactions using older technologies. To use an example, the privacy protection for ordinary email should be roughly equivalent to that of an ordinary postal letter. Conversely, the emergence of new technologies should not provide foreign agents with new ways to thwart legitimate and legally authorized foreign intelligence activities. The notion of technological neutrality takes into account both sides of the coin.

With these basic principles in mind, let me explain why I think each of the nine pertinent sections of the PATRIOT Act that would be made permanent by Section 101 of the proposed legislation are ones that properly enhance the abilities of intelligence officials in a manner that respects and preserves our freedoms.

(1)-(2) SECTIONS 203(b) AND 203(d)

These provisions, which authorize certain forms of information sharing between law enforcement officers and intelligence officials, are among the most important in the PATRIOT Act.

Specifically, section 203(b) authorizes the sharing of Title III wiretap information with intelligence and national security officials, subject to several conditions: (1) the information must have been obtained "by any means authorized by this chapter," *i.e.*, in accordance with the strict requirements of Title III; (2) the information to be shared must "include foreign intelligence or counterintelligence" or "foreign intelligence information" as those terms are specifically defined by the relevant statutes; (3) the information may only be used by such official "as necessary in the conduct of that person's official duties"; (4) any such official must also comply with "any limitations on the unauthorized disclosure of such information"; and (5) to the extent the information "identifies a United States person," the disclosure must comply with statutorily mandated guidelines issued by the Attorney General. *See* Pub. L. No. 107–56, § 203(b), (c), 115 Stat. at 280–81.

Section 203(d) more generally authorizes sharing of information "obtained as part of a criminal investigation," subject to the following restrictions: (1) the information to be shared must comprise "foreign intelligence or counterintelligence" or "foreign intelligence information" as those terms are specifically defined by the relevant statutes; (2) the information may only be used by such official "as necessary in the conduct of that person's official duties"; and (3) any such official must also comply with

"any limitations on the unauthorized disclosure of such information." *See* Pub. L. No. 107–56, § 203(d), 115 Stat. at 281.

As the 9/11 Commission and others have noted, the need for appropriate sharing of information between law enforcement and intelligence officials is absolutely critical to detecting and preventing terrorism. Moreover, the safeguards imposed by section 203(b) and section 203(d) seem properly tailored to ensure that law enforcement officials will only share information that qualifies as " foreign intelligence or counterintelligence" or "foreign intelligence information" and will do so only subject to appropriate restrictions. It must be emphasized that these modest provisions do *not*, as some critics have wrongly claimed, put the CIA in the business of "spying on Americans." By definition, *all* information subject to sharing under sections 203(b) and 203(d) has been obtained by *the lawful investigative activities of law enforcement officials* either under Title III or "as part of a criminal investigation."

(3) SECTION 204

Section 204 is a largely technical amendment that clarifies the relationship between the authorities under the criminal statute governing "pen registers" and "trap-and-trace" devices and the authorities under otherwise applicable Federal law concerning certain foreign intelligence activities. Pub. L. No. 107–56, § 204, 115 Stat. at 281. I am not aware of an substantial reason why this provision should not be made permanent.

(4) SECTION 206

Section 206 of the PATRIOT Act addresses the subject of so-called "roving wiretaps" under the Foreign Intelligence Surveillance Act of 1978 ("FISA"). In my view, section 206 strikes an appropriate balance on this subject and should be preserved.

Under the current version of Section 105(c)(1)(B) of FISA, a FISA order authorizing electronic surveillance only needs to *specify* the nature and location of each such facility or place "if known." 50 U.S.C. § 1805(c)(1)(B). Notably, the addition of the phrase "if known" was not made by the PATRIOT Act, but rather by the Intelligence Authorization Act for Fiscal Year 2002, Pub. L. No. 107–108, § 314(a)(2)(A), 115 Stat. 1394, 1402 (2001); that amendment is therefore not subject to the PATRIOT Act's sunset provision. Although current law thus dispenses with a *specification* requirement when the exact nature and location of the facilities or places are not known in advance, the existing version of Section 105(a)(3)(B) continues unambiguously to State that an authorizing order may only be issued if, *inter alia*, "there is probable cause to believe that . . . each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1805(a)(3)(B). Reading these provisions together, it would seem clear that, even when it cannot be specified in advance what are the *particular* facilities and places that will be surveilled, the Government must nonetheless provide a sufficient description of the categories of facilities and places that will be surveilled (presumably by describing their connection to the target) so as to permit the court to make the finding that remains required by Section 105(a)(3)(B).

The pertinent change made by Section 206 of the PATRIOT Act was merely to eliminate the requirement that the authorizing order in all cases *specify* in advance those third parties (*e.g.,* wire carriers) who were directed to supply assistance in carrying out the order. *See* Pub. L. No. 107–56, § 206, 115 Stat. at 282 (amending 50 U.S.C. § 1805(c)(2)(B)). Instead, the PATRIOT Act states that, if the court finds that "the actions of the target of the application may have the effect of thwarting the identification of a specified person," the order may require the cooperation of other such persons who have not been specified. *Id.* This modest change makes perfect sense: the prior third-party-assistance specification requirement had the obvious potential to allow targets to defeat surveillance simply by changing, for example, from one cell phone to another. Indeed, it is hard to see why one would want to allow this specific amendment to sunset: there is no apparent advantage to requiring the Government to go back to the FISA Court merely because the target has shifted from one wire service provider to another.

Some have called for making the roving wiretap provisions of FISA more analogous to those for ordinary criminal roving wiretaps in Title III. Under 18 U.S.C. § 2518(11), the requirement in δ 2518(1)(b)(ii) to provide a "particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted" does not apply if, *inter alia*, the application "identifies the person believed to be committing the offense." Setting aside the issue about what the "identification" requirement thus imposed by Title III requires here, the apparent intent of these critics of Section 206 is that FISA should mimic § 2518(11)

by imposing an identification requirement in any case in which the requirement to specify particular *places* has been waived. The analogy, however, is flawed, because of a crucial difference between δ 2518(11) and Section 105 of FISA.

In addition to waiving the specification-of-places requirement in § 2518(1)(b)(ii), the roving wiretap provision of Title III *also* waives the requirement in § 2518(3)(d) that the court must first find probable cause to believe that "the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or common used by [the target]." *See* 18 U.S.C. § 2518(11) (stating that the "requirements of subsections (1)(b)(ii) *and 3(d)* of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply" to roving wiretaps authorized under Title III). As I explained above, FISA's analog to § 2518(3)(d) of Title III is contained in Section 105(a)(3)(B) of FISA, which states that an authorizing order may only be issued if, *inter alia*, "there is probable cause to believe that . . . each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1805(a)(3)(B). It is important to note that *nothing in the roving wiretap provisions of FISA waives this requirement.* The apparent effect of that difference is that unlike Title III, a FISA roving wiretap application must still provide, as I explained earlier, a sufficient description of the categories of facilities and places that will be surveilled (presumably by describing their connection to the target) so as to permit the court to make the additional probable cause finding that remains required by Section 105(a)(3)(B). This additional safeguard strikes a different balance from Title III, but an appropriate one, and it makes any analogy to Title III inapt. That is, in light of FISA's preservation of this requirement, the need for a requirement to "identify" the target is doubtful. Indeed, because it overlooks this crucial additional requirement that only FISA imposes, the clear effect of incorporating Title III's restrictions would be to make FISA roving wiretaps *harder* to obtain that Title III wiretaps.

(5) SECTION 207

Section 207 extends the time periods for which the FISA Court can initially authorize, and later extend, electronic surveillance and physical searches. *See* Pub. L. No. 107–56, § 207, 115 Stat. at 282. Notably, Section 207 only peimits these more generous time periods to be used with respect to a FISA target who is *not* "a United States person." 50 U.S.C. § 1805(e)(1)(B), (e)(2)(B) (limiting this authority to "an agent of a foreign power, as defined in section 1801(b)(1)(A) of this title"); *id.*, § 1801(b)(1) (stating that the definition in that paragraph applies only to a "person *other than a United States person*") (emphasis added). Pre-existing law had already permitted more generous authorization periods for FISA orders directed at entities, organizations, and groups that constitute "foreign powers," 50 U.S.C. § 1805(e)(1)(A),(e)(2)(A), and Section 207 properly permits longer authorization periods to also be used only for that subset of *agents* of foreign powers who are not United States persons. There seems to be little advantage to allowing this provision to sunset; the net effect would merely be more paperwork and a diversion of scarce resources that would be more appropriately deployed on other matters.

(6) SECTION 214

Section 214 is one of several provisions of the PATRIOT Act that properly endeavor to ensure that there will be appropriate analogs, in *foreign intelligence* investigations, for the various tools that are available to assist law enforcement in *criminal* investigations. In particular, Section 214 addresses the use of "pen registers" and "trap and trace devices," *i.e.*, instruments for collecting information about the address or routing of a communication (*e.g.*, the telephone numbers of outgoing calls dialed on a telephone and the telephone numbers of incoming calls), but *not* the content of the communication.

The Supreme Court held long ago that the proper use of a pen register does not implicate the Fourth Amendment, because there is no reasonable expectation of privacy in the numbers dialed on a telephone—numbers that, by definition, the dialer has voluntarily turned over to a third party (*i.e.*, the telephone company). *Smith* v. *Maryland*, 442 U.S. 735, 744 (1979). Since 1986, however, Congress has appropriately regulated the use of such devices, requiring (*inter alia*) an attorney for the Government to make an application to a court in which the attorney certifies that the information to be collected is relevant to an ongoing criminal investigation. 18 U.S.C. § 3122(b)(2). Prior to Section 214, FISA analogously allowed the use of pen registers and trap and trace devices in foreign intelligence investigations, but the

limitations imposed by FISA on such devices were much more restrictive than in the criminal context. Specifically, in contrast to the more generous "relevance" standard imposed in criminal cases, FISA limited the use of such devices to situations where the facilities in question have been or are about to be used in communication with "an individual who is engaging or has engaged in international terrorism or clandestine intelligence activities" or a "foreign power or an agent of a foreign power." 50 U.S.C. § 1842(c)(3) (2000 ed.). Section 214 amended FISA's standards to permit appropriate use of such devices upon a certification that the device is likely to obtain (1) "foreign intelligence information not concerning a United States person" or (2) information that is "relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities." *See* Pub. L. No. 107–56, § 214(a)(2), 115 Stat. at 286. In the latter context, Section 214 provides explicit protection for the First Amendment rights of United States persons. *Id.*

Under Section 214, the ability to use pen registers and trap and trace devices under FISA is thus rendered more analogous in scope to its criminal counterpart. With respect to information concerning a United States person, Section 214 imposes the same standard of "relevance" to an ongoing investigation, but it also specifies that the investigation must be one to protect against "international terrorism" or "clandestine intelligence activities." Given that 18 U.S.C. § 3122 imposes a relevance standard in *all* ordinary criminal cases, it is hard to see why that standard is not sufficient in an intelligence investigation to protect against international terrorism and clandestine intelligence activities. That is, if relevance to an ongoing investigation is a sufficient basis for authorizing a pen register in, say, a fraud case or a drug case, why would it not be a sufficient basis for permitting the use of such a device to investigate international terrorism?

(7) SECTION 215

Section 215 of the PATRIOT Act is another provision designed to ensure that a tool available to assist law enforcement in ordinary criminal investigations will have an appropriate counterpart in foreign intelligence investigations. For a very long time, grand juries have had very broad authority to obtain, by subpoena, records and other tangible items that may be needed during the course of a criminal investigation. Section 215 provides a narrow analog to such subpoenas in the context of certain intelligence investigations under FISA. Indeed, in many respects, Section 215 contains more protections than the rules governing grand jury subpoenas:

- A court order is required. 50 U.S.C. § 1861(c).
- The court is *not* merely a rubber-stamp, because the statute explicitly recognizes the court's authority to "modif[y]" the requested order. *Id.*, § 1861(c)(1).
- The section has a narrow scope, and can be used in an investigation of a U.S. person only "to protect against international terrorism or clandestine intelligence activities." *Id.*, § 1861(a)(1), (b)(2). It cannot be used to investigate domestic terrorism.
- The section provides explicit protection for First Amendment rights. *Id.*, § 1861(a)(1), (a)(2)(B).

The draft bill would make the important clarification that the records may only be obtained if they are "relevant" to an investigation to protect against international terrorism or clandestine intelligence activities. *See* Section 211(a)(1)(A), (2). As I understand it, this amendment would not alter the current understanding of the provision, but would merely eliminate any doubt about whether the relevance standard is applicable here.

Some have called for a standard that is higher than "relevance" to an investigation, and have instead suggested that a Section 215 order should be granted only upon a showing of specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power. This is much too narrow a standard. Suppose that FBI agents suspected that an as-yet-unidentified individual foreign agent may have consulted certain specific technical titles on bomb-making or on nuclear power facilities, and they are informed that 5 persons have checked out those specific titles from public libraries in the relevant area and time period. Because it cannot be said that there are "specific and articulable facts" to suspect *all 5 persons* who checked out the books as all being foreign agents (the most that can be said is that one of them may be), application of such a high standard would seemingly require more evidence before any of the records could be obtained. Even if one were to agree that the general business records authority in Section 215 might benefit from greater reticulation in the contexts of particular types of records, this particular requirement seems too strict. Given the various safeguards already in place in Section 215, which adequately take account of the difference between investigations under FISA and ordinary criminal

investigations, there is insufficient justification for a standard that is so much more demanding than the ordinary "relevance" standard that has long governed grand jury subpoenas in criminal investigations (some of which, like the Versace murder and Zodiac gunman investigations, did consult library records).

Despite what some of its critics seem to imply, the narrowly drafted business records provision in Section 215 has no special focus on authorizing the obtaining of "library records." On the contrary, because the provision specifically forbids the use of its authority to investigate U.S. persons "solely upon the basis of activities protected by the first amendment to the Constitution," the provision explicitly does *not* authorize Federal agents to rummage through the library records of ordinary citizens. Because I think this language properly addresses a concern that has been raised about Section 215's sweep, I would recommend against retaining Section 211(a)(1)(B) of the draft legislation, which would appear to eliminate this clause of Section 215, *i.e.*, the clause that provides specific protection for first amendment rights. That is, while I disagree with those who recommend imposing additional significant substantive limitations on Section 215, I would also recommend against eliminating the substantive safeguards that are currently contained in the provision.

The draft legislation properly declines to create any sort of carve-out for libraries from the otherwise applicable scope of Section 215: that would simply establish libraries and library computers as a "safe harbor" for international terrorists. Indeed, over the years, grand juries have, on appropriate occasions, issued subpoenas for library records in connection with ordinary criminal investigations. In my view, a sensible privacy policy should allow an appropriately limited analog in the FISA context, and Section 215 is just that.

Section 211(b) of the draft bill would make appropriate and necessary clarifying changes to Section 215 by specifying that the prohibition on nondisclosure of Section 215 orders is not intended to preclude the recipient of such an order from consulting with counsel or from requesting permission from the FBI to make other appropriate consultations (e.g., perhaps consulting an accountant with respect to an order requesting financial records).

Section 211(c) properly establishes additional procedural protections by requiring the Attorney General to adopt "minimization procedures governing the retention and dissemination" of any items obtained under a Section 215 order.

The Attorney General, in his testimony before this Committee on April 27, 2005, indicated that the Department of Justice agreed that a recipient of a Section 215 order could bring a challenge to such an order in court. Section 215 is silent as to where and how such a review might be carried out, as is the draft bill. I would recommend that specific provisions establishing the proper venue and procedures for such challenges be set forth in legislation.

(8) SECTION 218

Despite being only one sentence long, Section 218 is one of the most important provisions in the PATRIOT Act. Prior to Section 218, an application for electronic surveillance under FISA had to contain a certification that "the purpose" of the surveillance "is to obtain foreign intelligence information." 50 U.S.C. § 1804(a)(7)(B) (2000 ed.). Section 218 changed the phrase "the purpose" to "a significance purpose," thus clarifying that the presence of other purposes (such as a possible criminal prosecution) did not preclude a FISA application. In doing so, Section 218 disapproved the "primary purpose" test that had been engrafted onto the pre-PATRIOT Act language. *In re Sealed Case*, 310 F.3d 717 (For. Intel. Surv. Ct. of Rev. 2002). This amendment, as many have noted, was important in tearing down the "wall" between intelligence personnel and law enforcement personnel. It should not be permitted to lapse. Moreover, allowing Section 218 to expire could potentially put the law in a state of confusion, because the Foreign Intelligence Surveillance Court of Review has cast doubt on whether the "primary purpose" test was a correct reading of the pre-PATRIOT Act statutory language. *In re Sealed Case, supra.* As a result, there is considerable room for argument over what exactly would be the effect of allowing this provision to lapse. The Congress should ensure clarity in this important area of the law by making Section 218 permanent. Section 101 of the draft legislation does that, and Section 203 also includes a further, appropriate amendment confirming the correctness of the Court of Review's conclusion that FISA Section 101(e)(1)'s reference to c, protect[ing]" against international terrorism, etc., includes protecting by means of a criminal prosecution that disables the foreign agents involved.

(9) SECTION 225

This section extends to the FISA statute the same immunity from civil liability that exists under Title III for wire or electronic communications service providers who assist in carrying out a *court order* or an emergency request for assistance under FISA. Pub. L. No. 107–56, § 225, 115 Stat. at 295–96. There is no good reason the immunity of a service provider for carrying out court orders for surveillance should depend upon whether the order was issued under Title III or under FISA. This provision should be made permanent.

ADDITIONAL PROVISIONS OF THE DRAFT LEGISLATION

The draft bill also contains detailed provisions providing for the use of "administrative subpoenas" in certain intelligence investigations, and codifying (with changes) the use of so-called "mail covers" in such investigations. *See* Sections 213 and 212. The authorization of administrative subpoenas by Section 213 would appear to be an appropriate invocation of the principle that, if a tool is available to fight other crimes, it should be available to fight terrorism. Under 18 U.S.C. § 3486(a), administrative subpoenas are currently authorized in the investigation of, *inter alia*, a "Federal health care offense" and "a Federal offense involving the sexual exploitation or abuse of children." As I said before, if the judgment has already been made that this tool is appropriate for fighting these other crimes, and that any privacy interests at stake must yield to that effort, then surely the tool should also be available to fight terrorism, and should have an analog in the foreign intelligence context. The appropriate questions should, in my view, instead focus on the technical issues concerning how such authority would be granted in the FISA context. Thus, for example, to the extent that the procedures specified in Section 213 differs from those in 18 U.S.C. § 3486, are those differences warranted by differential factors unique to the FISA context? Moreover, what should be the relation between the scope of the administrative subpoena authority in Section 213 of the draft bill and the business records provision in Section 215 of the PATRIOT Act? These are questions that I think warrant careful study and consideration. But I find it very hard to say that administrative subpoena authority is just fine when it comes to health care fraud, but is somehow a grave threat to liberty when it comes to fighting terrorism.

The "mail cover" provisions in Section 212 relate solely to information on the exterior of mail that is not subject to any reasonable expectation of privacy, such as addressing information. The provision appears to be fairly narrowly drafted in terms of the scope of the authority it confers, the high-level approval it requires, and the requirement for "minimization" with respect to retention and dissemination of records obtained by a mail cover under this section. Notably, the provision only applies to requests made to the "United States Postal Service." The apparent intent of the provision is to ensure appropriate cooperation from the Postal Service, while leaving the judgment whether to request the mail cover with the FBI. That formal allocation of authority seems sensible (since only the FBI will be privy to the full context of the intelligence investigation that leads to the request). The Committee should evaluate whether it is needed as a practical matter in light of the history on this issue between the FBI and the Postal Service.

I would also like to make a brief comment about Section 202 of the draft bill. This section would amend FISA's definition of "content" so that it more closely conforms with the definition of "content" under the Title III wiretap statute, 18 U.S.C. § 2510(8). This appears to be a sensible change. By defining "any information concerning the identity of the parties to [a] communication" as "contents," FISA's current definition could be misconstrued as casting doubt on whether mere addressing information, not derived from the substance of the communication, is "contents." As the pen register statutes reflect, mere addressing information is not ordinarily considered to be "contents," and there is no harm in eliminating a perceived potential ambiguity in FISA on this score.

I would be pleased to answer any questions the Committee might have on this subject.

STATEMENT OF DANIEL P. COLLINS, FORMER ASSOCIATE DEPUTY ATTORNEY GENERAL AND CHIEF PRIVACY OFFICER, U.S. DEPARTMENT OF JUSTICE

Mr. COLLINS. Chairman Roberts, Vice Chairman Rockefeller, members of the Committee, I'm pleased to testify before you today

on the important bill and the important subject that you've taken up.

The title of the PATRIOT Act, we're used to calling it the PATRIOT Act but that stands for Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. And part of this Committee's work is evaluating whether, in light of the opportunity since enactment of the PATRIOT Act to review those tools, whether they are still judged to be appropriate.

The draft bill before the Committee would make nine of those tools permanent, and I agree with that assessment. Today, as in 2001, they remain appropriate tools in the war on terror. I've addressed all nine of those in my written statement. I'd like to focus on two of them and then make a few comments on administrative subpoenas.

Section 206 on roving wiretaps has been a subject of significant controversy—section 206 of the PATRIOT Act. As I've set forth in my written statement, I think that it's based on a misunderstanding of the differences between FISA and Title III, because the primary criticism toward section 206 is that it does not incorporate all of the restrictions that are contained on roving wiretaps in Title III on the criminal side. But that is because Title III, on the other hand, waives certain other restrictions that are present in FISA.

So you have actually a different set of restrictions on each side of the ledger. It's a different balance struck on each side. But I think in both cases it's an adequate balance that is struck, and that therefore that provision should be made permanent without modification.

Section 215 of the PATRIOT Act is another provision that's designed to ensure that on the intelligence and national security side, there are counterparts in terms of investigative tools to the tools that are present on the criminal side. And that is the provision that allows for access with a court order to business records.

And the current version of Section 215 contains a number of protections. A court order is required. The court is not merely a rubber stamp, because the statute explicitly recognizes the right of the court to modify the requested order. It has a narrow scope that is specified in the statute. It can't be used to investigate, for example, domestic terrorism. And it provides explicit protection for First Amendment rights, a provision that I think should be retained in that statute.

The draft bill that's before the Committee would make this permanent, would make, I think, an important clarification that the relevance standard, which is actually not reflected on the text of the current provision, is meant to be in the provision and that is made explicit in the provision as modified by the bill before this Committee.

Also, the bill properly establishes additional procedural protections by requiring the Attorney General to adopt minimization procedures governing the retention and dissemination of any items obtained under a Section 215 order.

There's been reference this morning to the fact that the Attorney General, in his testimony before this Committee on April 27, indicated that judicial review should be available to challenge 215 orders. That is not a subject that is currently addressed in Section

215 and I would respectfully submit would be profitably addressed in draft legislation.

The draft bill also contains a provision which has been the subject of much discussion concerning administrative subpoenas. With respect to that provision, my basic approach to that is that with respect to terrorism—which is essentially one of our most important priorities, is fighting terrorism—there should be something equivalent to a most-favored-nations clause.

If we have a tool that is available for some other crime, for some lesser harm, and we have presumably already made the choice that privacy interests that are at stake with respect to that tool must yield in those other circumstances, then I think the burden is on those to say why that tool should not be extended to terrorism. It would seem that without more, it should be applied terrorism. And I think that is the basic logic behind the extension of the administrative subpoena here.

The placement of the administrative subpoena authority on the FISA side does raise, I think, a number of questions that need to be addressed. First and foremost is, what is the relationship between that authority and the authority that exists within Section 215, because there's certainly a significant overlap between the business records authority, and indeed the standards are described similarly in the two devices.

Senator Feinstein suggested that the administrative subpoena should apply only in emergency situations, and presumably would leave the Section 215 authority to be the authority that is invoked in the non-emergency situations. Another possibility would be, in crafting the regime of judicial review for Section 215, to make the standards more lenient—in other words, that the judicial review would be less searching on the Section 215 side than it might be on the administrative subpoena side if the Department went to the trouble of getting judicial review of the order before it was actually issued. There are a number of possibilities the Committee could consider in that regard.

Mr. Kris has raised the issue of delegation, that if there's concern about whether it should be placed with the Director or particular officials within the Bureau, that it could be raised to the Attorney General and leave the Attorney General with flexibility to change the designation.

There's also the issue of the court that should conduct the review. The current provision on administrative subpoenas here would give any district court in the United States the authority to hear the challenges. Another possibility would be to model the judicial review after, in a sense, the pen/trap provision that's in FISA, which allows the FISA court or, in that case, its magistrate judges, a list of magistrate judges publicly designated by the Chief Justice.

You could have a similar model apply to the districts across the country so that we would know that you were selecting venues that would have the capacity to act quickly in terms of the facilities, et cetera, to handle something that would involve in-camera review of sensitive material.

I would be pleased to answer any questions the committee may have.

Chairman ROBERTS. We thank you very much for your testimony, Mr. Collins. Mr. Dempsey, you're next. And I would like to put a bug in your ears. I'm not asking for a rendition of Capital Gang or anything that's on television, but if each of you would have a comment on any of the others' comments in terms of a suggestion, why, we would be interested in that after Mr. Dempsey finishes his testimony.

And so we will now ask Mr. Dempsey for his commentary, please.

[The prepared statement of Mr. Dempsey follows:]

PREPARED STATEMENT OF JAMES X. DEMPSEY, EXECUTIVE DIRECTOR, CENTER FOR DEMOCRACY & TECHNOLOGY*

Chairman Roberts, Vice Chairman Rockefeller, Members of the Committee, thank you for the opportunity to testify this morning. I previously testified before the Committee on April 19, at which time I urged the Committee to preserve the PATRIOT Act powers but to adopt checks and balances to make them more effective and less subject to abuse. In particular, I stressed the role of prior judicial review based upon a factual showing and particularized suspicion. The draft bill before the Committee takes some small steps in the right direction, but overall the draft shifts radically in exactly the wrong direction.

In particular, I will focus on the proposal for administrative subpoenas in national security investigations. This is a big deal. The first, threshold question of need has not been addressed. And contrary to what has been said by some, there is no precedent in existing law for the grant of administrative subpoena power to the FBI in national security cases. Given the unique nature of intelligence investigations, which call for greater not lower standards, we urge the Committee to reconsider and reject this proposal.

At the outset, let me re-emphasize some basic points on which I hope there is widespread agreement:

• Terrorism poses a grave and imminent threat to our nation. There are people—almost certainly some in the United States—today planning additional terrorist attacks, perhaps involving biological, chemical or nuclear materials.

• The government must have strong investigative authorities to collect information to prevent terrorism. These authorities must include the ability to conduct electronic surveillance, carry out physical searches effectively, and obtain transactional records or business records pertaining to suspected terrorists.

• These authorities, however, must be guided by the Fourth Amendment, and subject to meaningful judicial controls as well as executive and legislative oversight and a measure of public transparency.

INTELLIGENCE INVESTIGATIONS ARE MORE DANGEROUS TO LIBERTY THAN CRIMINAL INVESTIGATIONS—THEY ARE BROADER, CAN ENCOMPASS FIRST AMENDMENT ACTIVITIES AND ARE MORE SECRETIVE AND LESS SUBJECT TO AFTER-THE-FACT SCRUTINY—AND THEREFORE INTELLIGENCE POWERS REQUIRE STRONGER COMPENSATING PROTECTIONS

Throughout the PATRIOT Act debate, and now in the context of administrative subpoenas, the government has argued that it should have the same powers subject to the same standards in intelligence investigations that it has in criminal investigations. As we will explain below, administrative subpoenas are not normally available in criminal investigations, but even if they were, there are strong reasons not to extend criminal justice norms (like "relevance") to intelligence investigations.

Intelligence investigations are special, in ways that make them preferable to the government, but also in ways that make them more dangerous to liberty than criminal investigations. First, intelligence investigations are broader. They are not limited by the criminal code. They can investigate legal activity. In the case of foreign nationals in the United States, they can focus solely on First Amendment activities. Even in the case of U.S. persons, they can collect information about First Amendment activities. In this context, the concept of "relevance" has little meaning. Look

*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 information privacy and security issues.

at Section 215 and the proposed administrative subpoena authority. They refer to "an investigation to protect against international terrorism." The standard does not say "an investigation into international terrorism activities"—that would at least mean that there was some specific terrorism activity being investigated. Instead, it says "an investigation to protect against international terrorism." Think about an investigation to "protect against" tax fraud. Or an investigation to "protect against" bank robbery. How broad would that be?[1]

Second, intelligence investigations are conducted in much greater secret than criminal cases, even perpetual secret. When a person receives a grand jury subpoena or an administrative subpoena in an administrative proceeding, normally he can publicly complain about it. In a criminal case, even the target is often notified while the investigation is underway. Most searches in criminal cases are carried out with simultaneous notice to the target. Even though wiretaps are conducted in secret, the target is notified afterwards. Notice is an important element of Fourth Amendment norms, but most searches and wiretaps in intelligence investigations are secret forever. Under the proposed administrative subpoena authority, the FBI can compel the recipient to perpetual secrecy.

Third, the big show in a criminal investigation is the trial. A prosecutor knows that, at the end of the process, his actions will all come out in public. If he is overreaching, if he went on a fishing expedition, that will all be aired, and he will face public scrutiny and even ridicule. That's a powerful constraint. Similarly, an administrative agency like the SEC or the FTC must ultimately account in public for its actions, its successes and its failures. But most intelligence investigations never result in a trial or other public proceeding. The evidence is used clandestinely. Sometimes the desired result is the mere sense that the government is watching.

Since intelligence investigations are broader, more secret and there is no after the fact scrutiny, protections must be built in at the beginning. That is where the PATRIOT Act fell short and where the proposal for administrative subpoenas falls short.

THE DIGITAL REVOLUTION IS PLACING MORE AND MORE INFORMATION IN THE HANDS OF THIRD PARTIES

Section 215 of the PATRIOT Act and to an even greater degree the administrative subpoena authority are of especially grave concern because they exploit trends in technology that threaten to almost eliminate privacy. More and more information about our lives is collected in daily transactions by those with whom we transact business. Grocery stores, other merchants, hotels, travel agents, insurance companies, and banks all collect computerized information about our actions. Credit cards, EZ passes, cell phones, and the Internet generate digital fingerprints giving a broad picture of our interests and associations. Congress has tried to keep pace, with laws on financial privacy and medical privacy, but the administrative subpoena provisions of the draft bill would wipe those protections away.

Moreover, a storage revolution is sweeping the field of information and communications technology. ISPs, websites and other online service providers are offering very large quantities of online storage, for email, calendars, photographs and even voicemail. Increasingly, ordinary citizens are storing information not in their homes or even on portable devices but on networks, under the control of service providers who can be served with compulsory process and never have to tell the subscribers that their privacy has been invaded.

THE THRESHOLD QUESTION—THERE HAS BEEN NO SHOWING OF NEED

The 9/11 Commission concluded that the burden of proof for retaining—and equally so for adding—a particular governmental power should be on the executive to explain that the power actually materially enhances security. To show that a power is needed, the government must show that current powers are inadequate. With respect to administrative subpoenas, the government has not met that burden.

As the Justice Department itself has noted, the rationale behind administrative subpoenas is that "Without sufficient investigatory powers, including some authority to issue administrative subpoena requests, Federal governmental entities would be unable to fulfill their statutorily imposed responsibility to implement regulatory or fiscal policies." U.S. Department of Justice, Office of Legal Policy, "Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities, pursuant to Public Law 06–544" (2002) at p. 6. As the DOJ

[1] This point was articulated by Suzanne Spaulding in her May 10, 2005 testimony before the Senate Judiciary Committee.

goes on to note, limiting this authority "would leave administrative entities unable to execute their respective statutory authorities." Id at 7.

Under current law, the FBI already has far-reaching and sufficient compulsory powers to obtain any relevant information when it is investigating terrorism, under both its criminal and intelligence authorities:

• *Search Warrants.* In any criminal investigation of international terrorism, the FBI can obtain a search warrant for documents or other materials if there is a judicial finding of probable cause that a crime is being planned. Search warrants can be issued not only to search a suspect's home, but also to obtain documents from any other third party if they constitute evidence of a crime.

• *Grand Jury Subpoenas.* The FBI also can use grand jury subpoenas in any criminal investigation of international terrorism to obtain any documents or other materials.

• *FISA Orders and NSLs.* In internatiional terrorism cases, the FBI has sweeping authority to obtain business records and any other tangible things under the Foreign Intelligence Surveillance Act, as amended by the PATRIOT Act. This authority exists not only in Section 215, but also in the five National Security Letter authorities for those categories of records considered especially pertinent to intelligence investigations.

The government has made no showing that these powers are insufficient. To the contrary, it has repeatedly praised the PATRIOT Act as providing the necessary tools to prevent terrorism and to prosecute a host of terrorism-related cases. Given these broad existing powers, and given the widespread public and Congressional concern that some of the existing PATRIOT Act powers are not subject to sufficient checks and balances, there is no justification for going even further down the path of unchecked authority.

THERE IS NO PRECEDENT FOR GIVING THE FBI ADMINISTRATIVE SUBPOENA POWER—WHAT WE DO WITH "CROOKED DOCTORS" HAS NO BEARING ON NATIONAL SECURITY INVESTIGATIONS

Contrary to what has been said by some, there is no precedent for giving the FBI administrative subpoena power. The FBI has long sought, and Congress has long rejected granting it, the authority to issue its own orders compelling disclosure of records. This is an issue that goes back to the momentous debates around the "FBI Charter" in the late 1970s and early 1980s, when administrative demand authority was one of the most contentious issues. More recently, in July 1996, after the Oklahoma City bombing, the Administration sought administrative subpoena authority and Congress rejected it. In 2001, in the original PATRIOT Act proposal, the Administration again sought administrative subpoena power and again Congress rejected it.

Congress has repeatedly denied the FBI the power to write its own compulsory orders for good reason. An administrative subpoena is an extraordinary device. In this case, it is essentially a piece of paper signed by an FBI official that requires any recipient to disclose any documents or any other materials. (We note that the proposed administrative subpoena in the Committee draft would not convey the power to compel a person to give testimony to the FBI. This, at least, is an important line to draw.)

In a 2002 study, the Department of Justice identified approximately 335 administrative subpoena authorities existing in the law.[2] Of those, 330 are for administrative agencies and not really relevant here, since, to say the least, the FBI's intelligence division is not an administrative agency. The 330 are in the context of administrative, regulatory programs—such as OSHA and the SEC. They are subject to various checks and balances. They often issue directly to the subjects of investigations. They are generally not subject to secrecy rules. Only 5 are for use primarily in criminal investigations and even those have histories and limitations that make them unsuitable as analogies for what the FBI is seeking:

• *21 USC 876—Controlled Substances Act.* When the FBI in 1982 was given joint jurisdiction with the DEA over drug enforcement, it got for drug cases the administrative subpoena authority that went with the enforcement of the regulatory system for controlled substances. The subpoenas are served, for example, on pharmacies and doctors suspected of engaging in the diversion of controlled substances to the black market. According to CRS, "The earliest of the three Federal statutes used

[2] U.S. Department of Justice, Office of Legal Policy, "Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities, pursuant to Public Law 06–544" (2002). See also Charles Doyle, Congressional Research Service, "Administrative Subpoenas and National Security Letters in Criminal And Foreign Intelligence Investigations: Background and Proposed Adjustments" (April 15, 2005).

extensively for criminal investigative purposes appeared with little fanfare as part of the 1970 Controlled Substances Act. . . . [T]he legislative history of section 876 emphasizes the value of the subpoena power for administrative purposes—its utility in assigning and reassigning substances to the acct's various schedules and in regulating the activities of physicians, pharmacists and the pharmaceutical industry. . . ."

• *5 U.S.C. App. (III)—Inspectors General Act.* The Inspector General system is unique, because it is largely focused inward, toward the conduct of Federal agencies and programs. The Inspectors General seek to achieve systemic reform, and their powers are quasi-regulatory. They oversee the administration of Federal procurements, the use of Federal resources and the administration of Federal procurements.

• U.S.C. 3486(a)(1)(A)(i)(I)—In a little-noticed provision in the Health Insurance Portability and Accountability Act (HIPAA), the massive medical insurance law of 1996, the Department of Justice was given administrative subpoena authority for investigation of Medicare and Medicaid fraud. Notably, the Attorney General has not delegated his administrative subpoena power to the FBI in health care fraud investigations. The medical care sector is highly regulated. Medicare and Medicaid involve Federal tax dollars. Generally, in these cases, the government serves the subpoena on the entity it is investigating, not some third party. Thus, when the Justice Department demands records from a hospital or insurance company as part of a health care fraud investigation, it is investigating that hospital or insurance company—not the customers of those entities. That creates some built-in checks on the administrative subpoena process. Indeed, the HIPAA rules for administrative subpoenas require that individuals' health information contained in those records can be depersonalized whenever possible.

• 18 U.S.C. 3486(a)(1)(A)(i)(II)—The administrative subpoena provision for child abuse cases was also adopted without much debate and is used mainly to obtain subscriber account information from Internet Service Providers. See 18 U.S.C. 3486(a)(1)(C).

• 18 U.S.C. 3486(a)(1)(A)(ii)—The Secret Service has authority to issue administrative subpoenas, but only in cases involving an "imminent" threat to one of its protectees. According to the Department of Justice, "Where a finding of "imminence" is not appropriate, the Secret Service does not seek an administrative subpoena but proceeds, instead, through the process of procuring a grand jury subpoena through a local United States Attorney's office." DOJ report, p. 39. The provision was adopted in 2000, but the authority was not delegated to the Secret Service until November 2001, and in calendar 2001, neither the Secretary of the Treasury nor the Secret Service issued a single administrative subpoena.

It is apparent from the foregoing that the FBI's administrative subpoena authority is limited to only two situations, drug matters and child abuse cases. The former is largely related to the administration of a regulatory scheme and is often subject to the accountability that comes from serving the subpoena on the target (a drug company or pharmacy), rather than secretly on a third party. By contrast, the administrative subpoena proposal in the Committee draft is designed to allow the FBI to obtain information, in secret, from entities that are not under investigation themselves but have customers whose records the FBI is seeking. The person under investigation never knows that the FBI has sought or obtained those records. With no other external check like a court or grand jury, the FBI would have almost limitless power to collect sensitive personal information.

JUDICIAL CHALLENGE IS A LIMITED PROTECTION, INSUFFICIENT TO OVERCOME CONCERNS WITH THE AUTHORITY

The Committee bill would allow the recipient of an administrative subpoena to challenge it, and consideration is being given to providing some form of judicial challenge for Section 215 orders. While judicial challenge is appropriate, it does not resolve our concerns, for two reasons:

First, few recipients of Section 215 orders or administrative sybpoenas would be likely to challenge them. These disclosure orders are not served on individuals. They are served on businesses—airlines, hotel chains, and other third parties. These businesses are provided immunity for complying. They never have to tell their customers that there records have been soought and the customers never receive notice. So why would such a business go to the expense of challenging a Section 215 order or administrative subpoena? A business has little incentive to spend its money challenging a subpoena for records that pertain to someone else. And since the business is prohibited from notifying its customer of the existence of the subpoena, the customer has no right to challenge the subpoena.

Second, the rules for administrative subpoenas require the courts to be extremely deferential to executive branch agencies. Courts must defer to an agency's determination of relevancy "so long as it is not 'obviously wrong.'" *United States* v. *Hunton & Williams*, 952 F. 2d. 843, 845 (3rd Cir. 1995). The Third Circuit noted that the "reasonableness" inquiry in such cases is even more deferential than the Administrative Procedure Act's "arbitrary and capricious" standard for review of agency action. Id. As the Justice Department admits, "the burden of proof imposed on a challenger to an administrative subpoena is steep." DOJ Report. For example, a challenge based on bad faith will be successful only upon a showing of "institutionalized bad faith, not mere bad faith on the part of the official issuing the subpoena." *United States* v. *LaSalle Nat'l Bank,* 437 U.S. 298, 316 (1978).

INTELLIGENCE INVESTIGATIONS POSE UNIQUE RISKS AND REQUIRE SPECIAL PROTECTIONS

The argument is made, if over 300 agencies have administrative subpoena power, why shouldn't the FBI in intelligence investogations. The answer is that no doctor will be deatined and deported in a secret proceeding following use of the HIPAA administrative subpoena power, no pharmacist will be held in a military prison as an illegal enemy combatant based on information provided under the Controlled Substances Act, no subject of an administrative subpoena will be sent to Egypt via "rendition" in a child abuse investigation. The governemnt has claimed an extraordinarily broad range of powers in intelligence investigation, especially against foreign nationals but also against citizens. Given the secrecy with which these investigations are conducted, their breadth, and the lack of after-the-fact checks and balances, protections of liberty must come up front, in the form of meaningful judicial review based on a factual premise and particularized suspicion.

MAIL COVERS

We will say only a few words on the provisions related to mail covers. First, we know of no justification for this provision. We suspect that the problems the FBI has encountered with the Postal Service are minor and could be resolved by negotiation, perhaps mediated by this Committee.

Second, though, we fear that the proposal is not merely a codification of existing practice but rather than shift of power from the Postal Service to the FBI. We note that the Postal Services regulations start with an affirmation of the policy that the "U.S. Postal Service maintains rigid control and supervision with respect to the use of mail covers." 39 CFR 233.3. We are concerned that the FBI may not be as careful.

Finally, we note a fundamental question: Is the concept of a mail cover, whether administered by the Postal Service or the FBI, outdated? Congress has moved to bring a variety of intelligence processes under the supervision of the FISA court. Section 215 applies to business records, and FISA also requires court approval for use of pen registers and trap and trace devices. The mail cover is a little like a transactional record, although it requires effort to create it. The mail cover is also comparable to a pen register or trap and trace device: A mail cover collects to and from information on surface mail, a pen register collects to and from information on a telephone call or email. The records provision of FISA and the pen/trap are both subject to judicial approval. If the Committee really found a need to codify mail cover authorities, then it should consider making all transactional record provisions subject to the same standard: judicial approval, based on a factual showing and particularity.

CONCLUSION

Twenty-five public interest organizations from across the political spectrum have written to oppose the administrative subpoena provision. Their letter states:

> At the very time when there seems to be an emerging consensus around adding meaningful checks and balances to PATRIOT Act powers to protect against government abuse, "administrative subpoenas" would represent a new, unchecked power. At the very time when the Attorney General is supporting amendments to strengthen judicial oversight of orders under Section 215 of the PATRIOT Act, authorization of "administrative subpoenas" would move radically in the opposite direction.
>
> Indeed, Attorney General Gonzales has repeatedly emphasized that the *prior* judicial approval required for Section 215 orders is a safeguard against abuse. The Attorney General's assurances would be meaningless, however, if the FBI could issue disclosure orders with no judicial approval.

The Center for Democracy and Technology looks forward to working with you to strike the right balance, to ensure that the government has the tools it needs to prevent terrorism, and that those tools are subject to appropriate checks and balances.

STATEMENT OF JAMES X. DEMPSEY, EXECUTIVE DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. DEMPSEY. Chairman Roberts, Vice Chairman Rockefeller, good morning. Thank you for the opportunity to testify at this hearing.

The premise of my testimony, Mr. Chairman, is that terrorism poses a grave and urgent threat to our Nation and that the government must have strong investigative powers to collect information to prevent terrorism, and that these authorities must be subject to clear standards and meaningful judicial controls, as well as executive and legislative oversight.

Although we have serious concerns about the mail-cover proposal—and I'll be happy to address some of the other questions that Vice Chairman Rockefeller raised—I will focus on the proposal for administrative subpoenas.

What the bill proposes is a very big step. The first threshold question of need has not been addressed adequately. And, contrary to what has been said, administrative subpoena power is not generally available in criminal cases. Even if it were, the argument that the government should have the same powers, subject to the same standards, in intelligence investigations that it has in other investigations is off track.

The fact is, the government is seeking the tools of administrative or criminal investigations without the checks and balances. Intelligence investigations are different from criminal investigations in ways that make them preferable to the government but also in ways that make them more dangerous to liberty.

First, intelligence investigations are broader. They're not limited by the criminal code. They can investigate legal activity. Even in the case of U.S. persons, they can collect information about First Amendment activities.

Terrorism is uniquely ideological. By definition, it involves political views. In this context, the concept of relevance has little meaning.

Second, intelligence investigations are conducted in much greater secrecy than criminal or administrative cases, even perpetual secrecy. When a person receives a grand jury subpoena or an administrative subpoena, often he can complain about it at the time, and any secrecy imposed is limited. Intelligence investigations, of course, are generally kept secret forever.

Third, the big show in a criminal investigation is the trial. The prosecutor knows that at the end of the process, his actions will all come out in public. If he was on a fishing expedition, that will come out. He could be subject to ridicule. That's a powerful constraint.

Now, if the government really wanted the same powers in intelligence investigations that they have in criminal investigations, I would be inclined to say, "Fine, let them issue subpoenas publicly without secrecy. Let them inform the target. Let them be focused and limited only to investigating crimes." But that's not what intel-

ligence investigations are about. And that's why they need special protections.

Now, on the threshold question, there's been no showing of need. The government has failed to show need, with the one exception of speed—and I'll address the question of urgency or emergencies. Other than that, they have not shown that their current counterterrorism powers are inadequate.

Senator, why do 330 administrative agencies have administrative subpoena power? Because otherwise they could not do their jobs. They have no grand jury power. They have no National Security Letter authority. They have no orders under Section 215 of the PATRIOT Act and FISA. The justification for the administrative subpoenas is that those are non-criminal agencies.

In the absence of a showing of need, one argument for administrative subpoenas has been that, well, everybody else has it. But, if you look at the record closely, you will see that there is no precedent for granting the FBI administrative subpoena power in national security cases. This is an issue that goes back decades. I always tell people I have in my files on this mimeographed documents. Back in the momentous debate over the FBI charter in the seventies and eighties, the FBI sought administrative subpoena power, Congress declined to give it.

More recently, in 1996 after the Oklahoma City bombing and the African embassy bombings, the administration sought administrative subpoena power and Congress rejected it. In 2001, in the original PATRIOT Act proposal, the administration sought administrative subpoena power, and the Congress rejected it.

In 2002, the Justice Department completed a study in which they identified approximately 335 administrative subpoena authorities existing in law. Of those, 330 are for administrative agencies and not really relevant here since, to say the least, the FBI national security division is not an administrative agency. Only five of the administrative subpoena powers on the books are primarily used in criminal investigations and, of those, only two are available to the FBI.

Everybody talks about crooked doctors. The administrative subpoena power for health care investigations grows out of a regulatory scheme for Medicare and Medicaid and the administration of those systems. And as far as I know, that administrative subpoena power resides in the Justice Department and has not been delegated by the Attorney General to the FBI. If anybody has any information to the contrary, I'd welcome it, but, as far as I know, that is not an FBI power for health care investigations.

Second, is Inspectors General but they largely look inward. They administer government programs. There's no inspector general for the FBI, and there's no inspector general administrative subpoena power at the FBI. The Secret Service has administrative subpoenas, but only for imminent threats to protectees. Otherwise, the Secret Service has to go the grand jury route as well.

So, we come down to two—one for drugs, which also grows out of an administrative process; the whole scheduling of prescription drugs and narcotics, and the regulation of pharmacies to make sure drugs aren't diverted into the illegal market. And then one for child abuse cases, which is largely limited, if you look at the statute, to

obtaining customer identifying information in the case of communications, which for national security investigations, the FBI already has with the National Security Letter.

So the issue seems to boil down to the question of speed and, if so, then the solution is clear. And I think Senator Feinstein has offered it—an emergency exception to Section 215, the business records provision. Title III, the criminal wiretap law, the criminal pen register law, FISA for electronic surveillance, FISA for physical searches, all have emergency exceptions.

You have to go get a court order, generally, to do a wiretap or to get a pen register, but there's an emergency exception. Section 215 could have—maybe should have—an emergency exception, not as a matter of course, not as a general rule, but in those situations where speed is of the issue.

Intelligence investigations pose unique risks, and they require special protections. No doctor will be detained and deported in secret proceedings based upon an administrative subpoena issued in a healthcare investigation. No subject of an administrative subpoena will be sent to Egypt via rendition in a child abuse case. The Inspectors General are not worried about the use of political demonstrations as a cover for terrorism, but the FBI is.

The government has claimed an extraordinarily wide range of powers in intelligence investigations. Given the secrecy with which these investigations are conducted, their breadth, and the fact that most of them never come to light, that the subjects never know that they were being conducted, protections of liberty must come up front in the form of meaningful judicial review based on a factual premise and particularized suspicion.

I'll be happy to discuss mail covers and some of the other issues posed by both the Committee draft bill as well as the PATRIOT Act.

Thank you, Mr. Chairman. I look forward to your questions.

Chairman ROBERTS. We thank you Mr. Dempsey.

As I indicated, if any member of the panel has any comment to make at this particular time, hearing the summation of the total panel, now would be the time to offer any commentary. And we already have a hand raised with Mr. Onek.

Mr. ONEK. I'd like to take off on two comments by Mr. Collins. The first is when he talked about the most-favored nation rules. As I think my testimony and Mr. Dempsey's testimony suggest, we'll live by that rule, because there is no comparable subpoena power anywhere else. There is no subpoena power that's as broad and there is no subpoena power that's as secret. So, the most-favored nation rule is fine because there's nothing equivalent, and what is being suggested here is absolutely new.

Second, Mr. Collins was discussing Section 215, and definitely, and he said the court order is not a rubber stamp. And this is interesting because the administration, throughout the debate on the PATRIOT Act, as been going around the country saying how wonderful Section 215 is. Now, we tend to disagree, although we like the fact that Section 215 does have a court order, but now, after going around the country and saying how wonderful Section 215 is, they're eviscerating it. Section 215 will become unnecessary, because the FBI will simply be able to use administrative subpoenas.

So it's just inconsistent. You can't go around defending Section 215 and saying it's good because the judge is not a rubber stamp and the judge can do this and the judge can do that, and he can modify the order, et cetera, et cetera, and then propose something which just wipes Section 215 off the map. It's just totally inconsistent.

Chairman ROBERTS. Mr. Collins, I presume you would like to say something.

Mr. COLLINS. Yes I would, Mr. Chairman.

I think it is not accurate to say that there's no precedent. I think Mr. Dempsey has incorrectly described the scope of the administrative subpoena authority, for example, in child porn cases. He indicated that it was limited to the NSL-type information that can be requested under 2709.

If you look at 18 USC 3486, which describes the scope of the administrative subpoena authority in child porn cases, there is a specific provision that governs subpoenas in those cases to providers of electronic communications. That's in subparagraph C, but in the paragraph before, it says, except as provided in subparagraph C—so we treat electronic service providers differently—a subpoena issued under subparagraph A may require "the production of any records or other things relevant to the investigation" and "testimony by the custodian of the things required to be produced concerning the production and authenticity of those things."

It is as broad; it is indeed the model, so far as I can tell, for the draft bill that is before the Committee, where relevance is the operative standard. Indeed the draft bill before the Committee is in one respect narrower in that it does not authorize the actual taking of physical testimony. It does not require anyone to actually show up, but merely requires production of the documents and a certification. So in one respect, actually, it's even narrower than the child porn model that's already in existing law on the criminal side.

Chairman ROBERTS. Mr. Dempsey, do you have any response to that?

Mr. DEMPSEY. All I'll say, Mr. Chairman, is that the most important evidence in a child porn investigation is what's stored on the computer, or what's with the service provider.

Chairman ROBERTS. Or the child.

Mr. DEMPSEY. Well, you're trying to find the child, which means you're trying to find the person who might have him, and the administrative subpoena power is limited to subscriber identifying information.

Chairman ROBERTS. The distinguished vice chairman has a question.

Vice Chairman ROCKEFELLER. What interests me about all of this—neither the Chairman nor myself are lawyers, which is——

Chairman ROBERTS. A good thing.

[Laughter.]

Vice Chairman ROCKEFELLER. Which is a good thing. But it also causes us to look at the way people who are lawyers, whether they're from the FBI or formerly associated with other administrations, look at things. And it occurs to me that people get very hung up on precedents or the possibility of something going wrong and that somebody's rights might get violated.

I think we look at that, and without being conclusive in our thinking, as I indicated in my opening statement, this is kind of a new era. Now, we put into place the PATRIOT Act shortly after 9/11. There were a lot of new things in that, and some of them have—I would say for the most part, I have been impressed at how little criticism it has received except in some quarters, and there it's very, very hard, hard shell.

What is wrong in taking ideas, like an administrative procedures approach—subpoenas approach—and not making the conclusion that the government will set out to violate rights, but understanding that in a new world—and when I say that, I say that with the fullest, deepest concern about the future of our country—and homeland security is not only the great weak link, but homeland security also affects this conversation. So, it's a form of homeland security, security of the American people, also the rights of the American people.

What is wrong in taking something which could do good and which could very well pick up that person at the hotel more quickly that the DOJ witness referred to, and saying, as I think you did Mr. Kris—you just nodded, so I just picked on you—that you go with that.

You worry about it, but you don't make it permanent. You do what we did in fact with the original PATRIOT Act, which is to say we are introducing new concepts here, because 9/11 was extraordinary, and by the way, the situation in Iraq and across the world, in my judgment, generally speaking and not of interest to this panel, is that the world is getting worse quickly and that there will be results from that, and that you go with something with which you can nail down somebody who would do substantial damage to the country through a dirty bomb or something of that sort, but you don't let it be permanent. You say, let's come back and look at it in 4 years, just as we have done on the original parts of the PATRIOT Act. What is wrong with that?

Mr. ONEK. Senator, I was originally skeptical—I have to admit—of the sunsets, but in retrospect they were brilliant. They have worked. I think I cited to this Committee—but if I didn't, I think it's highly relevant—that the FBI's own internal memos on the PATRIOT Act talk about the fact that the sunsets are there, that these authorities will be subject to scrutiny, and therefore the FBI general counsel's office advised the field, be careful how you use these authorities because you're going to be subject to that sunset scrutiny.

Now, if we remove the sunsets entirely, where do the countervailing checks and balances come from? I would suggest that they should come from meaningful judicial review before the fact in all but emergency cases. I think the after-the-fact review is limited, as Ms. Caproni recognized. But if we remove the sunsets entirely, such as on Lone Wolf, which hasn't even been in effect for 6 months now, and on some of these other provisions that we may not be sure of, then where does the constraint come from?

Chairman ROBERTS. If I might, I think some of that review comes from the Congress. As Chairman of the Committee, and as Vice Chairman of the Committee, I know that both of us feel very strongly, as do all members of the Committee, if it were a sunset

of 4 years that means that we would have reviewed it eight times if it's on the 6-month basis; if it were more frequent than that, that would be the case.

And let me assure everyone here that while much of this is closed because of the classified nature of the operations, we do take this very, very seriously. I don't mean that you implied anything otherwise, but I did want to point out that this doesn't happen in a vacuum, that we do take it very seriously, we do review it very seriously, and I interrupted somebody.

Yes, Mr. Onek.

Mr. ONEK. Senator, we are in a new world, but as we just heard from the FBI spokesperson, all they've said is there may be emergency situations. So if that's the case, then I don't see why the Committee should do more than create some sort of new emergency provision. The ideal one, from our standpoint, would be a new emergency provision under FISA, just as you already have under FISA for searches and for wiretaps. Why do they need the total package—administrative subpoenas for everything when the only reason they really cite to is an emergency.

So, give them that, and if they feel somehow that that's not enough, or the emergency provision that the Congress writes is inadequate, they, of course, can come back and tell us. But they have not given any justification here or anywhere else for the broad sweeping power that they ask for.

The 9/11 Commission, which was certainly concerned with security, as are we all, said when the government asks for a new authority, it has to justify why it needs it. And the most we have heard here today is that there may be some emergency situations like the hotel situation. Fine, let's deal with that situation, but they're going way, way beyond it. They're asking—remember, what they are asking for is the ability to circumvent Section 215 altogether.

The Congress spent a lot of time on that provision in the PATRIOT Act. But the proposed legislation will do away with it. Why would anybody ever have to use Section 215 for anything, whether it's a library record, a medical record, if they can just issue a subpoena?

You're throwing away Section 215 of the PATRIOT Act. Why? The witness was right here. The most she could say was, "Gee, we sometimes have emergencies." I don't want to make light of that because obviously one emergency can obviously mean saving thousands of lives, so let's have an emergency exception. But why have this general, sweeping legislation way beyond anything that the government has ever seen before?

Don't kid yourself. Mr. Collins says, "Gee, there's broad authority under child porn." Well, yes, but it's about child porn only. There's only a narrow set of records you can get. The FBI, when it's investigating foreign intelligence, can potentially get every record about everything. And, of course, there's secrecy here that doesn't exist in these other situations. Why do you want to go down that road? It doesn't make any sense. What makes sense, if there is any emergency need, is an emergency exception, and as Jim Dempsey has pointed out, there are several models. There are emergency excep-

tions in Title III and in FISA, and there may be other models you can use. Sit down and work that out.

But there's no justification for something beyond an emergency provision. I just don't see it.

Vice Chairman ROCKEFELLER. I hear what you're saying, all of you, and I will need to decide what makes sense to me. Thank you.

Chairman ROBERTS. Mr. Kris, I think you have something to say.

Mr. KRIS. Yes, I guess I just wanted to sort of follow up. I was struck in listening to the testimony that both Mr. Dempsey and Mr. Onek both favor ex-ante judicial review over ex-post in a motion to quash.

And I don't speak for the government any longer, but if I were the government, I would happily trade motions to quash, particularly motions to quash filed in the Foreign Intelligence Surveillance Court, in exchange for a requirement for ex-ante judicial review before a magistrate, particularly if we want to spread the authority out into the field with an emergency exception.

I don't know if DOJ would make that trade, but once we get into the horse trading part of legislative deliberations it seems to be that that's a good bargain for the government, and I'm interested in the fact that the sort of civil libertarians are more focused on and think there is more value in ex-ante than ex-post judicial review.

Chairman ROBERTS. Yes, Mr. Collins.

Mr. COLLINS. Let me make one brief comment. The existing HIPAA and child porn administrative subpoena provision doesn't have a sunset and isn't limited to emergencies. If it were a choice between those two, I would probably lean in favor of a sunset over an emergency, because at least the sunset allows you to see it in operation and then make the informed choice at the end in light of the data actually received.

Because at that point you may have the same reaction that Mr. Dempsey had to the child porn, which is that, well, that hasn't turned out to be a problem because they actually look only at a narrow set of records. You could make that judgment rather than speculate about it.

Mr. DEMPSEY. Why not both? Why not emergency only and sunset? A sunset would certainly be better than no sunset, but when there's no justification for going beyond emergency, I think it would be extraordinary for this Committee to do that, truly extraordinary, sunset or not.

Chairman ROBERTS. I'm just having a little trouble subscribing to the notion that if you have something that would be an infrequent use of the constitutional investigative tool, that that means it should not be provided. Nor do I think, at least at this juncture, that we shouldn't provide or extend authority because another tool may be used less.

I don't know. Maybe it's because every week in this place, in the hallowed halls of Congress, we find ourselves in the park or someplace, the train station, some other area allegedly that is safe, and I think most people are getting a little tired of it, and I know my staff is and I know their parents are back in Kansas.

Maybe that's not analogous to the statements that have been made, but it just seems to me that we need more tools, not less,

when it comes to terrorism and espionage, and by saying that, don't misunderstand me. I appreciate all of your suggestions, more especially in regards to privacy and civil rights.

Mr. Dempsey, I was a bit struck, although it's not being fair because I was in the back and I heard you—I wasn't here but I was here; I was sort of in-camera, so to speak. But I think you asserted that the concept of relevance has no meaning in a terrorism investigation. What does that mean?

Mr. DEMPSEY. Well, Senator, look at Section 215 of the PATRIOT Act, the business records provision, or Section 214. They talk about investigations "to protect against" international terrorism—not investigations of international terrorism, not investigations of terrorist activities, but investigations "to protect against" international terrorism.

Think about an investigation to protect against tax fraud or an investigation to protect against bank robbery. How broad would that be? In the terrorism area, the intelligence area, the standard is foreign power and agent of a foreign power, which applies to organizations that engage in legal as well as illegal activity, and the scope of those investigations can encompass legal activity. In the case of non-U.S. persons, those investigations can be predicated solely on the basis of legal activity.

So, in an investigation to protect against international terrorism, I think the agent may think he knows what he's doing, but I think there should be some factual premise for that. The reason I have a problem with Section 215 is that it involves a judge, but the government comes in and says this information is relevant to an investigation to protect against international terrorism. They don't have to say which investigation, they don't have to say who they are looking for, they don't have to provide any factual evidence.

And the statute says the judge "shall" issue the order, as requested or modified. He can't even ask, tell me where this is going, why do you need these particular records? I agree with you entirely, Mr. Chairman, and with the Vice Chairman as well, the government needs access to information to prevent terrorism. But we know people under pressure—and absolutely the FBI and the other homeland security and intelligence agencies are under pressure—people under pressure cut corners. They do the easy thing rather than the hard thing. They go off on false tangents.

I don't think that it's incompatible with our national security to have checks and balances. I don't think that we're only talking here about privacy or civil liberties, although definitely we are. I think we're also talking about guidance, focus, effectiveness, ensuring that investigations are going somewhere, because the threats are pouring in every day, as you suggested—fleeing the Capitol here in response to what turned out to be in two cases false alarms.

There are a lot of false alarms out there and the agencies are drowning in information. They need more focus, not less. They need more standards and guidelines, not fewer. Sure, give them the tools, but make sure those tools are subject to controls.

And this Committee takes very seriously its oversight role, but given all the rest that this Committee has to deal with and that the members of this Committee have to deal with, it's very hard

to look at those individual FISA applications. I don't know, I would hesitate to wonder how many people here have actually read a pen register/trap and trace FISA application. There are thousands of them. There's a thousand FISA orders.

So, Committee is important. You know, Germany has a purely parliamentary approach to the approval of national security wiretaps. But that's not the route we've chosen to go here. We've chosen to combine judicial oversight. The U.K. has, of course, just ministerial, AG-type approval, but we've chosen to go with both judicial approval and with legislative and executive oversight based upon our system of checks and balances. And I think that should apply throughout, including to the mail covers.

Chairman ROBERTS. I think I've opened up Pandora's Box here. Mr. Kris.

Mr. KRIS. Let me just make a very brief and pretty narrow technical response to that. It's true that under section 1861 of FISA you can get records and tangible things if you certify that they're sought for an investigation against terrorism.

What I'm about to say, I don't know if it will make people feel better or worse, but if you compare that to the standards that govern a routine criminal grand jury investigation, I don't think they're very different. The Supreme Court has held in a case called The United States against R. Enterprises that a grand jury can issue a subpoena, which means effectively, that a grand jury, through an Assistant U.S. Attorney, can issue a subpoena to investigate even rank hearsay and gossip suggesting the possibility of a crime or even just to satisfy itself that no crime is being committed at all.

And the standards for trying to quash a grand jury subpoena are extremely difficult to meet. So, again, I don't know if that makes you feel better or worse, but I do think that standard in FISA is not all that different conceptually from the standard that governs a grand jury investigation. Those standards have to be low, because the acquisition of records occurs very early in an investigation when the government doesn't have all of the information that it has at the end.

Chairman ROBERTS. Well, I want to thank all of you members for your testimony. I think it's been very helpful and we will consider all of your suggestions and comments as we continue the markup of this legislation. As I've indicated before, this is an open process in which all members concerned will be seriously considered.

I would just say that I would hope that after the many incidents that we have seen happen not only in the United States but also throughout the world, that we do have an international problem and that we do want to stop terrorism before it counts, to detect and deter it as opposed to getting into the tragedy of consequence management.

I don't think it's a good idea to go back and to try to investigate it as a crime, and I don't mean that to perjure anything that anybody has said here in regard to this panel. I think you've offered some very fine advice and suggestions and I thank you for coming.

And since I'm the only person here that you would be testifying to, perhaps it's a good time to say the Committee stands adjourned.

[Whereupon, at 11:47 a.m., the Committee adjourned.]

○